Antivirus Mac Lab/CardioLab Consignes d'installation (FR)

Version logicielle de Mac-Lab/CardioLab 6.9.6

Introduction

Les fonctions du logiciel antivirus assurent la conformité aux réglementations de confidentialité, telles que HIPAA.

Objet du document

Ce document contient les instructions d'installation d'un logiciel antivirus validé pour le système Mac-Lab/CardioLab v6.9.6.

Historique des révisions

Révision	Date	Commentaires
A	16 février 2016	Première parution publique.
B	9 juin 2016	Mise à jour de Trend Micro pour compatibilité avec la fonction CO_2.
C	16 mai 2017	Mises à jour pour McAfee ePolicy Ochestrator, Trend Micro et Symantec.
D	10 juillet 2017	Mises à jour pour Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9, et McAfee VSE 8.8 Patch 9.
E	14 août 2017	Retrait des références à McAfee ePolicy Orchestrator 5.9 et McAfee VirusScan Enterprise 8.8 Patch 9. Ajout de 6.9.6 R3 UI languages.
F	25 septembre 2017	Ajout de McAfee ePO 5.9 et McAfee VSE 8.8 Patch 9. Liens de mise à jour pour Trend Micro 11 et 12.
G	9 mai 2019	• Ajout de McAfee ePO 5.10.0 et McAfee VSSE 8.8 Patch 12 • Ajout du logiciel antivirus Symantec 14.2.0 MP1 • Ajout de Trend Micro OfficeScan Client/Server Edition XG SP1

Mise en route

Exigences concernant le logiciel antivirus

AVERTISSEMENT : INSTALLATION DU LOGICIEL ANTIVIRUS REQUISE

Le système est fourni sans protection antivirus. Assurez-vous qu'un antivirus validé est installé sur le système avant de le connecter à un réseau. L'absence de protection antivirus validée peut entraîner une instabilité du système ou sa défaillance.

Notez les exigences suivantes :

- Aucun logiciel antivirus n'est fourni avec le système Mac-Lab/CardioLab et il incombe au client d'en acheter un, de l'installer et de le mettre à jour.
- Le client est responsable de la mise à jour des fichiers de définition de l'antivirus.
- Si un virus est détecté, contactez l'administrateur système de votre établissement et l'assistance technique GE.
- Seuls les logiciels antivirus figurant dans la liste des logiciels antivirus validés peuvent être installés.
- Pour appliquer les instructions présentées dans ce document, connectez-vous en tant qu'administrateur ou que membre de ce groupe.
- Utilisez si possible une version du logiciel antivirus validé dans la langue du système d'exploitation. S'il n'existe aucun logiciel antivirus validé dans la langue du système d'exploitation, installez la version anglaise du logiciel antivirus.

Logiciels antivirus validés

AVERTISSEMENT : INSTABILITÉ DU SYSTÈME

N'utilisez pas de logiciel antivirus non validé (ni de versions non validées de celui-ci). Cela risquerait d'entraîner l'instabilité du système ou sa défaillance. Utilisez uniquement un logiciel antivirus validé dans la langue appropriée.

REMARQUE : Si le logiciel antivirus n'est pas disponible dans la langue que vous souhaitez, installez-le dans la version anglaise.

Les systèmes Mac-Lab/CardioLab version 6.9.6 ont été validés pour fonctionner avec les logiciels répertoriés dans le tableau suivant.

Logiciels antivirus pris en charge	Langues MLCL prises en charge	Versions de logiciels antivirus pris en charge
McAfee VirusScan Enterprise	Anglais, français, allemand, italien, espagnol, suédois, norvégien, danois, néerlandais, chinois, japonais	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9 8.8 Patch 12

Logiciels antivirus pris en charge	Langues MLCL prises en charge	Versions de logiciels antivirus pris en charge
McAfee ePolicy Orchestrator (avec McAfee VirusScan Enterprise)	Anglais, français, allemand, italien, espagnol, suédois, norvégien, danois, néerlandais, chinois, japonais	v5.0 v5.3.2 v5.9 v5.10
Symantec EndPoint Protection	Anglais, français, allemand, italien, espagnol, suédois, norvégien, danois, néerlandais, chinois, japonais	12.1.2, 12.1.6 MP5, 14.0 MP1, 14.2.0 MP1
Trend Micro OfficeScan Client/Server Edition	Anglais, français, allemand, italien, espagnol, suédois, norvégien, danois, néerlandais, chinois, japonais	10.6 SP2, 11.0 SP1, XG 12.0, XG SP1

Le logiciel antivirus pris en charge est disponible dans les langues répertoriées dans le tableau suivant.

Version MLCL	Langues MLCL prises en charge
6.9.6 R1	Anglais
6.9.6 R2	Anglais, français, allemand
6.9.6 R3	Anglais, français, allemand, italien, espagnol, suédois, norvégien, danois, néerlandais, chinois, japonais

Configuration du serveur de la console de gestion de l'antivirus

La console de gestion de l'antivirus doit être installée sur le serveur de la console de gestion de l'antivirus.

La communication entre le serveur de la console de gestion de l'antivirus et les périphériques Mac-Lab/CardioLab peut être assurée de différentes manières en fonction de l'environnement :

1. Environnement du contrôleur de domaine INW - Le serveur de la console de gestion de l'antivirus est extérieur au domaine du serveur INW
   - Type de communication n° 1 <Même réseau avec même masque de sous-réseau>
   - Type de communication n° 2 <Réseau différent avec masque de sous-réseau différent>
2. Environnement du contrôleur du domaine de l'hôpital - Le serveur de la console de gestion de l'antivirus est extérieur au domaine du contrôleur du domaine de l'hôpital
   - Type de communication n° 1 <Réseau différent avec masque de sous-réseau différent>
3. Environnement du contrôleur du domaine de l'hôpital - Le serveur de la console de gestion de l'antivirus est à l'intérieur du domaine du contrôleur du domaine de l'hôpital
   - Type de communication n° 1 <Même réseau avec même masque de sous-réseau>

REMARQUE : Le serveur de la console de gestion de l'antivirus doit être équipé de deux ports réseau, l'un pour la connexion au réseau Centricity Cardiology INW et l'autre pour la connexion au réseau de l'hôpital.

Schéma fonctionnel de l'environnement du contrôleur de domaine INW

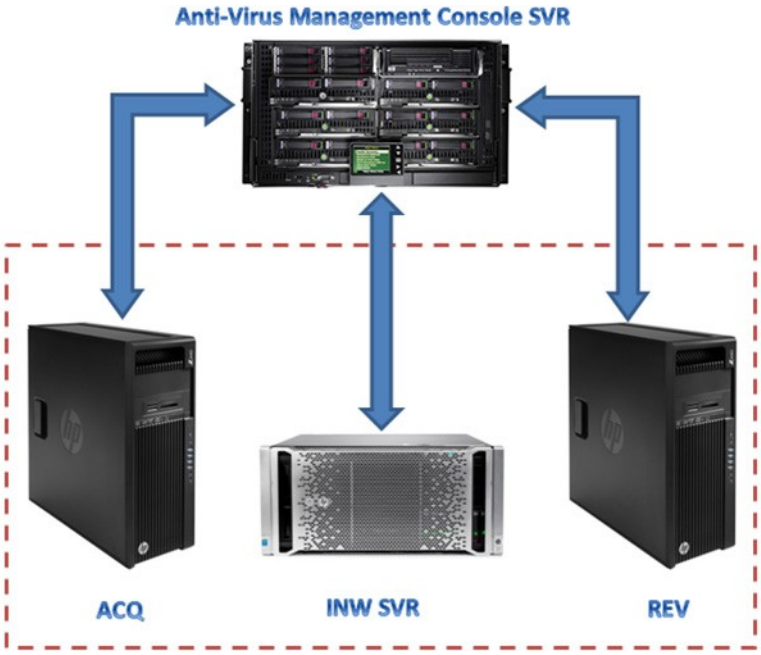
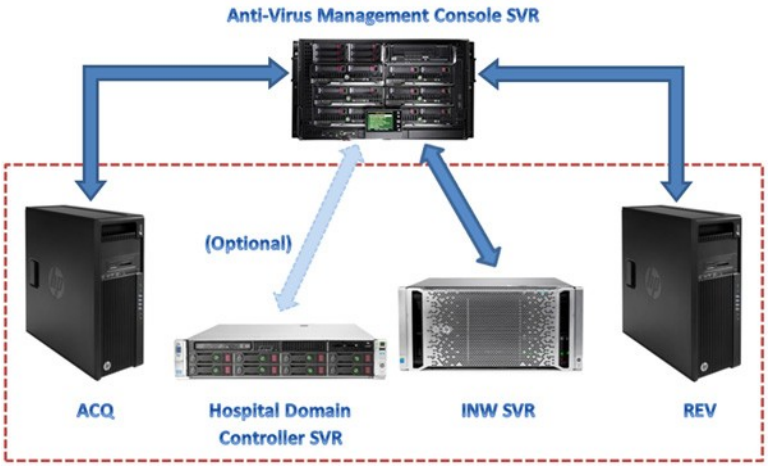
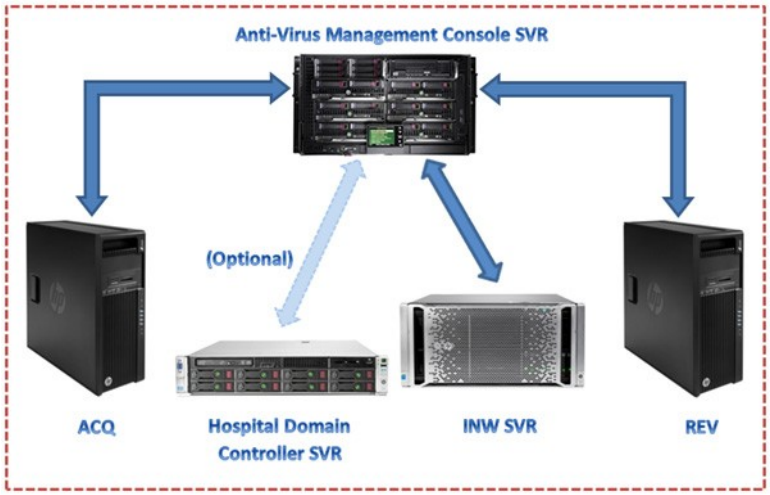


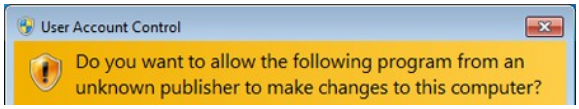
Schéma fonctionnel de l'environnement du contrôleur du domaine de l'hôpital





Contrôle de compte d'utilisateur

Le contrôle de compte d'utilisateur est une fonction Windows qui assure une protection contre les risques de modifications non autorisées apportées à un ordinateur. Un message de contrôle de compte d'utilisateur peut s'afficher lors de certaines procédures appliquées dans ce manuel.



Ne tenez pas compte de ce message s'il est lié à des procédures contenues dans ce manuel ; vous pouvez poursuivre votre travail en toute sécurité.

Instructions d'installation de l'antivirus

Cliquez sur le logiciel antivirus que vous souhaitez installer :

Procédure d'installation du logiciel antivirus

Appliquez les instructions fournies dans cette section lorsqu'elles figurent dans les instructions d'installation du logiciel antivirus.

Désactivation de la connexion de bouclage

Sur un système d'acquisition connecté à l'environnement Mac-Lab/CardioLab, désactivez la connexion de bouclage afin de détecter tous les systèmes clients possédant le même masque de sous-réseau sur le domaine.

1. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe.
2. Cliquez avec le bouton droit sur ***Network*** (Réseau) sur le bureau et sélectionnez ***Properties*** (Propriétés).
3. Cliquez sur ***Change adapter settings*** (Modifier les paramètres de l'adaptateur).
4. Cliquez avec le bouton droit sur ***Loopback Connection*** (Connexion de bouclage) et sélectionnez ***Disable*** (Désactiver).
5. Redémarrez le système d'acquisition.

REMARQUE : Il est nécessaire de désactiver la connexion de bouclage sur le système d'acquisition pour détecter tous les systèmes clients utilisant le même masque de sous-réseau sur le domaine.

Activation de la connexion de bouclage

Sur un système d'acquisition connecté à l'environnement Mac-Lab/CardioLab, activez la connexion de bouclage en appliquant les instructions ci-dessous.

1. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe.
2. Cliquez avec le bouton droit sur ***Network*** (Réseau) sur le bureau et sélectionnez ***Properties*** (Propriétés).
3. Cliquez sur ***Change adapter settings*** (Modifier les paramètres de l'adaptateur).
4. Cliquez avec le bouton droit sur ***Loopback Connection*** (Connexion de bouclage) et sélectionnez ***Enable*** (Activer).
5. Redémarrez le système d'acquisition.

Configuration du service Remote Registry (Accès à distance du registre) avant l'installation de l'antivirus

Vérifiez le paramètre service Remote Registry (Accès à distance du registre) des systèmes d'acquisition et de consultation en réseau pour vous assurer qu'il est configuré correctement.

1. Cliquez sur Start > Run (Démarrer > Exécuter).
2. Entrez services.msc et appuyez sur Entrée.
3. Double-cliquez sur le service Remote Registry (Accès à distance du registre).
4. Notez le type de démarrage pour le service Remote Registry (Accès à distance du registre) _____.
5. Vérifiez que le Startup Type (Type de démarrage) est réglé sur Automatic (Automatique). Si ce n'est pas le cas, rétablissez ce réglage et cliquez sur Start (Démarrer).
6. Cliquez sur OK.
7. Fermez la fenêtre Services.

Configuration du partage de fichiers simple avant l'installation de l'antivirus

1. Ouvrez l'Explorateur de fichiers.
2. Sélectionnez sur Tools > Folder Options (Outils > Options des dossiers).
3. Sélectionnez l'onglet View (Affichage).
4. Faites défiler vers le bas et décochez l'option Use Sharing Wizard (Recommended) (Utiliser l'Assistant Partage [recommandé]).
5. Cliquez sur Apply (Appliquer), puis sur OK.

Configuration du service Explorateur d'ordinateurs avant l'installation de l'antivirus

Vérifiez le paramètre service Computer Browser (Explorateur d'ordinateurs) des systèmes d'acquisition et de consultation en réseau pour vous assurer qu'il est correctement configuré.

1. Cliquez sur ***Start > Control Panel > Network and Sharing Center*** (Démarrer > Panneau de configuration > Centre Réseau et partage).
2. Cliquez sur ***Change advanced sharing settings*** (Modifier les paramètres de partage avancés).
3. Développez ***Home or Work*** (Domicile ou travail).
4. Vérifiez que l'option ***Turn on file and printer sharing*** (Activer le partage de fichiers et d'imprimantes) est sélectionnée.
5. Cliquez sur ***Save changes*** (Enregistrer les modifications).
6. Cliquez sur ***Start > Run*** (Démarrer > Exécuter).
7. Saisissez **services.msc** et appuyez sur **Entrée**.
8. Double-cliquez sur le service ***Computer Browser*** (Explorateur d'ordinateurs).
9. Vérifiez que le ***Startup Type*** (Type de démarrage) est réglé sur ***Automatic*** (Automatique). Si ce n'est pas le cas, rétablissez ce réglage et cliquez sur ***Start*** (Démarrer).
10. Cliquez sur ***OK***.
11. Fermez la fenêtre ***Services***.

Configuration du partage de fichiers simple après l'installation de l'antivirus

1. Ouvrez l'Explorateur de fichiers.
2. Sélectionnez sur Tools > Folder Options (Outils > Options des dossiers).
3. Sélectionnez l'onglet View (Affichage).
4. Faites défiler vers le bas et décochez l'option Use Sharing Wizard (Recommended) (Utiliser l'Assistant Partage [recommandé]).
5. Cliquez sur Apply (Appliquer), puis sur OK.

Configuration du service Remote Registry (Accès à distance du registre) après l'installation de l'antivirus

Vérifiez le paramètre service Remote Registry (Accès à distance du registre) des systèmes d'acquisition et de consultation en réseau pour vous assurer qu'il est configuré correctement.

1. Cliquez sur ***Start > Run*** (Démarrer > Exécuter).
2. Entrez **services.msc** et appuyez sur **Entrée**.
3. Double-cliquez sur le service ***Remote Registry*** (Accès à distance du registre).
4. Modifiez le Startup type (Type de démarrage) à l'état enregistré à l'étape 4 de la section Configuration du service Remote Registry (Accès à distance du registre) avant l'installation de l'antivirus.
5. Cliquez sur ***OK***.
6. Fermez la fenêtre ***Services***.

Configuration du service Explorateur d'ordinateurs après l'installation de l'antivirus

Après avoir installé le logiciel antivirus, vérifiez les paramètres du service Computer Browser (Explorateur d'ordinateurs) des systèmes
d'acquisition et de consultation en réseau pour vous assurer qu'il est configuré correctement.

1. Cliquez sur ***Start > Run*** (Démarrer > Exécuter).
2. Saisissez **services.msc** et appuyez sur **Entrée**.
3. Double-cliquez sur le service ***Computer Browser*** (Explorateur d'ordinateurs).
4. Réglez ***Startup type*** (Type de démarrage) sur ***Manual*** (Manuel).
5. Cliquez sur ***OK***.
6. Fermez la fenêtre ***Services***.

Symantec EndPoint Protection (12.1.2, 12.1.6 MP5, 14.0 MP1, 14.2.0 MP1)

Présentation de l'installation

Installez Symantec EndPoint Protection dans les environnements Mac-Lab/CardioLab en réseau uniquement. Dans un environnement en réseau, le logiciel Symantec EndPoint Protection doit être installé sur le serveur de la console de gestion de l'antivirus avant d'être déployé en tant que client sur le serveur Centricity Cardiology INW et les postes de travail d'acquisition/de consultation. Procédez comme suit pour installer et configurer ***Symantec EndPoint Protection***.

La mise à jour des listes de virus incombe à l'établissement. Mettez régulièrement à jour les définitions afin de bénéficier de la toute dernière protection sur le système.

REMARQUE : Symantec EndPoint Protection 14.2.0 MP1 est pris en charge par les configurations en réseau et autonome Mac-Lab/CardioLab.

Consignes de pré-installation

1. La console de gestion de l'antivirus Symantec est censée avoir été installée conformément aux instructions de Symantec et être en bon état de fonctionnement.
2. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur tous les systèmes clients (acquisition, consultation et serveur INW) pour installer le logiciel antivirus.
3. Ouvrez l'invite Commande en mode ***Run as administrator*** (Exécuter en tant qu'administrateur).
4. Accédez à C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

REMARQUE : Pour configurer le serveur INW, accédez à C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Entrez **UpdateRegSymantec.ps1** et appuyez sur ***Entrée***.
6. Confirmez la bonne exécution du script.

   Si le chemin indiqué ci-dessus n'est pas présent, réalisez les étapes suivantes pour tous les systèmes MLCL, à l'exception du serveur MLCL 6.9.6R1 INW (Système d'exploitation du serveur : Windows Server 2008R2).

   a. Cliquez sur le bouton ***Start*** (Démarrer), puis sur ***Run*** (Exécuter).

   b. Saisissez **Regedit.exe**, puis cliquez sur ***OK***.

   c. Accédez à ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\TrustProviders\Software Publishing.***

   d. Recherchez le registre ***State*** (État) puis double-cliquez dessus.

   e. Réglez la ***Base*** sur ***Decimal*** (Décimal).

   f. Réglez ***Value data*** (Données de valeur) sur ***146432***.

   g. Reprenez de l'étape **c** à l'étape **f** ci-dessus pour ***HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***

   h. Cliquez sur ***OK*** puis fermez le registre.

7. Désactivez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Désactivation de la connexion de bouclage, page 6.
8. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs avant l'installation de l'antivirus, page 7.

Configuration de l'adaptateur réseau pour les systèmes Symantec en réseau et autonomes avant l'installation de l'antivirus

Procédez comme suit pour configurer votre adaptateur réseau pour le déploiement de Symantec AV sur les systèmes ACQ, consultation, consultation virtuelle, serveur INW et le serveur de la console de gestion de Symantec (MC).

1. Cliquez sur Start (Démarrer) et accédez à Control panel > Network and Sharing center > Change adapter settings (Panneau de configuration > Centre Réseau et partage > Modifier les paramètres de l'adaptateur).

2. Cliquez avec le bouton droit de la souris sur Local Area Connection (Connexion au réseau local) et sélectionnez Properties (Propriétés).
3. Cliquez sur Internet Protocol Versions 4 (TCP/IPv4) (Protocole Internet versions 4 [TCP/IPv4]).
4. Cliquez sur Properties (Propriétés).
5. Saisissez la passerelle par défaut pour les systèmes autonomes et les systèmes du domaine.

   REMARQUE : L'adresse IP de la console de gestion Symantec AV peut être utilisée comme passerelle par défaut s'il n'y a pas de passerelle par défaut dans l'environnement.
6. Saisissez le serveur DNS préféré pour les systèmes réseau.

Configurez Remote User Access Control (LocalAccountTokenFilterPolicy) (Contrôles d'accès à distance de l'utilisateur) pour les systèmes Symantec en réseau et autonomes avant l'installation de l'antivirus

Procédez comme suit pour créer/configurer les paramètres de registre UAC sur ACQ, Consultation, Consultation virtuelle et le serveur InW.

1. Ouvrez l'invite de commande avec des droits d'administrateur.
2. Exécutez la commande suivante
3. reg add “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system” /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

Symantec EndPoint Protection - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée)

1. Cliquez sur ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec* Endpoint Protection Manager** (Démarrer > Tous les programmes > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager).
2. Saisissez le nom d'utilisateur et le mot de passe pour vous connecter au Symantec Endpoint Protection Manager. (Cliquez sur ***Yes*** (Oui) en cas d'affichage d'un message de sécurité.)
3. Cochez la case ***Do not show this Welcome Page again*** (Ne plus afficher cette page d'accueil) et cliquez sur ***Close*** (Fermer) pour fermer l'écran d'accueil.

REMARQUE : Pour la version 14.0 MP1, cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Getting Started on Symantec EndPoint Protection*** (Commencer à utiliser Symantec EndPoint Protection).

4. Cliquez sur ***Admin*** dans la fenêtre ***Symantec EndPoint Protection Manager***.
5. Cliquez sur ***Install Packages*** (Installer les Packages) dans le volet inférieur.
6. Cliquez sur ***Client Install Feature Set*** (Fonctions d'installation du client) dans le volet supérieur.
7. Cliquez avec le bouton droit sur la fenêtre ***Client Install Feature Set*** (Fonctions d'installation du client) et sélectionnez ***Add*** (Ajouter). La fenêtre Add Client Install Feature Set (Ajouter des fonctions d'installation du client) s'ouvre.
8. Saisissez le nom choisi et notez-le car vous en aurez besoin plus tard.
9. Vérifiez que la ***Feature set version*** (Version des fonctions) est ***12.1 RU2 and later*** (12.1 RU2 et suivantes).

10. Sélectionnez uniquement les fonctions suivantes et désélectionnez toutes les autres.
    - ***Virus, Spyware, and Basic Download Protection*** (Protection contre les virus et les logiciels espions, et protection de base du téléchargement).
    - ***Advanced Download Protection*** (Protection avancée du téléchargement).
11. Cliquez sur ***OK*** dans la zone de message.
12. Pour les versions 12.1.2, 12.1.6 MP5 et 14.2.0 MP1 uniquement, cliquez sur ***OK*** pour fermer la fenêtre ***Add Client Install Feature Set*** (Ajouter des fonctions d'installation du client).
13. Selon la version logicielle, effectuez l'une des actions suivantes :
    - **Versions 12.1.2 et 12.1.6 MP5 :**
      Cliquez sur ***Home*** (Accueil) dans la fenêtre ***Symantec Endpoint Protection Manager***. Sélectionnez ***Install protection client to computers*** (Installer le client de protection sur les ordinateurs) dans la liste déroulante ***Common Tasks*** (Tâches courantes) en haut à droite de la fenêtre ***Home*** (Accueil). L'écran Client Deployment Type (Type de déploiement du client) s'affiche.
    - **Version 14.0 MP1 et 14.2.0 MP1 :** Cliquez sur ***Clients*** dans la fenêtre ***Symantec Endpoint Protection Manager***. Dans ***Tasks*** (Tâches), cliquez sur ***Install a client*** (Installer un client). L'écran ***Client Deployment wizard*** (Assistant de déploiement du client) s'affiche.
14. Sélectionnez ***New Package Deployment*** (Nouveau déploiement de package) et cliquez sur ***Next*** (Suivant).
15. Sélectionnez le nom des fonctions choisi à l'étape 8. Conservez les autres paramètres par défaut et cliquez sur ***Next*** (Suivant).
16. Sélectionnez ***Remote push*** (« Push » à distance) et cliquez sur ***Next*** (Suivant). Attendez que l'écran ***Computer selection*** (Sélection des ordinateurs) s'affiche.
17. Développez le ***<Domaine>*** (par exemple : INW). Les systèmes connectés au domaine sont affichés dans la fenêtre ***Computer selection*** (Sélection des ordinateurs).

REMARQUE : Si aucun système n'est reconnu, cliquez sur ***Search Network*** (Rechercher sur le réseau) puis sur ***Find Computers*** (Rechercher les ordinateurs). Appliquez la méthode de détection ***Search by IP address*** (Rechercher par adresse IP) pour identifier les systèmes clients (acquisition, consultation et serveur INW).

18. Sélectionnez toutes les machines du client Mac-Lab/CardioLab qui sont connectées au domaine et cliquez sur **>>**. L'écran des ***Login Credentials*** (Paramètres de connexion) s'affiche.
19. Saisissez le nom d'utilisateur, le mot de passe et le nom du domaine/ordinateur et cliquez sur ***OK***.
20. Vérifiez que toutes les machines sélectionnées s'affichent sous ***Install Protection Client*** (Installer le client de protection) et cliquez sur ***Next*** (Suivant).
21. Cliquez sur ***Send*** (Envoyer) et attendez que le logiciel antivirus Symantec soit déployé sur tous les systèmes clients (acquisition, consultation et serveur INW). Lorsque vous avez terminé, l'écran ***Deployment Summary*** (Résumé du déploiement) s'affiche.
22. Cliquez sur ***Next*** (Suivant) puis sur ***Finish*** (Terminer) pour fermer le Client Deployment Wizard (Assistant de déploiement du client).
23. Attendez que l'icône Symantec s'affiche sur la barre des tâches puis redémarrez les machines clientes (acquisition, consultation et serveur INW). Après le redémarrage, connectez-vous en tant qu'administrateur ou membre de ce groupe sur toutes les machines clientes.

Configurations de la console Symantec EndPoint Protection Server

1. Sélectionnez ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager*** (Démarrer > Tous les programmes > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager). La fenêtre de connexion à Symantec EndPoint Protection Manager s'ouvre.
2. Entrez le mot de passe Symantec Endpoint Protection Manager Console et cliquez sur ***Log On*** (se connecter).
3. Sélectionnez l'onglet ***Policies*** (Stratégies) et cliquez sur ***Virus and Spyware Protection*** (Protection contre les virus et les logiciels espions) dans ***Policies*** (Stratégies). La fenêtre ***Virus and Spyware Protection Policies*** (Stratégies antivirus et anti-logiciels espions) s'ouvre.
4. Cliquez sur la stratégie ***Add a Virus and Spyware Protection*** (Ajouter une protection antivirus et anti-logiciels espions dans ***Tasks*** (Tâches). La fenêtre ***Virus and Spyware Protection*** (Protection antivirus et anti-spyware) s'ouvre.
5. Dans ***Windows Settings > Scheduled Scans*** (Paramètres Windows > Analyses planifiées), cliquez sur ***Administrator-Defined Scans*** (Analyses définies par l'administrateur).
6. Sélectionnez ***Daily Scheduled Scan*** *(Analyses quotidiennes planifiées)* et cliquez sur ***Edit*** *(Modifier)*. La fenêtre ***Edit Scheduled Scan*** (Modifier l'analyse planifiée) s'ouvre.
7. Changez le nom et la description de l'analyse en ***Weekly Scheduled Scan*** *(Analyses hebdomadaires planifiées)* et ***Weekly Scan at 00:00*** *(Analyse hebdomadaire à 00h00)*, respectivement.
8. Sélectionnez le ***Scan type*** (Type d'analyse) ***Full Scan*** (Analyse complète).
9. Sélectionnez l'onglet ***Schedule*** (Planifier).
10. Dans ***Scanning Schedule*** (Planification des analyses), sélectionnez ***Weekly*** (Hebdomadaire) et remplacez l'heure par ***00:00***.
11. Dans ***Scan Duration*** (Durée de l'analyse), désélectionnez la case ***Randomize scan start time within this period*** *(recommended in VMs)* (Définir une heure de début d'analyse de manière aléatoire pendant cette période [recommandé dans les VM]) et sélectionnez ***Scan until finished*** *(recommended to optimize scan performance)* (Analyser jusqu'à la fin [recommandé pour optimiser la performance de l'analyse]).
12. Dans ***Missed Scheduled Scans*** (Analyses planifiées manquées), désélectionnez la case ***Retry the scan within*** (Recommencer l'analyse dans).
13. Cliquez sur l'onglet ***Notifications***.
14. Désélectionnez la case ***Display a notification message on the infected computer*** *(Afficher un message de notification sur l'ordinateur infecté)*, puis cliquez sur ***OK***.
15. Cliquez sur l'onglet ***Advanced*** *(Avancé)* dans la fenêtre ***Administrator-Defined Scans*** *(Analyses définies par l'administrateur)*.
16. Dans ***Scheduled Scans*** (Analyses planifiées), désélectionnez ***Delay scheduled scans when running on batteries*** (Ajourner les analyses planifiées en cas de fonctionnement sur piles), ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Autoriser l'exécution des analyses planifiées définies par l'utilisateur lorsque l'auteur de l'analyse n'est pas connecté) et ***Display notifications about detections when the user logs on*** (Afficher les notifications sur les détections lorsque l'utilisateur se connecte).

REMARQUE : Pour la version 14.0 MP1 et 14.2.0 MP1, dans ***Scheduled Scans*** (Analyses planifiées), désélectionnez ***Delay scheduled scans when running on batteries*** (Ajourner les analyses planifiées en cas de fonctionnement sur piles) et ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Autoriser l'exécution des analyses planifiées définies par l'utilisateur lorsque l'auteur de l'analyse n'est pas connecté).

17. Dans ***Startup and Triggered Scans*** (Démarrage et analyses déclenchées), désélectionnez ***Run an Active Scan when new definitions arrive*** (Exécuter une analyse active lorsque de nouvelles définitions arrivent).
18. Dans ***Windows Settings > Protection Technology*** (Paramètres Windows > Technologie de Protection), cliquez sur ***Auto-Protect*** (Protection automatique).
19. Cliquez sur l'onglet ***Scan Details*** (Détails de l'analyse) et cochez la case ***Enable Auto-Protect*** (Activer la protection automatique).
20. Cliquez sur l'onglet ***Notifications*** et désélectionnez les cases ***Display a notification message on the infected computer*** (Afficher un message de notification sur l'ordinateur infecté) et ***Display the Auto-Protect results dialog on the infected Computer*** (Afficher la fenêtre des résultats de la protection automatique sur l'ordinateur infecté).
21. Cliquez sur l'onglet ***Advanced*** (Avancé) et, dans ***Auto-Protect Reloading and Enablement*** (Rechargement et activation de la protection automatique), cochez l'option ***When Auto-Protect is disabled, Enable after:*** (Lorsque la protection automatique est désactivée, activer au bout de :).
22. Dans ***Additional Options*** *(Options supplémentaires)*, cliquez sur File Cache (Fichier cache). La fenêtre ***File Cache*** (Fichier cache) s'ouvre.
23. Désélectionnez ***Rescan cache when new definitions load*** (Réanalyser la mémoire cache lors du chargement des nouvelles définitions) et cliquez sur ***OK***.
24. Dans ***Windows Settings > Protection Technology*** (Paramètres Windows > Technologie de protection), cliquez sur ***Download Protection*** (Protection du téléchargement).
25. Cliquez sur l'onglet ***Notifications*** et désélectionnez la case ***Display a notification message on the infected computer*** (Afficher un message de notification sur l'ordinateur infecté).
26. Dans ***Windows Settings > Protection Technology*** (Paramètres Windows > Technologie de protection), cliquez sur ***SONAR***.
27. Cliquez sur l'onglet ***SONAR Settings*** (Paramètres SONAR) et désélectionnez la case ***Enable SONAR*** (Activer SONAR).
28. Dans ***Windows Settings > Protection Technology*** (Paramètres Windows > Technologie de protection), cliquez sur ***Early Launch Anti-Malware Driver*** (Pilote du logiciel anti-malware à lancement anticipé).
29. Désélectionnez la case ***Enable Symantec early lauch anti-malware*** (Activer le logiciel anti-malware à lancement anticipé de Symantec).
30. Dans ***Windows Settings > Email Scans*** (Paramètres Windows > Analyse des courriers électroniques), cliquez sur ***Internet Email Auto-Protect*** (Protection automatique du courrier électronique Internet).
31. Cliquez sur l'onglet ***Scan Details*** (Détails de l'analyse) et désélectionnez la case ***Enable Internet Email Auto-Protect*** (Activer la protection automatique du courrier électronique Internet).
32. Cliquez sur l'onglet ***Notifications*** et désélectionnez les cases ***Display a notification message on the infected computer*** (Afficher un message de notification sur l'ordinateur infecté), ***Display a progress indicator when email is being sent*** (Afficher un indicateur de progression lorsque le courrier électronique est en cours d'envoi) et ***Display a notification area icon*** (Afficher une icône de zone de notification).
33. Dans ***Windows Settings > Email Scans*** (Paramètres Windows > Analyse des courriers électroniques), cliquez sur ***Microsoft Outlook Auto-Protect*** (Protection automatique Microsoft Outlook).
34. ***Cliquez sur l'onglet Scan Details*** (Détails de l'analyse) et désélectionnez la case ***Enable Microsoft Outlook Auto-Protect*** (Activer la protection automatique Microsoft Outlook).
35. Cliquez sur l'onglet ***Notifications*** et désélectionnez la case ***Display a notification message on the infected computer*** (Afficher un message de notification sur l'ordinateur infecté).

36. Dans ***Windows Settings > Email Scans*** (Paramètres Windows > Analyse des courriers électroniques), cliquez sur ***Lotus Notes Auto-Protect*** (Protection automatique Lotus Notes).
37. Cliquez sur l'onglet ***Scan Details*** (Détails de l'analyse) et désélectionnez la case ***Enable Lotus Notes Auto-Protect*** (Activer la protection automatique Lotus Notes).
38. Cliquez sur l'onglet ***Notifications*** et désélectionnez la case ***Display a notification message on infected computer*** (Afficher un message de notification sur l'ordinateur infecté).
39. Dans ***Windows Settings > Advanced Options*** (Paramètres Windows > Options avancées), cliquez sur ***Global Scan Options*** (Options globales d'analyse).
40. Dans ***Bloodhound(™) Detection Settings*** (Paramètres de détection Bloodhound(™)), désélectionnez la case ***Enable Bloodhound(™) heuristic virus detection*** (Activer la détection heuristique des virus Bloodhound(™)).
41. Dans ***Windows Settings > Advanced Options*** (Paramètres Windows > Options avancées), cliquez sur ***Quarantine*** (Mise en quarantaine).
42. Cliquez sur l'onglet ***General*** (Général) et, dans ***When New Virus Definitions Arrive*** (Lorsque de nouvelles définitions de virus arrivent), sélectionnez ***Do nothing*** (Ne rien faire).
43. Dans ***Windows Settings > Advanced Options*** (Paramètres Windows > Options avancées), cliquez sur ***Miscellaneous*** (Divers).
44. Cliquez sur l'onglet ***Notifications*** et désélectionnez ***Display a notification message on the client computer when definitions are outdated*** (Afficher un message de notification sur l'ordinateur client lorsque les définitions sont dépassées), ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** (Afficher un message de notification sur l'ordinateur client lorsque Symantec Endpoint Protection fonctionne sans définitions de virus) et ***Display error messages with a URL to a solution*** (Afficher des messages d'erreur avec une URL vers la solution).
45. Cliquez sur ***OK*** pour fermer la fenêtre de stratégie de ***Virus and Spyware Protection*** (Protection antivirus et anti-logiciels espions).
46. Cliquez sur ***Yes*** (Oui) dans la zone de message ***Assign Policies*** (Affecter les stratégies).
47. Sélectionnez ***My Company*** (Ma société) et cliquez sur ***Assign*** (Affecter).
48. Cliquez sur ***Yes*** (Oui) dans la zone de message.
49. Dans ***Policies*** (Stratégies), cliquez sur ***Firewall*** (Pare-feu).
50. Cliquez sur ***Firewall policy*** (Stratégie pare-feu) dans ***Firewall Policies*** (Stratégies pare-feu) et cliquez sur ***Edit the policy*** (Modifier la stratégie) dans ***Tasks*** (Tâches).
51. Cliquez sur l'onglet ***Policy Name*** (Nom de la stratégie), puis désélectionnez ***Enable this policy*** (Activer cette stratégie).
52. Cliquez sur ***OK***.
53. Dans ***Policies*** (Stratégies), cliquez sur ***Intrusion Prevention*** (Prévention des intrusions).
54. Cliquez sur la stratégie ***Intrusion Prevention*** (Prévention des intrusions) dans ***Intrusion Prevention Policies*** (Stratégies de prévention des intrusions) et cliquez sur ***Edit the policy*** (Modifier la stratégie) dans ***Tasks*** (Tâches).
55. Cliquez sur l'onglet ***Policy Name*** (Nom de la stratégie), puis désélectionnez ***Enable this policy*** (Activer cette stratégie).
56. Selon la version logicielle, effectuez l'une des actions suivantes :
    - **Version 12.1.2 :** Cliquez sur ***Settings*** (Paramètres) dans le volet de gauche.
    - **Versions 12.1.6 MP5, 14.0 MP1 et 14.2.0 MP1 :** Dans le volet de gauche, cliquez sur ***Intrusion Prevention*** (Prévention des intrusions).

57. Désélectionnez les cases ***Enable Network Intrusion Prevention*** (Activer la prévention des intrusions sur le réseau) et ***Enable Browser Intrusion Prevention for Windows*** (Activer la prévention des intrusions sur le navigateur pour Windows).
58. Cliquez sur ***OK***.
59. Dans ***Policies*** (Stratégies), cliquez sur ***Application and Device Control*** (Contrôle des applications et des périphériques).
60. Cliquez sur ***Application and Device Control Policy*** (Stratégie de contrôle des applications et des périphériques) dans ***Application and Device Control Policies*** (Stratégies de contrôle des applications et des périphériques), puis cliquez sur ***Edit the policy*** (Modifier la stratégie) dans ***Tasks*** (Tâches).
61. Cliquez sur l'onglet ***Policy Name*** (Nom de la stratégie), puis désélectionnez ***Enable this policy*** (Activer cette stratégie).
62. Cliquez sur ***OK***.
63. Dans ***Policies*** (Stratégies), cliquez sur ***LiveUpdate*** (Mise à jour en direct).
64. Sélectionnez ***LiveUpdate Settings policy*** (Stratégie des paramètres de mise à jour en direct [LiveUpdate]) et, dans ***Tasks*** (Tâches), cliquez sur ***Edit the policy*** (Modifier la stratégie).
65. Dans ***Overview > Windows Settings*** (Présentation > Paramètres Windows), cliquez sur ***Server Settings*** (Paramètres serveur).
66. Dans ***Internal or External LiveUpdate Server*** (Serveur LiveUpdate interne ou externe), vérifiez que l'option ***Use the default management server*** (Utiliser le serveur de gestion par défaut) est sélectionnée, et désélectionnez l'option ***Use a LiveUpdate server*** (Utiliser un serveur LiveUpdate).
67. Cliquez sur ***OK***.
68. Dans ***Policies*** (Stratégies), cliquez sur ***Exceptions***.
69. Cliquez sur ***Exceptions policy*** (Stratégie d'exception) et, dans ***Tasks*** (Tâches), cliquez sur ***Edit the policy*** (Modifier la stratégie).
70. Selon la version logicielle, effectuez l'une des actions suivantes :
    - **Versions 12.1.2 et 12.1.6 MP5 :** Cliquez sur ***Exceptions > Add > Windows Exceptions > Folder*** (Exceptions > Ajouter > Exceptions Windows > Dossier).
    - **Version 14.0 MP1 et 14.2.0 MP1 :** Cliquez sur la liste déroulante ***Add*** (Ajouter) et sélectionnez ***Windows Exceptions > Folder*** (Exceptions Windows > Dossier).
71. Entrez l'un après l'autre les chemins d'accès **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** puis procédez comme suit :

    a. Vérifiez que l'option ***Include subfolders*** (Inclure les sous-dossiers) est sélectionnée.

    REMARQUE : Cliquez sur ***Yes*** (Oui) si la zone de message ***Are you sure you want to exclude all subfolders from protection?*** (Êtes-vous sûr de vouloir exclure tous les sous-dossiers de la protection ?) s'affiche.

    b. Sélectionnez ***All*** (Tous) dans ***Specify the type of scan that excludes this folder*** (Indiquer le type d'analyse dont ce dossier est exclu).

    c. Pour la version 14.0 MP1 et 14.2.0 MP1, cliquez sur ***OK*** pour ajouter l'exception.
72. Cliquez sur ***OK***.
73. Cliquez sur Assign the policy (Affecter la stratégie) dans Tasks (Tâches).
74. Sélectionnez ***My Company*** (Ma société) et cliquez sur ***Assign*** (Affecter).
75. Cliquez sur ***Yes*** (Oui).

76. Cliquez sur ***Clients*** dans le volet de gauche et sélectionnez l'onglet ***Policies*** (Stratégies).

77. Dans ***My Company*** (Ma société), sélectionnez ***Default Group*** (Groupe par défaut), désélectionnez ***Inherit policies and settings from parent group "My Company"*** (Hériter des stratégies et des paramètres du groupe parent Ma société) et cliquez sur ***Communications Settings*** (Paramètres de communication) dans ***Location-Independent Policies and Settings*** (Stratégies et paramètres indépendants de l'emplacement).

REMARQUE : Si un message d'avertissement s'affiche, cliquez sur ***OK***, puis cliquez à nouveau sur ***Communications Settings*** (Paramètres de communication) dans ***Location-Independent Policies and Settings*** (Stratégies et paramètres indépendants de l'emplacement).

78. Dans ***Download*** (Télécharger), vérifiez que l'option ***Download policies and content from the management server*** (Télécharger les stratégies et les contenus depuis le serveur de gestion) est cochée et que ***Push mode*** (Mode « Push ») est sélectionné.

79. Cliquez sur ***OK***.

80. Cliquez sur General Settings (Paramètres généraux) dans Location-independent Policies and Settings (Stratégies et paramètres indépendants de l'emplacement).

81. ***Cliquez sur l'onglet Tamper Protection*** (Protection contre la falsification) et désélectionnez la case ***Protect Symantec security software from being tampered with or shut down*** (Protéger le logiciel de sécurité Symantec contre la falsification ou la fermeture).

82. Cliquez sur ***OK***.

83. Cliquez sur ***Admin*** et sélectionnez ***Servers*** (Serveurs).

84. Dans ***Servers*** (Serveurs), sélectionnez ***Local Site*** **(My Site)** (Site local [mon site]).

85. Dans ***Tasks*** (Tâches), sélectionnez ***Edit Site Properties*** (Modifier les propriétés du site). La fenêtre ***Site Properties for Locate Site*** *(My Site)* (Propriétés du site en vue de la localisation du site [Mon site]) s'ouvre.

86. Cliquez sur l'onglet ***LiveUpdate*** et, dans ***Download Schedule*** (Programme de téléchargement), vérifiez que le programme est réglé sur ***Every 4 hour(s)*** (Toutes les 4 heures).

87. Cliquez sur ***OK***.

88. Cliquez sur ***Log Off*** (Déconnexion) et fermez Symantec EndPoint Protection Manager Console. Vérifiez que les stratégies de Symantec Endpoint Protection sont communiquées aux systèmes clients en mode « Push ».

Après l'installation de Symantec EndPoint Protection

1. Activez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Activation de la connexion de bouclage, page 6.

2. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs après l'installation de l'antivirus, page 7.

3. Ouvrez l'invite Commande en mode ***Run as administrator*** (Exécuter en tant qu'administrateur).

4. Accédez à C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

REMARQUE : Pour configurer le serveur INW, accédez à C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Entrez **RestoreRegSymantec.ps1** et appuyez sur ***Entrée***.

6. Confirmez la bonne exécution du script.
   Remarque : Vous devez confirmer la bonne exécution du script **RestoreRegSymantec.ps1** avant de continuer.

   Si le chemin indiqué ci-dessus n'est pas présent, réalisez les étapes suivantes pour tous les systèmes MLCL, à l'exception du serveur MLCL 6.9.6R1 INW (Système d'exploitation du serveur : Windows Server 2008R2).

   a. Cliquez sur le bouton ***Start*** (Démarrer), puis sur ***Run*** (Exécuter).

   b. Saisissez **Regedit.exe**, puis cliquez sur ***OK***.

   c. Accédez à ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion \WinTrust\Trust Providers\Software Publishing.***

   d. Recherchez le registre ***State*** (État) puis double-cliquez dessus.

   e. Réglez la ***Base*** sur ***Decimal*** (Décimal).

   f. Réglez ***Value data*** (Données de valeur) sur ***65536***.

   g. Reprenez de l'étape **c** à l'étape **f** pour ***HKEY_USERS\DEFAULT \Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***

   h. Cliquez sur ***OK*** puis fermez le registre.

McAfee VirusScan Enterprise

Présentation de l'installation

McAfee VirusScan Enterprise doit être installé individuellement sur un système Mac-Lab/CardioLab et géré de façon séparée. Procédez comme suit pour installer et configurer McAfee VirusScan Enterprise.

La mise à jour des listes de virus incombe à l'établissement. Mettez régulièrement à jour les définitions afin de bénéficier de la toute dernière protection sur le système.

Procédure d'installation de McAfee VirusScan Enterprise

1. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe.
2. Insérez le CD **McAfee VirusScan Enterprise 8.8 Patch 3**, **McAfee VirusScan Enterprise 8.8 Patch 4**, **McAfee VirusScan Enterprise 8.8 Patch 8 CD**, **McAfee VirusScan Enterprise 8.8 Patch 9 CD ou McAfee VirusScan Enterprise 8.8 Patch 12 CD** dans le lecteur CD.
3. Double-cliquez sur ***SetupVSE.Exe***. La boîte de dialogue Windows Defender s'ouvre.
4. Cliquez sur ***Yes*** (Oui). L'écran d'installation de McAfee VirusScan Enterprise s'affiche.
5. Cliquez sur ***Next*** (Suivant). L'écran du contrat de licence d'utilisateur final McAfee s'affiche.
6. Lisez ce contrat de licence et saisissez les informations demandées dans les champs correspondants, puis cliquez sur ***OK*** lorsque vous avez terminé. L'écran de sélection du type d'installation s'affiche.
7. Sélectionnez ***Typical*** (Classique) et cliquez sur ***Next*** (Suivant). L'écran Select Access Protection Level (Sélection du niveau de protection d'accès) s'affiche.

8. Sélectionnez ***Standard Protection*** (Protection standard) et cliquez sur ***Next*** (Suivant). L'écran Ready to Install (Prêt pour l'installation) s'affiche.
9. Cliquez sur ***Install*** (Installer) et attendez la fin de l'installation. Une fois l'installation de McAfee VirusScan Enterprise terminée, le message ***McAfee Virus Scan Enterprise Setup has completed successfully*** (L'installation de McAfee Virus Scan Enterprise s'est déroulée avec succès) s'affiche.
10. Désélectionnez la case ***Run On-Demand Scan*** (Lancer une analyse à la demande) et cliquez sur ***Finish*** (Terminer).
11. Si la fenêtre ***Update in Progress*** (Mise à jour en cours) s'ouvre, cliquez sur ***Cancel*** (Annuler).
12. Si un message vous demandant de redémarrer le système s'affiche, cliquez sur ***OK***.
13. Redémarrez le système.
14. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe.

Configuration de McAfee VirusScan Enterprise

1. Cliquez sur ***Start > All Programs > McAfee > VirusScan Console*** (Démarrer > Tous les programmes > McAfee > Console VirusScan). L'écran ***VirusScan Console*** (Console VirusScan) s'affiche.
2. Cliquez avec le bouton droit de la souris sur ***Access Protection*** (Protection d'accès) et sélectionnez ***Properties*** (Propriétés). L'écran ***Access Protection Properties*** (Propriétés de protection d'accès) s'affiche.
3. Cliquez sur l'onglet ***Access Protection*** (Protection d'accès) et désélectionnez ***Enable access protection*** (Activer la protection d'accès) et ***Prevent McAfee services from being stopped*** (Empêcher l'arrêt des services McAfee).
4. Cliquez sur ***OK***.
5. Cliquez avec le bouton droit sur ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon) et sélectionnez ***Properties*** (Propriétés). L'écran ***Buffer Overflow Protection Properties*** (Propriétés de protection contre les dépassements de tampon) s'affiche.
6. Cliquez sur l'onglet ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon) et désélectionnez ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings*** (Afficher la boîte de dialogue des messages lorsqu'un dépassement de tampon est détecté dans les paramètres de dépassement de tampon).
7. Désélectionnez ***Enable buffer overflow protection*** (Activer la protection contre les dépassements de tampon) dans ***Buffer overflow settings*** (Paramètres de dépassement de tampon).
8. Cliquez sur ***OK***.
9. Cliquez avec le bouton droit sur ***On-Delivery Email Scanner*** (Analyse des courriers électroniques à la réception) et sélectionnez ***Properties*** (Propriétés). L'écran ***On-Delivery Email Scanner Properties*** (Propriétés de l'analyse des courriers électroniques à la réception) s'affiche.
10. Cliquez sur l'onglet ***Scan items*** (Analyser les éléments) et désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown program threats and trojans*** (Rechercher les menaces et les chevaux de Troie inconnus).
    - ***Find unknown macro threats*** (Rechercher les macrovirus inconnus).
    - ***Find attachments with multiple extensions*** (Rechercher les pièces jointes à plusieurs extensions).

11. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
12. Sélectionnez ***Disabled*** (Désactivé) en regard de l'option ***Sensitivity level*** (Niveau de sensibilité) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
13. Cliquez sur ***OK***.
14. Cliquez avec le bouton droit sur ***On-Delivery Email Scanner*** (Analyse des courriers électroniques à la réception) et sélectionnez ***Disable*** (Désactiver).
15. Cliquez avec le bouton droit sur ***On-Access Scanner*** (Analyse à l'accès) et sélectionnez ***Properties*** (Propriétés). L'écran ***On-Access Scan Properties*** (Propriétés de l'analyse à l'accès) s'affiche.
16. Cliquez sur l'onglet ***General*** (Général) et sélectionnez ***Disabled*** (Désactivé) en regard de l'option ***Sensitivity level*** (Niveau de sensibilité) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
17. Cliquez sur l'onglet ***ScriptScan*** *(Analyse des scripts)* et désélectionnez Enable scanning of scripts (Activer l'analyse des scripts).
18. Cliquez sur l'onglet ***Blocking*** (Blocage) et désélectionnez ***Block the connection when a threat is detected in a shared folder*** (Bloquer la connexion si une menace est détectée dans un dossier partagé).
19. Cliquez sur l'onglet ***Messages*** et désélectionnez ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Afficher la boîte de dialogue des messages lors de la détection d'une menace et afficher le texte spécifié dans le message).
20. Cliquez sur ***All Processes*** (Tous les processus) dans le volet de gauche.
21. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments) et désélectionnez les options suivantes dans Heuristics (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** (Rechercher les programmes indésirables et les chevaux de Troie inconnus).
    - ***Find unknown macro threats*** (Rechercher les macrovirus inconnus).
22. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
23. Dans l'onglet ***Exclusions***, cliquez sur ***Exclusions***. L'écran ***Set Exclusions*** (Définir les exclusions) s'affiche.
24. Cliquez sur ***Add*** (Ajouter). L'écran ***Add Exclusion Item*** (Ajouter l'élément à exclure) s'affiche.
25. Sélectionnez ***By name/location*** (Par nom/emplacement) et cliquez sur ***Browse*** (Rechercher). L'écran ***Browse for Files or Folders*** (Rechercher des fichiers ou des dossiers) s'affiche.
26. Accédez aux dossiers ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** l'un après l'autre et sélectionnez ***OK***.
27. Sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers) dans la fenêtre ***Add Exclusion Item*** (Ajouter l'élément à exclure) et cliquez sur ***OK***.
28. Assurez-vous que les dossiers C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ sont présents dans la fenêtre Set Exclusions (Définir les exclusions).
29. Cliquez sur ***OK***.
30. Cliquez avec le bouton droit de la souris sur ***AutoUpdate*** (Mise à jour automatique) et sélectionnez ***Properties*** (Propriétés). L'écran McAfee AutoUpdate Properties - AutoUpdate (Propriétés de la mise à jour automatique McAfee - Mise à jour automatique) s'affiche.

31. Désélectionnez les options suivantes dans ***Update Options*** (Options de mise à jour) :
    - ***Get new detection engine and datas if available*** (Obtenir le nouveau moteur et les données de détection s'ils sont disponibles).
    - ***Get other available updates (service packs, upgrades, etc.)*** (Obtenir les autres mises à jour disponibles [service packs, mises à niveau, etc.]).
32. Cliquez sur ***Schedule*** (Planifier). L'écran Schedule Settings (Paramètres de planification) s'affiche.
33. Désélectionnez ***Enable*** *(scheduled task runs at specified time)* (Activer [les tâches planifiées sont exécutées à une heure prédéfinie]) dans ***Schedule Settings*** (Paramètres de planification).
34. Cliquez sur ***OK***.
35. Cliquez sur ***OK***.
36. Cliquez avec le bouton droit sur la fenêtre ***VirusScan Console*** (Console VirusScan) et sélectionnez ***New On-Demand Scan Task*** (Nouvelle analyse à la demande).
37. Renommez l'analyse ***Weekly Scheduled Scan*** (Analyse planifiée hebdomadaire). L'écran ***On-Demand Scan Properties - Weekly Scheduled Scan*** (Propriétés de l'analyse à la demande - Analyse planifiée hebdomadaire) s'affiche.
38. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments) et désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Options***.
39. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown programs threats*** (Rechercher les menaces inconnues).
    - ***Find unknown macro threats*** (Rechercher les macrovirus inconnus).
40. Dans l'onglet ***Exclusions***, cliquez sur ***Exclusions***. L'écran ***Set Exclusions*** (Définir les exclusions) s'affiche.
41. Cliquez sur ***Add*** (Ajouter). L'écran ***Add Exclusion Item*** (Ajouter l'élément à exclure) s'affiche.
42. Sélectionnez ***By name/location*** (Par nom/emplacement) et cliquez sur ***Browse*** (Rechercher). L'écran ***Browse for Files or Folders*** (Rechercher des fichiers ou des dossiers) s'affiche.
43. Accédez aux dossiers ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** l'un après l'autre et sélectionnez ***OK***.
44. Sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers) dans la fenêtre ***Add Exclusion Item*** (Ajouter l'élément à exclure) et cliquez sur ***OK***.
45. Assurez-vous que les dossiers ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** sont présents dans la fenêtre ***Set Exclusions*** (Définir les exclusions).
46. Cliquez sur ***OK***.
47. Cliquez sur l'onglet ***Performance*** et sélectionnez ***Disabled*** (Désactivé) en regard de l'option ***Sensitivity level*** (Niveau de sensibilité) dans ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
48. Cliquez sur ***Schedule*** (Planifier). L'écran ***Schedule Settings*** (Paramètres de planification) s'affiche.
49. Cliquez sur l'onglet ***Task*** (Tâche) et sélectionnez ***Enable (scheduled task runs at specified time)*** (Activer [les tâches planifiées sont exécutées à une heure prédéfinie]) dans ***Schedule Settings*** (Paramètres de planification).
50. Cliquez sur l'onglet ***Schedule*** (Planification) et sélectionnez les éléments suivants :

    a. Run task (Exécuter la tâche) : Weekly (toutes les semaines).

    b. Start Time (Heure de début) : 12:00 AM

    c. Every (Fréquence) : 1 Weeks, Sunday (hebdomadaire, le dimanche).

51. Cliquez sur ***OK***.
52. Cliquez sur ***OK***.
53. Cliquez sur ***Tools > Alerts*** (Outils > Alertes) dans la fenêtre ***VirusScan Console*** (Console VirusScan). L'écran Alert Properties (Propriétés des alertes) s'affiche.
54. Désélectionnez les cases ***On-Access Scan*** (Analyse à l'accès), ***On-Demand Scan and scheduled scans*** (Analyse à la demande et analyses planifiées), ***Email Scan*** (Analyse des courriers électroniques) et ***AutoUpdate*** (Mise à jour automatique).
55. Cliquez sur ***Destination***. L'écran ***Alert Manager Client Configuration*** (Configuration côté client du gestionnaire d'alertes) s'affiche.
56. Cochez la case ***Disable alerting*** (Désactiver l'alerte).
57. Cliquez sur ***OK***. L'écran ***Alert Properties*** (Propriétés des alertes) s'affiche.
58. Cliquez sur l'onglet ***Additional Alerting Options*** (Options d'alerte supplémentaires).
59. Sélectionnez l'option ***Suppress all alerts (severities 0 to 4)*** (Supprimer toutes les alertes [gravité de 0 à 4]) sur la liste déroulante ***Severity Filter*** (Filtre de gravité).
60. Cliquez sur l'onglet ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes).
61. Désélectionnez la case ***Access Protection*** (Protection d'accès).
62. Cliquez sur ***OK*** pour fermer la fenêtre ***Alert Properties*** (Propriétés de l'alerte).
63. Fermez la fenêtre ***VirusScan Console*** (Console VirusScan).

McAfee ePolicy Orchestrator

Présentation de l'installation

McAfee ePolicy Orchestrator doit être installé uniquement dans les environnements Mac-Lab/CardioLab en réseau. McAfee ePolicy Orchestrator doit être installé sur un serveur de console de gestion de l'antivirus et McAfee VirusScan Enterprise doit être déployé en tant que client sur le serveur Centricity Cardiology INW et les postes de travail d'acquisition/de consultation. Procédez comme suit pour installer et configurer McAfee ePolicy Orchestrator.

Les instructions présentées ci-dessous pour le mode « Push » et la configuration de McAfee VirusScan Enterprise sont compatibles avec le Patch 3, le Patch 4, le Patch 8, le Patch 9 et le Patch 12.

La mise à jour des listes de virus incombe à l'établissement. Mettez régulièrement à jour les définitions afin de bénéficier de la toute dernière protection sur le système.

Consignes de pré-installation

1. La console de gestion de l'antivirus McAfee est censée avoir été installée conformément aux instructions de McAfee et être en bon état de fonctionnement.
2. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur tous les systèmes clients (acquisition, consultation et serveur INW) pour installer le logiciel antivirus.
3. Désactivez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Désactivation de la connexion de bouclage, page 6.

4. Pour déployer McAfee VirusScan Enterprise 8.8 Patch 9, contactez McAfee afin qu'il installe les certificats d'autorité racine UTN- USERFirst-Object et VeriSign uniquement sur les serveurs INW. Redémarrez le système une fois que les certificats sont installés.

REMARQUE : Si les certificats d'autorité racine UTN-USERSFirst-Object et VeriSign ne sont pas installés, l'installation de McAfee VirusScan Enterprise 8.8 Patch 9 échoue sur les serveurs INW.

5. Pour toute nouvelle installation, ajoutez la version suivante de l'agent dans le référentiel principal de la console McAfee ePolicy Orchestrator : ***- McAfee Agent v5.0.5.658***

Remarque : Pour McAfee ePolicy Orchestrator Version 5.10, ajoutez - **McAfee Agent v5.6.0.207**

6. Pour toute nouvelle installation, ajoutez le package suivant dans le référentiel principal de la console McAfee ePolicy Orchestrator :
   - McAfee VirusScan Enterprise 8.8 Patch 3 : VSE880LMLRP3.ZIP (v8.8.0.0,1128).
   - McAfee VirusScan Enterprise 8.8 Patch 4 : VSE880LMLRP4.ZIP (v8.8.0.0,1247).
   - McAfee VirusScan Enterprise 8.8 Patch 8 : VSE880LMLRP8.ZIP (v8.8.0.1599).
   - McAfee VirusScan Enterprise 8.8 Patch 9 : VSE880MLRP9.ZIP (v8.8.0.1804).
   - McAfee VirusScan Enterprise 8.8 Patch 12 : VSE880LMLRP12.ZIP (v8.8.0.2024)

REMARQUE : Le fichier VSE880LMLRP3.zip contient les packages d'installation du Patch 2 et du Patch 3. Le Patch 2 est destiné aux systèmes d'exploitation Windows 7 et Windows Server 2008 et le Patch 3 est destiné à Windows 8 et Windows Server 2012. Le programme d'installation de McAfee identifie la version de WIndows utilisée et installe le patch correspondant.

7. Pour toute nouvelle installation, ajoutez les extensions suivantes dans le tableau d'extensions de la console McAfee ePolicy Orchestrator :
   - McAfee VirusScan Enterprise 8.8 Patch 3 : VIRUSSCAN8800 v8.8.0.0,348 et VIRUSSCANREPORTS v1.2.0.0,228
   - McAfee VirusScan Enterprise 8.8 Patch 4 : VIRUSSCAN8800 v8.8.0.0,368 et VIRUSSCANREPORTS v1.2.0.0,236
   - McAfee VirusScan Enterprise 8.8 Patch 8 : VIRUSSCAN8800 v8.8.0.0,511 et VIRUSSCANREPORTS v1.2.0.0,311
   - McAfee VirusScan Enterprise 8.8 Patch 9 : VIRUSSCAN8800 v8.8.0.548 et VIRUSSCANREPORTS v1.2.0.346
   - McAfee VirusScan Enterprise 8.8 Patch 12 : VIRUSSCAN8800 v8.8.0.0,687 et VIRUSSCANREPORTS v1.2.0.0,427

REMARQUE : Les fichiers VIRUSSCAN8800(348).zip et VIRUSSCANREPORTS120(228).zip se trouvent dans le package McAfee VirusScan Enterprise 8.8 Patch 3.

Les fichiers VIRUSSCAN8800(368).zip et VIRUSSCANREPORTS120(236).zip se trouvent dans le package McAfee VirusScan Enterprise 8.8 Patch 4.

Les fichiers VIRUSSCAN8800(511).zip et VIRUSSCANREPORTS120(311).zip se trouvent dans le package McAfee VirusScan Enterprise 8.8 Patch 8.

Les fichiers VIRUSSCAN8800(548).zip et VIRUSSCANREPORTS120(346).zip se trouvent dans le package McAfee VirusScan Enterprise 8.8 Patch 9.

Les fichiers VIRUSSCAN8800(687).zip et VIRUSSCANREPORTS120(426).zip se trouvent dans le package McAfee VirusScan Enterprise 8.8 Patch 12.

McAfee ePolicy Orchestrator 5.0 ou 5.3.2- Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée)

1. Selon la version logicielle, sélectionnez ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.0.0) ou ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.3.2) pour vous connecter à la console ePolicy Orchestrator.

REMARQUE : Cliquez sur ***Continue with this website*** (Rester sur ce site Internet) si le message ***Security Alert*** (Alerte de sécurité) s'affiche.

2. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
3. Sélectionnez ***Menu > System > System Tree*** (Menu > Système > Arborescence du système). La fenêtre System Tree (Arborescence du système) s'ouvre.
4. Cliquez sur ***My Organization*** (Mon organisation) et, tout en restant sur ***My Organization*** (Mon organisation), cliquez sur ***System Tree Actions > New Systems*** (Actions liées à l'arborescence du système > Nouveaux systèmes) dans l'angle inférieur gauche de l'écran.
5. Sélectionnez ***Push agents and add systems to the current group (My Organization)*** (Communiquer les agents en mode « Push » et ajouter des systèmes au groupe actuel [Mon organisation]) et cliquez sur ***Browse*** (Rechercher) dans les systèmes Target (Cibles).
6. Entrez le nom d'utilisateur et le mot de passe du **domain/local administrator** (administrateur de domaine/local) et cliquez sur ***OK***.
7. Sélectionnez le domaine ***INW*** dans la liste déroulante ***Domain*** (Domaines).
8. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) connectées au domaine et cliquez sur ***OK***.

REMARQUE : Si le nom du domaine ne figure pas dans la liste déroulante ***Domain*** (Domaines), procédez comme indiqué ci-dessous :

- Dans les fenêtres ***Browse for Systems*** (Rechercher des systèmes), cliquez sur ***Cancel*** (Annuler).
- Dans la fenêtre ***New Systems*** (Nouveaux systèmes), entrez manuellement le nom du système des machines clientes (acquisition, consultation et serveur INW) dans le champ ***Target systems*** (Systèmes cibles) et procédez aux manipulations suivantes.

9. Réglez ***Agent Version*** (Version de l'agent) sur ***McAfee Agent for Windows 4.8.0 (Current)*** (McAfee Agent pour Windows 4.8.0 (actuel)) ou ***McAfee Agent for Windows 5.0.4 (Current)*** (McAfee Agent pour Windows 5.0.4 (actuel)). Entrez le nom d'utilisateur et le mot de passe du **Domain administrator** (Administrateur du domaine) et cliquez sur ***OK***.
10. Sur les machines clientes (acquisition, consultation et serveur INW), confirmez que les répertoires ont été correctement créés, selon la version du patch :

- Pour les patchs 3 et 4, vérifiez que le répertoire ***C:\Program Files\McAfee\Common Framework*** est présent et que McAfee Agent est installé dans le même répertoire.

REMARQUE : Pour le Serveur INW, vérifiez que le répertoire ***C:\Program Files (x86)\McAfee\Common Framework*** est présent et que McAfee Agent est installé dans le même répertoire.

- Pour le patch 8, vérifiez que le répertoire ***C:\Program Files\McAfee\Agent*** est présent et que McAfee Agent est installé dans le même répertoire.

REMARQUE : Pour le serveur INW, assurez-vous que le répertoire ***C:\Program Files (x86)\McAfee\Common Framework*** est présent.

11. Redémarrez les machines clientes (acquisition, consultation et serveur INW) et connectez-vous en tant que **Domain administrator** (Administrateur du domaine) ou membre de ce groupe.
12. Selon la version logicielle, cliquez sur ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.0.0) ou ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.3.2).
13. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
14. Cliquez sur ***Menu > Systems > System Tree*** (Menu > Systèmes > Arborescence du système).
15. Cliquez sur ***My Organization*** (Mon organisation) et, tout en restant sur ***My Organization*** (Mon organisation), cliquez sur l'onglet ***Assigned Client Tasks*** (Tâches client affectées).
16. Cliquez sur le bouton ***Actions > New Client Task Assignment*** (Actions > Nouvelle affectation de tâche client) qui se trouve au bas de l'écran. L'écran Client Task Assignment Builder (Création d'affectations de tâches client) s'affiche.
17. Sélectionnez les éléments suivants :

    a. **Product** (Produit) : McAfee Agent

    b. **Task Type** (Type de tâche) : Product Deployment (Déploiement produit)

    c. **Task name** (Nom de la tâche) : Create New Task (Créer une tâche)
18. Sur l'écran ***Client Task Catalog: New Task- McAfee Agent: Product Deployment*** (Catalogue des tâches client : Nouvelle tâche - McAfee Agent : Déploiement du produit), renseignez les champs suivants :

    a. **Task Name** (Nom de la tâche) : Entrez le nom de la tâche

    b. **Target platforms** (Plate-formes cibles) : Windows

    c. **Products and components** (Produits et composants) : Version de VirusScan Enterprise compatible avec v6.9.6

    d. **Options :** exécuter à chaque application de stratégie (Windows uniquement) si ***Options*** est disponible
19. Cliquez sur ***Save*** (Enregistrer).
20. Sur l'écran ***1 Select Task*** (Sélectionner la tâche), sélectionnez les éléments suivants :

    a. **Product** (Produit) : McAfee Agent

    b. **Task Type** (Type de tâche) : Product Deployment (Déploiement produit)

    c. **Task Name** (Nom de la tâche) : Nom de tâche nouvellement créée
21. Cliquez sur ***Next*** (Suivant). L'écran 2 Schedule (Planification) s'affiche.
22. Sélectionnez ***Run immediately*** (Exécuter immédiatement) dans la liste déroulante ***Schedule type*** (Type de planification).
23. Cliquez sur ***Next*** (Suivant). L'écran 3 Summary (Résumé) s'affiche.
24. Cliquez sur ***Save*** (Enregistrer). L'écran ***System Tree*** (Arborescence du système) s'affiche.
25. Cliquez sur l'onglet ***Systems*** (Systèmes), puis sélectionnez toutes les machines clientes (acquisition, consultation et serveur INW) connectées au domaine.
26. Cliquez sur ***Wake up Agents*** (Réveiller les agents) au bas de la fenêtre.
27. Conservez les paramètres par défaut et cliquez sur ***OK***.

28. Attendez que l'icône McAfee s'affiche dans la barre des tâches, puis redémarrez toutes les machines clientes (acquisition, consultation et serveur INW) et connectez-vous en tant qu'**Administrator** (Administrateur) ou que membre de ce groupe sur toutes les machines clientes.
29. Cliquez sur le lien ***Log Off*** (Déconnexion) pour arrêter la console McAfee ePolicy Orchestrator.

McAfee ePolicy Orchestrator 5.9.0 et 5.10.0 - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée)

1. Sélectionnez ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.9.0) pour vous connecter à la console ePolicy Orchestrator.

   REMARQUE :
   - Cliquez sur ***Continue with this website*** (Rester sur ce site Internet) si le message ***Security Alert*** (Alerte de sécurité) s'affiche.
   - Pour la version 5.10.0, *Launch McAfee ePolicy Orchestrator 5.10.0 Console* (Lancer la console McAfee ePolicy Orchestrator 5.10.0).

2. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
3. Sélectionnez ***Menu > System > System Tree*** (Menu > Système > Arborescence du système). La fenêtre ***System Tree*** (Arborescence du système) s'ouvre.
4. Cliquez sur ***My Organization*** (Mon organisation) et, tout en restant sur ***My Organization*** (Mon organisation), cliquez sur ***New Systems*** (Nouveaux systèmes) en haut de l'écran.
5. Sélectionnez ***Push agents and add systems to the current group (My Organization)*** (Communiquer les agents en mode « Push » et ajouter des systèmes au groupe actuel [Mon organisation]) et cliquez sur ***Browse*** (Rechercher) dans les systèmes Target (Cibles).
6. Entrez le nom d'utilisateur et le mot de passe du **domain/local administrator** (administrateur de domaine/local) et cliquez sur ***OK***.
7. Sélectionnez le domaine ***INW*** dans la liste déroulante ***Domain*** (Domaines).
8. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) connectées au domaine et cliquez sur ***OK***.

REMARQUE : Si le nom du domaine ne figure pas dans la liste déroulante ***Domain*** (Domaines), procédez comme indiqué ci-dessous :

- Dans les fenêtres ***Browse for Systems*** (Rechercher des systèmes), cliquez sur ***Cancel*** (Annuler).
- Dans la fenêtre ***New Systems*** (Nouveaux systèmes), entrez manuellement le nom du système des machines clientes en les séparant par une virgule (acquisition, consultation et serveur INW) dans le champ ***Target systems*** (Systèmes cibles) et procédez aux manipulations suivantes.

9. Sélectionnez la ***Agent Version*** (Version de l'agent) ***McAfee Agent for Windows 5.0.5 (Current)*** (Version actuelle). Entrez le nom d'utilisateur et le mot de passe du **Domain administrator** (Administrateur du domaine) et cliquez sur ***OK***.
10. Dans les machines clientes (acquisition, consultation et serveur INW), confirmez que les répertoires sous ***C:\Program Files\McAfee\Agent*** ont été créés correctement.
11. Redémarrez les machines clientes (acquisition, consultation et serveur INW) et connectez-vous en tant que **Domain administrator** (Administrateur du domaine) ou membre de ce groupe.

12. Sélectionnez ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.9.0) pour vous connecter à la console ePolicy Orchestrator.
    REMARQUE : Pour la version 5.10.0, ***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** (Lancer la console McAfee ePolicy Orchestrator 5.10.0).
13. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
14. Cliquez sur ***Menu > Systems > System Tree*** (Menu > Systèmes > Arborescence du système).
15. Cliquez sur ***My Organization*** (Mon organisation) et, tout en restant sur ***My Organization*** (Mon organisation), cliquez sur l'onglet ***Assigned Client Tasks*** (Tâches client affectées).
16. Cliquez sur le bouton ***Actions > New Client Task Assignment*** (Actions > Nouvelle affectation de tâche client) qui se trouve au bas de l'écran. L'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client) s'affiche.
17. Sélectionnez les éléments suivants :
    a. **Product** (Produit) : McAfee Agent
    b. **Task Type** (Type de tâche) : Product Deployment (Déploiement produit)
18. Cliquez sur ***Task Actions > Create New Task*** (Actions de tâche > Créer une tâche). L'écran ***Create New Task*** (Créer une tâche) s'affiche.
19. Sur l'écran ***Create New Task*** (Créer une tâche), renseignez les champs comme suit :
    a. **Task Name** (Nom de la tâche) : Entrez le nom de la tâche
    b. **Target platforms** (Plate-formes cibles) : Windows (décochez toutes les autres options)
    c. **Products and components** (Produits et composants) : VirusScan Enterprise 8.8.0.1804
    REMARQUE : Pour la version 5.10.0, Mise à jour 2 **Produits et composants :** VirusScan Enterprise 8.8.0.0,2024
20. Cliquez sur ***Save*** (Enregistrer). L'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client) s'affiche.
21. Sur l'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client), sélectionnez les éléments suivants :
    a. **Product** (Produit) : McAfee Agent
    b. **Task Type** (Type de tâche) : Product Deployment (Déploiement produit)
    c. **Task Name** (Nom de la tâche) : Nom de tâche nouvellement créée
    d. **Schedule Type** (Type de planification) : Run immediately (Exécuter immédiatement)
22. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Client Tasks*** (Tâches client affectées) s'affiche.
23. Cliquez sur l'onglet ***Systems*** (Systèmes), puis sélectionnez toutes les machines clientes (acquisition, consultation et serveur INW) connectées au domaine.
24. Cliquez sur ***Wake up Agents*** (Réveiller les agents) au bas de la fenêtre.
25. Conservez les paramètres par défaut et cliquez sur ***OK***.
26. Attendez que l'icône McAfee s'affiche dans la barre des tâches, puis redémarrez toutes les machines clientes (acquisition, consultation et serveur INW) et connectez-vous en tant qu'**Administrator** (Administrateur) ou que membre de ce groupe sur toutes les machines clientes.
27. Cliquez sur le lien ***Log Off*** (Déconnexion) pour arrêter la console McAfee ePolicy Orchestrator.

Configuration de la console McAfee ePolicy Orchestrator Server 5.0 et 5.3.2

1. Selon la version logicielle, cliquez sur ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.0.0) ou ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.3.2).
2. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
3. Cliquez sur ***Menu > Systems > System Tree*** (Menu > Systèmes > Arborescence du système).
4. Cliquez sur ***My Organization*** (Mon organisation) et, tout en restant sur My Organization (Mon organisation), cliquez sur l'onglet ***Assigned Client Tasks*** (Tâches client affectées).
5. Cliquez sur le bouton ***Actions > New Client Task Assignment*** (Nouvelle affectation de tâche client) au bas de l'écran. L'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client) s'affiche.
6. Sélectionnez les éléments suivants :

   a. ***Product*** (Produit) : VirusScan Enterprise 8.8.0.0

   b. ***Task Type*** (Type de tâche) : On Demand Scan (Analyse à la demande)

   c. ***Task name*** (Nom de la tâche) : Create New Task (Créer une tâche)
7. Sur l'écran ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan*** (Catalogue des tâches client : Nouvelle tâche - VirusScan Enterprise 8.8.0 : Analyse à la demande), renseignez les champs suivants :

   a. ***Task Name*** (Nom de la tâche) : Weekly Scheduled Scan (Analyse planifiée hebdomadaire)

   b. ***Description*** : Weekly Scheduled Scan (Analyse planifiée hebdomadaire)
8. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
9. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Options***.
10. Désélectionnez les options suivantes dans Heuristics (Heuristique) :
    - ***Find unknown program threats*** *(Rechercher les menaces inconnues).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
11. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
12. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
13. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez Also exclude subfolders (Exclure également les sous-dossiers). Cliquez sur ***OK***.
14. Cliquez sur l'onglet ***Performance***. L'écran ***Performance*** s'affiche.
15. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
16. Cliquez sur ***Save*** (Enregistrer).

17. Sur l'écran ***1 Select Task*** (Sélectionner la tâche), sélectionnez les éléments suivants :
    - ***Product*** *(Produit) :* VirusScan Enterprise 8.8.0.0
    - ***Task Type*** *(Type de tâche)* ***:*** On Demand Scan (Analyse à la demande)
    - ***Task Name*** *(Nom de la tâche)* ***:*** Weekly Scheduled Scan (Analyse planifiée hebdomadaire)
18. Cliquez sur ***Next*** (Suivant). L'écran ***2 Schedule*** (Planification) s'affiche.
19. Sélectionnez ***Weekly*** (Hebdomadaire) dans la liste déroulante ***Scheduled type*** (Type planifié) et sélectionnez ***Sunday*** (Dimanche).
20. Réglez ***Start time*** (Heure de début) sur ***12:00 AM*** (12h00) et sélectionnez ***Run Once at that time*** (Exécuter une fois à cette heure).
21. Cliquez sur ***Next*** (Suivant). L'écran ***3 Summary*** (Résumé) s'affiche.
22. Cliquez sur ***Save*** (Enregistrer). L'écran ***System Tree*** (Arborescence du système) s'affiche.
23. Cliquez sur l'onglet ***Assigned Policies*** (Stratégies affectées). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
24. Dans la liste déroulante ***Product*** *(Produit)*, sélectionnez ***VirusScan Enterprise 8.8.0***.
25. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* pour ***On-Access General Policies*** *(Stratégies générales à l'accès)*. L'écran ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies générales à l'accès > Ma stratégie par défaut) s'affiche.
26. Sélectionnez ***Workstation*** (Poste de travail) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***General*** (Général). L'écran ***General*** (Général) s'affiche.
27. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
28. Cliquez sur l'onglet ***ScriptScan*** (Analyse des scripts). L'écran ***Script Scan*** (Analyse des scripts) s'affiche.
29. Désélectionnez ***Enable scanning of scripts*** (Activer l'analyse des scripts).
30. Cliquez sur l'onglet ***Blocking*** (Blocage). L'écran ***Blocking*** (Blocage) s'ouvre.
31. Désélectionnez ***Block the connection when a threatened file is detected in a shared folder*** (Bloquer la connexion si une menace est détectée dans un dossier partagé).
32. Cliquez sur l'onglet ***Messages***. L'écran ***Messages*** s'affiche.
33. Désélectionnez la case ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Afficher la boîte de dialogue des messages lors de la détection d'une menace et afficher le texte spécifié dans le message).
34. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***General*** (Général). L'écran ***General*** (Général) s'affiche.
35. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
36. Cliquez sur l'onglet ***ScriptScan*** (Analyse des scripts). L'écran ***Script Scan*** (Analyse des scripts) s'affiche.
37. Vérifiez que ***Enable scanning of scripts*** (Activer l'analyse des scripts) est désélectionné.
38. Cliquez sur l'onglet ***Blocking*** (Blocage). L'écran ***Blocking*** (Blocage) s'ouvre.
39. Désélectionnez ***Block the connection when a threatened file is detected in a shared folder*** (Bloquer la connexion si une menace est détectée dans un dossier partagé).
40. Cliquez sur l'onglet ***Messages***. L'écran ***Messages*** s'affiche.

41. Désélectionnez la case ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Afficher la boîte de dialogue des messages lors de la détection d'une menace et afficher le texte spécifié dans le message).
42. Cliquez sur ***Save*** (Enregistrer).
43. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* en regard de l'option ***ON-Access Default Processes Policies*** *(Stratégies des processus par défaut à l'accès)*. L'écran ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies des processus par défaut à l'accès > Ma stratégie par défaut) s'affiche.
44. Sélectionnez ***Workstation (****Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour)*.
45. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
46. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
47. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
48. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
49. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
50. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
51. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
52. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
53. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
54. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
55. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
56. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
57. Cliquez sur ***Save*** (Enregistrer).
58. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***On-Access Low-Risk Processes Policies*** (Stratégies des processus à faible risque à l'accès). L'écran ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies des processus à faible risque à l'accès > Ma stratégie par défaut) s'ouvre.

59. Sélectionnez ***Workstation (****Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour)*.
60. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
61. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
62. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
63. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
64. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
65. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
66. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
67. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
68. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
69. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
70. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
71. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
72. Cliquez sur ***Save*** (Enregistrer).
73. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***On-Access High-Risk Processes Policies*** (Stratégies des processus à risque élevé à l'accès). L'écran ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies des processus à risque élevé à l'accès > Ma stratégie par défaut) s'affiche.
74. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour)*.
75. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
76. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*

77. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
78. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
79. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
80. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
81. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
82. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
83. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
84. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
85. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
86. Sélectionnez By pattern (Par type) et entrez les dossiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
87. Cliquez sur ***Save*** (Enregistrer).
88. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***On Delivery Email Scan Policies*** (Stratégies d'analyse des courriers électroniques à la réception). L'écran ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies d'analyse des courriers électroniques à la réception > Ma stratégie par défaut) s'affiche.
89. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
90. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
91. Désélectionnez les options suivantes dans ***Heuristics*** *(Heuristique)*.
    - ***Find unknown program threats and trojans*** *(Rechercher les menaces et les chevaux de Troie inconnus)**.***
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
    - ***Find attachments with multiple extensions*** *(Rechercher les pièces jointes à plusieurs extensions).*
92. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
93. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
94. Désélectionnez ***Enable on-delivery email scanning*** (Activer l'analyse des courriers électroniques à la réception) dans ***Scanning of email*** (Analyse des courriers électroniques).
95. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.

96. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
97. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown program threats and trojans*** *(Rechercher les menaces et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
    - ***Find attachments with multiple extensions*** *(Rechercher les pièces jointes à plusieurs extensions).*
98. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
99. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
100. Désélectionnez ***Enable on-delivery email scanning*** (Activer l'analyse des courriers électroniques à la réception) dans ***Scanning of email*** (Analyse des courriers électroniques).
101. Cliquez sur ***Save*** (Enregistrer).
102. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***General Options Policies*** (Stratégies concernant les options générales). L'écran ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies concernant les options générales > Ma stratégie par défaut) s'affiche.
103. Sélectionnez ***Workstation*** (Poste de travail) dans la liste déroulante ***Settings for*** (Paramètres de).
104. Cliquez sur l'onglet ***Display Options*** (Options d'affichage). L'écran ***Display Options*** (Options d'affichage) s'ouvre.
105. Sélectionnez les éléments suivants dans ***Console options*** (Options de la console) :
    - ***Display managed tasks in the client console*** *(Afficher les tâches de gestion dans la console du client).*
    - ***Disable default AutoUpdate task schedule*** *(Désactiver la planification de la tâche de mise à jour automatique par défaut).*
106. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de).
107. Cliquez sur l'onglet ***Display Options*** (Options d'affichage). L'écran ***Display Options*** (Options d'affichage) s'ouvre.
108. Sélectionnez les éléments suivants dans ***Console options*** (Options de la console) :
    - ***Display managed tasks in the client console*** *(Afficher les tâches de gestion dans la console du client).*
    - ***Disable default AutoUpdate task schedule*** *(Désactiver la planification de la tâche de mise à jour automatique par défaut).*
109. Cliquez sur ***Save*** (Enregistrer).
110. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* pour ***Alert Policies*** *(Stratégies d'alerte)*. L'écran ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies d'alerte > Ma stratégie par défaut) s'affiche.
111. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
112. Cliquez sur l'onglet ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes). L'écran ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes) s'affiche.

113. Désélectionnez ***On-Access Scan*** (Analyse à l'accès), ***On-Demand Scan and scheduled scans*** (Analyses à la demande et analyses planifiées), ***Email Scan*** (Analyse des courriers électroniques) et ***AutoUpdate*** (Mise à jour automatique) dans ***Components that generate alerts*** (Composants générant des alertes).
114. Sélectionnez ***Disable alerting*** (Désactiver les alertes) dans les options ***Alert Manager*** (Gestionnaire d'alertes).
115. Désélectionnez ***Access Protection*** (Protection d'accès) dans ***Components that generate alerts*** (Composants générant des alertes).
116. Cliquez sur ***Additional Alerting Options*** (Options d'alerte supplémentaires). L'écran ***Additional Alerting Options*** (Options d'alerte supplémentaires) s'affiche.
117. Dans le menu déroulant ***Severity Filters*** *(Filtre de gravité)*, sélectionnez ***Suppress all alerts*** *(severities 0 to 4) (Supprimer toutes les alertes (gravités de 0 à 4)***)**.
118. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)* et cliquez sur l'onglet ***Alert Manager Alerts*** *(Alertes du gestionnaire d'alertes)*. L'écran ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes) s'affiche.
119. Désélectionnez ***On-Access Scan*** (Analyse à l'accès), ***On-Demand Scan and scheduled scans*** (Analyses à la demande et analyses planifiées), ***Email Scan*** (Analyse des courriers électroniques) et ***AutoUpdate*** (Mise à jour automatique) dans ***Components that generate alerts*** (Composants générant des alertes).
120. Cochez ***Disable alerting*** (Désactiver l'alerte) dans les options ***Alert Manager*** (Gestionnaire d'alertes).
121. Désélectionnez ***Access Protection*** (Protection d'accès) dans ***Components that generate alerts*** (Composants générant des alertes).
122. Cliquez sur ***Additional Alerting Options*** (Options d'alerte supplémentaires). L'écran Additional Alerting Options (Options d'alerte supplémentaires) s'affiche.
123. Dans le menu déroulant ***Severity Filters*** *(Filtre de gravité)*, sélectionnez ***Suppress all alerts*** *(severities 0 to 4) (Supprimer toutes les alertes (gravités de 0 à 4))*.
124. Cliquez sur ***Save*** (Enregistrer).
125. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***Access Protection Policies*** (Stratégies de protection d'accès). L'écran ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies de protection d'accès > Ma stratégie par défaut) s'affiche.
126. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
127. Cliquez sur l'onglet ***Access Protection*** (Protection d'accès). L'écran ***Access Protection*** (Protection d'accès) s'affiche.
128. Désélectionnez les options suivantes dans ***Access protection settings*** (Paramètres de protection d'accès) :
    - ***Enable access protection*** *(Activer la protection d'accès).*
    - ***Prevent McAfee services from being stopped*** *(Empêcher l'arrêt des services McAfee).*
129. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
130. Cliquez sur l'onglet ***Access Protection*** (Protection d'accès). L'écran ***Access Protection*** (Protection d'accès) s'affiche.
131. Désélectionnez les options suivantes dans ***Access protection settings*** (Paramètres de protection d'accès) :
    - ***Enable access protection*** *(Activer la protection d'accès).*
    - ***Prevent McAfee services from being stopped*** *(Empêcher l'arrêt des services McAfee).*

132. Cliquez sur ***Save*** (Enregistrer).
133. Sélectionnez ***My Default*** (Ma stratégie par défaut) en regard de l'option ***Buffer Overflow Protection Policies*** (Stratégies de protection contre les dépassements de tampon). L'écran ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies de protection contre les dépassements de tampon > Ma stratégie par défaut) s'affiche.
134. Sélectionnez ***Workstation (****Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour)*.
135. Cliquez sur l'onglet ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon). L'écran ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon) s'affiche.
136. Désélectionnez ***Show the message dialog box when a buffer overflow is detected*** (Afficher la boîte de dialogue des messages lors de la détection d'un dépassement de tampon) dans ***Client system warning*** (Alerte système client).
137. Désélectionnez ***Enable buffer overflow protection*** (Activer la protection contre les dépassements de tampon) dans ***Buffer overflow settings*** (Paramètres de dépassement de tampon).
138. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
139. Cliquez sur l'onglet ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon). L'écran ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon) s'affiche.
140. Désélectionnez ***Show the message dialog box when a buffer overflow is detected*** (Afficher la boîte de dialogue des messages lors de la détection d'un dépassement de tampon) dans ***Client system warning*** (Alerte système client).
141. Désélectionnez ***Enable buffer overflow protection*** (Activer la protection contre les dépassements de tampon) dans ***Buffer overflow settings*** (Paramètres de dépassement de tampon).
142. Cliquez sur ***Save*** (Enregistrer).
143. Dans le menu déroulant ***Product*** *(Produit)*, sélectionnez ***McAfee Agent***. La fenêtre ***Policies*** (Stratégies) correspondant à McAfee Agent s'ouvre.
144. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* en regard de l'option ***Repository*** *(Référentiel)*. L'écran ***McAfee Agent > Repository > My Default*** (McAfee Agent > Référentiel > Ma stratégie par défaut) s'affiche.
145. Cliquez sur l'onglet ***Proxy***. L'écran ***Proxy*** s'affiche.
146. Sélectionnez ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Utiliser les paramètres Internet Explorer [pour Windows]/les paramètres de préférences du système [pour Mac OSX]) dans ***Proxy settings*** (Paramètres Proxy).
147. Cliquez sur ***Save*** (Enregistrer).
148. Cliquez sur l'onglet ***Settings*** (Paramètres).
149. Sélectionnez tous les systèmes du client (postes de travail d'acquisition, de consultation et serveur Centricity Cardiology INW) sur lesquels les stratégies configurées doivent être déployées.
150. Sélectionnez ***Wake Up Agents*** (Réveiller les agents). L'écran ***Wake Up Agent*** (Réveiller l'agent) s'affiche.
151. Cliquez sur ***OK***.
152. Déconnectez-vous d'ePolicy Orchestrator.

Configuration de la console McAfee ePolicy Orchestrator Server 5.9.0 et 5.10.0

1. Selon la version du logiciel, cliquez sur ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Démarrer > Tous les programmes > McAfee > ePolicy Orchestrator > Lancer la console McAfee ePolicy Orchestrator 5.9.0).
   Remarque : Pour la version 5.10.0, ***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** (Lancer la console McAfee ePolicy Orchestrator 5.10.0)
2. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
3. Cliquez sur ***Menu > Systems > System Tree*** (Menu > Systèmes > Arborescence du système).
4. Cliquez sur ***My Organization*** (Mon organisation) et, tout en restant sur My Organization (Mon organisation), cliquez sur l'onglet ***Assigned Client Tasks*** (Tâches client affectées).
5. Cliquez sur le bouton ***Actions > New Client Task Assignment*** (Nouvelle affectation de tâche client) au bas de l'écran. L'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client) s'affiche.
6. Sélectionnez les éléments suivants :
   a. ***Product*** (Produit) : VirusScan Enterprise 8.8.0.0
   b. ***Task Type*** (Type de tâche) : On Demand Scan (Analyse à la demande)
7. Cliquez sur ***Create New Task*** (Créer une tâche) sous ***Task Actions*** (Actions de tâche). L'écran ***Create New Task*** (Créer une tâche) apparaît.
8. Sur l'écran ***Create New Task*** (Créer une tâche), renseignez les champs comme suit :
   a. ***Task Name*** (Nom de la tâche) : Weekly Scheduled Scan (Analyse planifiée hebdomadaire)
   b. ***Description*** : Weekly Scheduled Scan (Analyse planifiée hebdomadaire)
9. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
10. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Options***.
11. Désélectionnez les options suivantes dans Heuristics (Heuristique) :
    - ***Find unknown program threats*** *(Rechercher les menaces inconnues).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
12. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
13. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
14. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez Also exclude subfolders (Exclure également les sous-dossiers). Cliquez sur ***OK***.
15. Cliquez sur l'onglet ***Performance***. L'écran ***Performance*** s'affiche.
16. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
17. Cliquez sur ***Save*** (Enregistrer). L'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client) s'affiche.

18. Sur l'écran ***Client Task Assignment Builder*** (Création d'affectations de tâches client), sélectionnez les éléments suivants :
    - ***Product*** *(Produit)* **:** VirusScan Enterprise 8.8.0.0
    - ***Task Type*** *(Type de tâche)* **:** On Demand Scan (Analyse à la demande)
    - ***Task Name*** *(Nom de la tâche)* **:** Weekly Scheduled Scan (Analyse planifiée hebdomadaire)
19. Sélectionnez ***Weekly*** (Hebdomadaire) dans la liste déroulante ***Scheduled type*** (Type planifié) et sélectionnez ***Sunday*** (Dimanche).
20. Réglez ***Start time*** (Heure de début) sur ***12:00 AM*** et sélectionnez ***Run Once at that time*** (Exécuter une fois à cette heure).
21. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Client Tasks*** (Tâches client affectées) s'affiche.
22. Cliquez sur l'onglet ***Assigned Policies*** (Stratégies affectées). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
23. Dans la liste déroulante ***Product*** *(Produit)*, sélectionnez ***VirusScan Enterprise 8.8.0***.
24. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* pour ***On-Access General Policies*** *(Stratégies générales à l'accès)*. L'écran ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies générales à l'accès > Ma stratégie par défaut) s'affiche.
25. Sélectionnez ***Workstation*** (Poste de travail) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***General*** (Général). L'écran ***General*** (Général) s'affiche.
26. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
27. Cliquez sur l'onglet ***ScriptScan*** (Analyse des scripts). L'écran ***Script Scan*** (Analyse des scripts) s'affiche.
28. Désélectionnez ***Enable scanning of scripts*** (Activer l'analyse des scripts).
29. Cliquez sur l'onglet ***Blocking*** (Blocage). L'écran ***Blocking*** (Blocage) s'ouvre.
30. Désélectionnez ***Block the connection when a threatened file is detected in a shared folder*** (Bloquer la connexion si une menace est détectée dans un dossier partagé).
31. Cliquez sur l'onglet ***Messages***. L'écran ***Messages*** s'affiche.
32. Désélectionnez la case ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Afficher la boîte de dialogue des messages lors de la détection d'une menace et afficher le texte spécifié dans le message).
33. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***General*** (Général). L'écran ***General*** (Général) s'affiche.
34. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
35. Cliquez sur l'onglet ***ScriptScan*** (Analyse des scripts). L'écran ***Script Scan*** (Analyse des scripts) s'affiche.
36. Vérifiez que ***Enable scanning of scripts*** (Activer l'analyse des scripts) est désélectionné.
37. Cliquez sur l'onglet ***Blocking*** (Blocage). L'écran ***Blocking*** (Blocage) s'ouvre.
38. Désélectionnez ***Block the connection when a threatened file is detected in a shared folder*** (Bloquer la connexion si une menace est détectée dans un dossier partagé).
39. Cliquez sur l'onglet ***Messages***. L'écran ***Messages*** s'affiche.

40. Désélectionnez la case ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Afficher la boîte de dialogue des messages lors de la détection d'une menace et afficher le texte spécifié dans le message).
41. Cliquez sur ***Save*** (Enregistrer). L'écran Assigned Policies (Stratégies affectées) s'affiche.
42. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* en regard de l'option ***ON-Access Default Processes Policies*** *(Stratégies des processus par défaut à l'accès)*. L'écran ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies des processus par défaut à l'accès > Ma stratégie par défaut) s'affiche.
43. Sélectionnez ***Workstation (****Poste de travail)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
44. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
45. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
46. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
47. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
48. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
49. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
50. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
51. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
52. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
53. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
54. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
55. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
56. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
57. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***On-Access Low-Risk Processes Policies*** (Stratégies des processus à faible risque à l'accès). L'écran ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies des processus à faible risque à l'accès > Ma stratégie par défaut) s'ouvre.

58. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
59. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
60. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
61. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
62. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
63. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
64. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
65. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
66. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
67. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
68. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
69. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
70. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
71. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
72. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***On-Access High-Risk Processes Policies*** (Stratégies des processus à risque élevé à l'accès). L'écran ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies des processus à risque élevé à l'accès > Ma stratégie par défaut) s'affiche.
73. Sélectionnez ***Workstation (****Poste de travail)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
74. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
75. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*

76. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
77. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
78. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
79. Sélectionnez ***By pattern*** (Par type) et entrez les dossiers **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
80. Sélectionnez ***Server*** (Serveur) dans la liste déroulante ***Settings for*** (Paramètres de) et cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
81. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown unwanted programs and trojans*** *(Rechercher les programmes indésirables et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
82. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
83. Cliquez sur l'onglet ***Exclusions***. L'écran ***Exclusions*** s'affiche.
84. Cliquez sur ***Add*** (Ajouter). L'écran ***Add/Edit Exclusion Item*** (Ajouter/modifier un élément à exclure) s'affiche.
85. Sélectionnez By pattern (Par type) et entrez les dossiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** un par un et sélectionnez ***Also exclude subfolders*** (Exclure également les sous-dossiers). Cliquez sur ***OK***.
86. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
87. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***On Delivery Email Scan Policies*** (Stratégies d'analyse des courriers électroniques à la réception). L'écran ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies d'analyse des courriers électroniques à la réception > Ma stratégie par défaut) s'affiche.
88. Sélectionnez ***Workstation (****Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour)*.
89. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
90. Désélectionnez les options suivantes dans ***Heuristics*** *(Heuristique)*.
    - ***Find unknown program threats and trojans*** *(Rechercher les menaces et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
    - ***Find attachments with multiple extensions*** *(Rechercher les pièces jointes à plusieurs extensions).*
91. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
92. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
93. Désélectionnez ***Enable on-delivery email scanning*** (Activer l'analyse des courriers électroniques à la réception) dans ***Scanning of email*** (Analyse des courriers électroniques).
94. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.

95. Cliquez sur l'onglet ***Scan Items*** (Analyser les éléments). L'écran ***Scan Items*** (Analyser les éléments) s'affiche.
96. Désélectionnez les options suivantes dans ***Heuristics*** (Heuristique) :
    - ***Find unknown program threats and trojans*** *(Rechercher les menaces et les chevaux de Troie inconnus).*
    - ***Find unknown macro threats*** *(Rechercher les macrovirus inconnus).*
    - ***Find attachments with multiple extensions*** *(Rechercher les pièces jointes à plusieurs extensions).*
97. Désélectionnez ***Detect unwanted programs*** (Détecter les programmes indésirables) dans ***Unwanted programs detection*** (Détection des programmes indésirables).
98. Sélectionnez ***Disabled*** (Désactivé) dans ***Artemis*** *(Heuristic network check for suspicious files)* (Artemis [Recherche heuristique de fichiers suspects sur le réseau]).
99. Désélectionnez ***Enable on-delivery email scanning*** (Activer l'analyse des courriers électroniques à la réception) dans ***Scanning of email*** (Analyse des courriers électroniques).
100. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
101. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***General Options Policies*** (Stratégies concernant les options générales). L'écran ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies concernant les options générales > Ma stratégie par défaut) s'affiche.
102. Sélectionnez ***Workstation*** (Poste de travail) dans la liste déroulante ***Settings for*** (Paramètres de).
103. Cliquez sur l'onglet ***Display Options*** (Options d'affichage). L'écran ***Display Options*** (Options d'affichage) s'ouvre.
104. Sélectionnez les éléments suivants dans ***Console options*** (Options de la console) :
    - ***Display managed tasks in the client console*** *(Afficher les tâches de gestion dans la console du client).*
    - ***Disable default AutoUpdate task schedule*** *(Désactiver la planification de la tâche de mise à jour automatique par défaut).*
105. Sélectionnez ***Server (Serveur)*** dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
106. Cliquez sur l'onglet ***Display Options*** (Options d'affichage). L'écran ***Display Options*** (Options d'affichage) s'ouvre.
107. Sélectionnez les éléments suivants dans ***Console options*** (Options de la console) :
    - ***Display managed tasks in the client console*** *(Afficher les tâches de gestion dans la console du client).*
    - ***Disable default AutoUpdate task schedule*** *(Désactiver la planification de la tâche de mise à jour automatique par défaut).*
108. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
109. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* pour ***Alert Policies*** *(Stratégies d'alerte)*. L'écran ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies d'alerte > Ma stratégie par défaut) s'affiche.
110. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour)*.
111. Cliquez sur l'onglet ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes). L'écran ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes) s'affiche.

112. Désélectionnez ***On-Access Scan*** (Analyse à l'accès), ***On-Demand Scan and scheduled scans*** (Analyses à la demande et analyses planifiées), ***Email Scan*** (Analyse des courriers électroniques) et ***AutoUpdate*** (Mise à jour automatique) dans ***Components that generate alerts*** (Composants générant des alertes).
113. Sélectionnez ***Disable alerting*** (Désactiver les alertes) dans les options ***Alert Manager*** (Gestionnaire d'alertes).
114. Désélectionnez ***Access Protection*** (Protection d'accès) dans ***Components that generate alerts*** (Composants générant des alertes).
115. Cliquez sur ***Additional Alerting Options*** (Options d'alerte supplémentaires). L'écran ***Additional Alerting Options*** (Options d'alerte supplémentaires) s'affiche.
116. Dans le menu déroulant ***Severity Filters*** *(Filtre de gravité)*, sélectionnez ***Suppress all alerts*** *(severities 0 to 4) (Supprimer toutes les alertes (gravités de 0 à 4))*.
117. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)* et cliquez sur l'onglet ***Alert Manager Alerts*** *(Alertes du gestionnaire d'alertes)*. L'écran ***Alert Manager Alerts*** (Alertes du gestionnaire d'alertes) s'affiche.
118. Désélectionnez ***On-Access Scan*** (Analyse à l'accès), ***On-Demand Scan and scheduled scans*** (Analyses à la demande et analyses planifiées), ***Email Scan*** (Analyse des courriers électroniques) et ***AutoUpdate*** (Mise à jour automatique) dans ***Components that generate alerts*** (Composants générant des alertes).
119. Cochez ***Disable alerting*** (Désactiver l'alerte) dans les options ***Alert Manager*** (Gestionnaire d'alertes).
120. Désélectionnez ***Access Protection*** (Protection d'accès) dans ***Components that generate alerts*** (Composants générant des alertes).
121. Cliquez sur ***Additional Alerting Options*** (Options d'alerte supplémentaires). L'écran Additional Alerting Options (Options d'alerte supplémentaires) s'affiche.
122. Dans le menu déroulant ***Severity Filters*** *(Filtre de gravité)*, sélectionnez ***Suppress all alerts*** *(severities 0 to 4) (Supprimer toutes les alertes (gravités de 0 à 4))*.
123. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
124. Cliquez sur ***My Default*** (Ma stratégie par défaut) en regard de l'option ***Access Protection Policies*** (Stratégies de protection d'accès). L'écran ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies de protection d'accès > Ma stratégie par défaut) s'affiche.
125. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for*** ***(****Paramètres pour****)***.
126. Cliquez sur l'onglet ***Access Protection*** (Protection d'accès). L'écran ***Access Protection*** (Protection d'accès) s'affiche.
127. Désélectionnez les options suivantes dans ***Access protection settings*** (Paramètres de protection d'accès) :
    - ***Enable access protection*** *(Activer la protection d'accès).*
    - ***Prevent McAfee services from being stopped*** *(Empêcher l'arrêt des services McAfee).*
    - ***Enable Enhanced Self-Protection*** *(Activer l'autoprotection renforcée).*
128. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
129. Cliquez sur l'onglet ***Access Protection*** (Protection d'accès). L'écran ***Access Protection*** (Protection d'accès) s'affiche.

130. Désélectionnez les options suivantes dans ***Access protection settings*** (Paramètres de protection d'accès) :
    - ***Enable access protection*** *(Activer la protection d'accès).*
    - ***Prevent McAfee services from being stopped*** *(Empêcher l'arrêt des services McAfee).*
    - ***Enable Enhanced Self-Protection*** *(Activer l'autoprotection renforcée).*
131. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
132. Sélectionnez ***My Default*** (Ma stratégie par défaut) en regard de l'option ***Buffer Overflow Protection Policies*** (Stratégies de protection contre les dépassements de tampon). L'écran ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Stratégies de protection contre les dépassements de tampon > Ma stratégie par défaut) s'affiche.
133. Sélectionnez ***Workstation*** *(Poste de travail)* dans la liste déroulante ***Settings for (****Paramètres pour****)***.
134. Cliquez sur l'onglet ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon). L'écran ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon) s'affiche.
135. Désélectionnez ***Show the message dialog box when a buffer overflow is detected*** (Afficher la boîte de dialogue des messages lors de la détection d'un dépassement de tampon) dans ***Client system warning*** (Alerte système client).
136. Désélectionnez ***Enable buffer overflow protection*** (Activer la protection contre les dépassements de tampon) dans ***Buffer overflow settings*** (Paramètres de dépassement de tampon).
137. Sélectionnez ***Server*** *(Serveur)* dans la liste déroulante ***Settings for*** *(Paramètres pour)*.
138. Cliquez sur l'onglet ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon). L'écran ***Buffer Overflow Protection*** (Protection contre les dépassements de tampon) s'affiche.
139. Désélectionnez ***Show the message dialog box when a buffer overflow is detected*** (Afficher la boîte de dialogue des messages lors de la détection d'un dépassement de tampon) dans ***Client system warning*** (Alerte système client).
140. Désélectionnez ***Enable buffer overflow protection*** (Activer la protection contre les dépassements de tampon) dans ***Buffer overflow settings*** (Paramètres de dépassement de tampon).
141. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
142. Dans le menu déroulant ***Product*** *(Produit)*, sélectionnez ***McAfee Agent***. La fenêtre ***Policies*** (Stratégies) correspondant à McAfee Agent s'ouvre.
143. Cliquez sur ***My Default*** *(Ma stratégie par défaut)* en regard de l'option ***Repository*** *(Référentiel)*. L'écran ***McAfee Agent > Repository > My Default*** (McAfee Agent > Référentiel > Ma stratégie par défaut) s'affiche.
144. Cliquez sur l'onglet ***Proxy***. L'écran ***Proxy*** s'affiche.
145. Veillez à ce que l'option ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Utiliser les paramètres Internet Explorer [pour Windows]/les paramètres de préférences du système [pour Mac OSX]) dans ***Proxy settings*** (Paramètres Proxy) soit sélectionnée.
146. Cliquez sur ***Save*** (Enregistrer). L'écran ***Assigned Policies*** (Stratégies affectées) s'affiche.
147. Cliquez sur l'onglet ***Settings*** (Paramètres).
148. Sélectionnez tous les systèmes clients (postes de travail d'acquisition, de consultation et serveur Centricity Cardiology INW) sur lesquels les stratégies configurées doivent être déployées.

149. Cliquez sur ***OK***.

150. Déconnectez-vous d'ePolicy Orchestrator.

Après l'installation de McAfee ePolicy Orchestrator

Activez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Activation de la connexion de bouclage, page 6.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Présentation de l'installation

Installez Trend Micro OfficeScan Client/Server Edition uniquement dans un environnement Mac-Lab/CardioLab en réseau. Le logiciel Trend Micro OfficeScan doit être installé sur le serveur de la console de gestion de l'antivirus avant d'être déployé en tant que client sur le serveur Centricity Cardiology INW et les postes de travail d'acquisition et de consultation. Suivez les instructions ci-dessous pour installer ***Trend Micro OfficeScan Client/Server Edition***.

La mise à jour des listes de virus incombe à l'établissement. Mettez régulièrement à jour les définitions afin de bénéficier de la toute dernière protection sur le système.

Consignes de pré-installation

1. La console de gestion de l'antivirus Trend Micro est censée avoir été installée conformément aux instructions de Trend Micro et être en bon état de fonctionnement.
2. Durant l'installation de Trend Micro OfficeScan, procédez comme indiqué ci-dessous sur le serveur de la console de gestion de l'antivirus :
   a. Désélectionnez ***Enable firewall*** (Activer le pare-feu) dans la fenêtre ***Anti-virus Feature*** (Fonction antivirus).
   b. Sélectionnez ***No, Please do not enable assessment mode*** (Ne pas activer le mode d'évaluation) dans la fenêtre ***Anti-spyware Feature*** (Fonction anti-logiciels espions).
   c. Désélectionnez ***Enable web reputation policy*** (Activer la stratégie d'e-réputation) dans la fenêtre ***Web Reputation Feature*** (Fonction e-réputation).
3. Trend Micro OfficeScan n'est pas recommandé lors de l'utilisation de la fonction ***CO_2*** avec le PDM sur les systèmes Mac-Lab/CardioLab.
4. Si Trend Micro OfficeScan est nécessaire :
   a. Il est recommandé de configurer un serveur de la console de gestion de l'antivirus Trend Micro séparé pour les systèmes Mac-Lab/CardioLab. Une modification globale des paramètres de l'antivirus est nécessaire pour utiliser la fonction ***CO_2*** avec le PDM sur les systèmes Mac-Lab/CardioLab.
   b. Si un serveur de la console de gestion de l'antivirus Trend Micro séparé ne peut pas être configuré, il est nécessaire d'effectuer une modification des paramètres globaux du serveur de la console de gestion de l'antivirus Trend Micro existant après l'installation. Dans la mesure où cette modification aura un impact sur tous les systèmes clients connectés au serveur de la console de gestion de l'antivirus Trend Micro existant, un technicien informatique doit être consulté avant de poursuivre.

5. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur tous les systèmes clients (acquisition, consultation et serveur INW) pour installer le logiciel antivirus.
6. Désactivez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Désactivation de la connexion de bouclage, page 6.
7. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs avant l'installation de l'antivirus, page 7.

Trend Micro OfficeScan - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée)

1. Sélectionnez ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan - <nom du serveur> > Console Web OfficeScan).

REMARQUE : Sélectionnez ensuite ***Continue to this website (not recommended)*** (Rester sur ce site Internet [déconseillé]). Dans la fenêtre Security Alert (Alerte de sécurité), cochez ***In the future, do not show this warning*** (Ne plus afficher cet avertissement à l'avenir) et cliquez sur ***OK***.

2. Si vous recevez un certificat d'erreur indiquant qu'il ne s'agit pas d'un site de confiance, gérez vos certificats de manière à intégrer Trend Micro OfficeScan parmi les sites fiables.
3. Installez les additifs ***AtxEnc*** si le système vous y invite. L'écran Security Warning (Alerte de sécurité) s'affiche.
4. Cliquez sur ***Install*** (Installer).
5. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
6. Cliquez sur ***Update Now*** (Effectuer la mise à jour maintenant) pour installer de nouveaux widgets si le système vous y invite. Attendez que l'installation des nouveaux widgets soit terminée. L'écran Update is completed (Mise à jour terminée) s'affiche.
7. Cliquez sur ***OK***.
8. Dans la barre de menu gauche, cliquez sur ***Networked Computers > Client Installation > Remote*** (Ordinateurs en réseau > Installation du client > Installation distante).
9. Installez les additifs ***AtxConsole*** si le système vous y invite. L'écran Security Warning (Alerte de sécurité) s'affiche.
10. Cliquez sur ***Install*** (Installer).
11. Double-cliquez sur ***My Company*** (Ma société) dans la fenêtre ***Remote Installation*** (Installation distante). Tous les domaines sont répertoriés dans ***My Company*** (Ma société).
12. Développez le domaine (par exemple : INW) dans la liste. Tous les systèmes connectés au domaine apparaissent.
13. Si des domaines ou des systèmes n'apparaissent pas dans la fenêtre ***Domain and Computers*** (Domaine et ordinateurs), effectuez les opérations suivantes dans chacun des systèmes clients (acquisition, consultation et serveur INW) :
    a. Connectez-vous en tant qu'administrateur ou membre de ce groupe sur toutes les machines clientes.
    b. Cliquez sur ***Start > Run*** (Démarrer > Exécuter).
    c. Entrez ***<Anti-Virus Management Console_server_IP_address>*** et appuyez sur la touche ***Entrée***. Saisissez le nom d'utilisateur et le mot de passe de l'administrateur lorsque le système vous y invite.

d. Allez sur ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** et double-cliquez sur ***AutoPcc.exe***. Saisissez le nom d'utilisateur et le mot de passe de l'administrateur lorsque le système vous y invite.

e. Redémarrez les systèmes clients une fois l'installation terminée.

f. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur toutes les machines clientes et attendez que l'icône Trend Micro OfficeScan présente dans la barre des tâches soit de couleur bleue.

g. Sautez les étapes restantes de cette procédure et passez à la procédure de configuration de la console Trend Micro OfficeScan Server.

14. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) et cliquez sur ***Add*** (Ajouter).
15. Entrez le <domain name>\username (<nom de domaine>\nom d'utilisateur) et le mot de passe et cliquez sur ***Log on*** (Se connecter).
16. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) une par une dans le volet ***Selected Computers*** (Ordinateurs sélectionnés) et cliquez sur ***Install*** (Installer).
17. Cliquez sur ***Yes*** (Oui) dans la zone de confirmation.
18. Cliquez sur ***OK*** dans la zone de message ***Number of clients to which notifications were sent*** (Nombre de clients auxquels les notifications ont été envoyées).
19. Redémarrez toutes les machines clientes (acquisition, consultation et serveur INW), connectez-vous en tant qu'Administrateur ou membre de ce groupe sur toutes les machines clientes et attendez que l'icône Trend Micro OfficeScan présente dans la barre des tâches soit de couleur bleue avec une coche verte.
20. Cliquez sur le lien ***Log Off*** (Déconnexion) pour fermer la fenêtre ***OfficeScan Web Console*** (Console Web OfficeScan).

Configuration de la console Trend Micro OfficeScan

1. Cliquez sur ***Start > All Programs > TrendMicro OfficeScan server <servername> > OfficeScan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan <nomduserveur> > Console Web OfficeScan). L'écran de connexion ***Trend Micro OfficeScan Login*** (Connexion à Trend Micro OfficeScan) s'affiche.
2. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur ***Login*** (Ouvrir une session). L'écran ***Summary*** (Résumé) s'affiche.
3. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
4. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
5. Parmi les options ***Settings*** *(Paramètres)*, sélectionnez ***Scan Settings*** *(Paramètres d'analyse)* ***> Manual Scan Settings*** *(Paramètres d'analyse manuelle)*. L'écran ***Manual Scan Settings*** (Paramètres d'analyse manuelle) s'affiche.
6. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :

   - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
   - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
   - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*

- ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
- ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
- ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
- ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to client Computers Exclusion list*** *(Liste d'exclusion de l'analyse [répertoires] > Exclure les répertoires dans lesquels les produits Trend Micro sont installés et sélectionner Ajouter le chemin à la liste d'exclusion des ordinateurs clients).*
- Saisissez les fichiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** et **G:** l'un après l'autre et cliquez sur ***Add*** (Ajouter).

7. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
8. Cliquez sur ***OK*** lorsque vous recevez le message suivant : ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.*** (La liste d'exclusions affichée sur cet écran remplacera la liste d'exclusions des clients ou domaines que vous avez sélectionnée dans l'arborescence du client). ***Do you want to proceed?*** *(Souhaitez-vous continuer ?)* s'affiche.
9. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Manual Scan Settings*** (Paramètres d'analyse manuelle).
10. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
11. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
12. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Real-time Scan Settings*** (Paramètres d'analyse > Paramètres d'analyse en temps réel). L'écran ***Real-time Scan Settings*** (Paramètres d'analyse en temps réel) s'affiche.
13. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Real-Time Scan Settings > Enable virus/malware scan*** *(Paramètres d'analyse en temps réel > Activer l'analyse antivirus/anti-malware).*
    - ***Real-Time Scan Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse en temps réel > Activer l'analyse anti-logiciels espions/anti-grayware).*
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings Only > Enable IntelliTrap*** *(Paramètres d'analyse antivirus/anti-logiciel malveillant uniquement > Activer IntelliTrap).*
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*

- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
- Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** et ***G:*** sont présents dans la ***Exclusion List*** (Liste d'exclusions).

14. Cliquez sur l'onglet ***Action***.
15. Conservez les paramètres par défaut et désélectionnez les options suivantes :
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected*** *(Virus/malware > Afficher un message de notification sur l'ordinateur client lorsqu'un virus/malware est détecté).*
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected*** *(Logiciels espions/Grayware > Afficher un message de notification sur l'ordinateur client lorsqu'un logiciel espion/grayware est détecté).*
16. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
17. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Real-time Scan Settings*** (Paramètres d'analyse en temps réel).
18. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
19. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
20. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Scheduled Scan Settings*** (Paramètres d'analyse > Paramètres d'analyse planifiée). L'écran ***Scheduled Scan Settings*** (Paramètres d'analyse planifiée) s'ouvre.
21. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scheduled Scan Settings > Enable virus/malware scan*** *(Paramètres d'analyse planifiée > Activer l'analyse antivirus/anti-malware).*
    - ***Scheduled Scan Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse planifiée > Activer l'analyse anti-logiciels espions/grayware).*
    - ***Schedule > Weekly, every Sunday, Start time:*** *(Planification > Hebdomadaire, tous les dimanches, Heure de début :)* ***00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
    - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*

- Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** et ***G:*** sont présents dans la Exclusion List (Liste d'exclusions).

22. Cliquez sur l'onglet ***Action***.
23. Conservez les paramètres par défaut et désélectionnez les options suivantes :
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected*** *(Virus/malware > Afficher un message de notification sur l'ordinateur client lorsqu'un virus/malware est détecté).*
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected*** *(Logiciels espions/Grayware > Afficher un message de notification sur l'ordinateur client lorsqu'un logiciel espion/grayware est détecté).*
24. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
25. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Scheduled Scan Settings*** (Paramètres d'analyse planifiée).
26. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
27. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
28. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Scan Now Settings*** (Paramètres d'analyse > Paramètres d'analyse immédiate). L'écran ***Scan Now Settings*** (Paramètres d'analyse immédiate) s'affiche.
29. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Now Settings > Enable virus/malware scan*** *(Paramètres d'analyse immédiate > Activer l'analyse antivirus/anti-malware).*
    - ***Scan Now Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse immédiate > Activer l'analyse anti-logiciels espion/grayware).*
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
    - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
    - Vérifiez que les fichiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** et ***G:***
30. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
31. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Scan Now Settings*** (Paramètres d'analyse immédiate).

32. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
33. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
34. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Web Reputation Settings*** (Paramètres d'e-réputation). L'écran ***Web Reputation Settings*** (Paramètres d'e-réputation) s'affiche.
35. Cliquez sur l'onglet ***External Clients*** (Clients externes) et désélectionnez ***Enable Web reputation policy on the following operating systems*** (Activer la stratégie d'e-réputation sur les systèmes d'exploitation suivants) si vous avez sélectionné cette option pendant l'installation.
36. Cliquez sur l'onglet ***Internal Clients*** (Clients internes) et désélectionnez ***Enable Web reputation policy on the following operating systems*** (Activer la stratégie d'e-réputation sur les systèmes d'exploitation suivants) si vous avez sélectionné cette option pendant l'installation.
37. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
38. Cliquez sur ***Close*** pour fermer l'écran ***Web Reputation*** (E-réputation).
39. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
40. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
41. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Behavior Monitoring Settings*** (Paramètres de surveillance des comportements). L'écran ***Behavior Monitoring Settings*** (Paramètres de surveillance des comportements) s'affiche.
42. Désélectionnez les options ***Enable Malware Behavior Blocking*** (Activer le blocage des comportements de malware) et ***Enable Event Monitoring*** (Activer la surveillance des événements).
43. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
44. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Behavior Monitoring*** (Surveillance des événements).
45. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
46. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
47. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Device Control Settings*** (Paramètres de contrôle des périphériques). L'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques) s'affiche.
48. Cliquez sur l'onglet ***External Clients*** (Clients externes) et désélectionnez les options suivantes :
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access*** *(Afficher un message de notification sur l'ordinateur client lorsqu'OfficeScan détecte un accès par un périphérique non autorisé).*
    - ***Block the AutoRun function on USB storage devices*** *(Bloquer la fonction AutoRun [exécution automatique] sur les périphériques de stockage USB).*
    - ***Enable Device Control*** *(Activer le contrôle des périphériques).*
49. Cliquez sur l'onglet ***Internal Clients*** (Clients internes) et désélectionnez les options suivantes :
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access*** *(Afficher un message de notification sur l'ordinateur client lorsqu'OfficeScan détecte un accès par un périphérique non autorisé).*

- ***Block the AutoRun function on USB storage devices*** *(Bloquer la fonction AutoRun [exécution automatique] sur les périphériques de stockage USB).*
- ***Enable Device Control*** *(Activer le contrôle des périphériques).*

50. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
51. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques).
52. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).
53. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
54. Parmi les options ***Settings*** *(Paramètres)*, sélectionnez ***Privileges and Other Settings*** *(Privilèges et autres paramètres)*.
55. Cliquez sur l'onglet ***Privileges*** (Privilèges) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Privileges > Configure Manual Scan Settings*** *(Privilèges d'analyse > Configurer les paramètres de l'analyse manuelle).*
    - ***Scan Privileges > Configure Real-time Scan Settings*** *(Privilèges d'analyse > Configurer les paramètres de l'analyse en temps réel).*
    - ***Scan Privileges > Configure Scheduled Scan Settings*** *(Privilèges d'analyse > Configurer les paramètres d'analyse planifiée).*
    - ***Proxy Setting Privileges > Allow the client user to configure proxy settings*** *(Privilèges de paramètre proxy > Autoriser l'utilisateur client pour configurer les paramètres proxy).*
    - ***Uninstallation > Require a password for the user to uninstall the OfficeScan Client*** *(Désinstallation > Demander un mot de passe pour que l'utilisateur désinstalle le client OfficeScan).* Saisissez un mot de passe valide et confirmez-le.
    - ***Unloading > Require a password for the user to unload the OfficeScan client*** *(Déchargement > Demander un mot de passe pour que l'utilisateur décharge le client OfficeScan).* Saisissez un mot de passe valide et confirmez-le.
56. Cliquez sur l'onglet ***Other Settings*** (Autres paramètres).
57. Sélectionnez ***Client Security Settings > Normal*** (Paramètres de sécurité du client > Normaux) et désactivez les autres options.

REMARQUE : Les options suivantes doivent impérativement être désactivées.

- ***Client Self-protection > Protect OfficeScan client services*** *(Auto-protection du client > Protéger les services du client OfficeScan).*
- ***Client Self-protection > Protect files in the OfficeScan client installation folder*** *(Auto-protection du client > Protéger les fichiers présents dans le dossier d'installation du client OfficeScan).*
- ***Client Self-protection > Protect OfficeScan client registry keys*** *(Auto-protection du client > Protéger les clés de registre du client OfficeScan).*
- ***Client Self-protection > Protect OfficeScan client processes*** *(Auto-protection du client > Protéger les processus du client OfficeScan).*

58. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
59. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Privileges and Other Settings*** (Privilèges et autres paramètres).
60. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Client Management*** (Ordinateurs en réseau > Administration du client).

61. A droite, sélectionnez ***OfficeScan Server*** (Serveur OfficeScan).
62. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Additionnal Service Settings*** (Paramètres de service supplémentaires).
63. Désélectionnez l'option ***Enable service on the following operating systems*** (Activer le service sur les systèmes d'exploitation suivants).
64. Cliquez sur ***Apply to All Clients*** (Appliquer à tous les clients).
65. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Additional Service Settings*** (Paramètres de service supplémentaires).
66. Dans le volet de gauche, cliquez sur le lien ***Networked Computers > Global Client Settings (Ordinateurs en réseau > Paramètres client globaux)***.
67. Cochez uniquement les options suivantes et désélectionnez les autres options :
    - ***Scan Settings > Configure Scan settings for large compressed files*** *(Paramètres d'analyse > Configurer les paramètres d'analyse des fichiers compressés volumineux).*
    - ***Scan Settings > Do not scan files in the compressed file if the size exceeds 2 MB*** *(Paramètres de numérisation > Ne pas analyser les fichiers du fichier compressé si la taille est supérieure à 2 Mo).*
    - ***Scan Settings > In a compressed file scan only the first 100 files*** *(Paramètres de numérisation > Dans un fichier compressé, analyser uniquement les 100 premiers fichiers).*
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan*** *(Paramètres de numérisation > Exclure le dossier de base de données du serveur OfficeScan de l'analyse en temps réel).*
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans*** *(Paramètres d'analyse > Exclure les dossiers et fichiers du serveur Microsoft Exchange de l'analyse).*
    - ***Reserved Disk Space > Reserve 60 MB of disk space for updates*** *(Espace disque réservé > Réserver 60 Mo d'espace disque pour les mises à jour).*
    - ***Proxy Configuration > Automatically detect settings*** *(Configuration du proxy > Paramètres de détection automatique).*

REMARQUE : Il est important de désélectionner ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver*** (Paramètres d'alerte > Afficher un message de notification si l'ordinateur client doit redémarrer pour charger un pilote de noyau).

68. Cliquez sur ***Save*** (Enregistrer).
69. Dans le volet de gauche, cliquez sur le lien ***Updates > Networked Computers > Manual Updates*** (Mises à jour > Ordinateurs en réseau > Mises à jour manuelles).
70. Sélectionnez ***Manually select client*** (Sélectionner le client manuellement) et cliquez sur ***Select*** (Sélectionner).
71. Cliquez sur le nom de domaine correspondant dans ***OfficeScan Server*** (Serveur OfficeScan).
72. Sélectionnez les systèmes clients un par un et cliquez sur ***Initiate Component Update*** (Lancer la mise à jour du composant).
73. Cliquez sur ***OK*** dans la zone de message.
74. Cliquez sur le lien ***Log Off*** (Déconnexion) et fermez la fenêtre OfficeScan Web Console (Console OfficeScan Web).

Après l'installation de Trend Micro OfficeScan

1. Sur le(s) système(s) d'acquisition, procédez comme suit pour configurer Trend Micro :

   a. Cliquez sur ***Start > Control Panel > Network and Sharing Center*** (Démarrer > Panneau de configuration > Centre Réseau et partage).

   b. Cliquez sur ***Change adapter settings*** (Modifier les paramètres de l'adaptateur).

   c. Cliquez avec le bouton droit de la souris sur ***Local Area Connection*** (Connexion au réseau local) et sélectionnez ***Properties*** (Propriétés).

   d. Sélectionnez ***Internet Protocol Version 4 (TCP/IPv4)*** (Protocole Internet Version 4 [TCP/IPv4]), puis cliquez sur ***Properties*** (Propriétés).

   e. Notez l'adresse IP _____.

   f. Fermez toutes les fenêtres.

   g. Cliquez sur ***Start > Run*** (Démarrer > Exécuter) et entrez **regedit**.

   h. Accédez à ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.

   i. Sur le volet de droite, cliquez avec le bouton droit de la souris sur un espace vide et sélectionnez ***New > String value*** (Nouveau > Valeur de chaîne).

   j. Saisissez le nom **IP Template** et appuyez sur la touche **Entrée**.

   k. Double-cliquez sur le registre ***IP Template***.

   l. Dans le champ de données ***Value*** (Valeur), saisissez l'adresse IP de connexion au réseau local notée à l'étape .

   m. Cliquez sur ***OK***.

   n. Fermez l'éditeur de registre.

2. Activez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Activation de la connexion de bouclage, page 6.

3. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs après l'installation de l'antivirus, page 8.

Configurations des paramètres globaux de Trend Micro

REMARQUE : Les instructions suivantes doivent être suivies uniquement lors de l'utilisation de la fonction CO_2 avec le PDM sur les systèmes Mac-Lab/CardioLab. Avant d'effectuer les étapes ci-dessous, assurez-vous d'avoir consulté un technicien informatique.

1. Sur le serveur de la console de gestion de l'antivirus, accédez au dossier ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.

2. Ouvrez le fichier ***ofcscan.ini*** dans un éditeur de texte.

3. Dans la section ***Global Setting*** (Paramètre global), réglez la valeur de la clé suivante à « **1** » : [Global Setting] ***RmvTmTDI=1***

4. Enregistrez le fichier ofcscan.ini, puis fermez-le.

5. Sélectionnez ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan - <nom du serveur> > Console Web OfficeScan).

6. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter). L'écran ***Summary*** (Résumé) s'affiche.
7. Cliquez sur ***Networked Computers > Global Client Settings*** (Ordinateurs en réseau > Paramètres client globaux).
8. Cliquez sur ***Save*** (Enregistrer).
9. Dans le volet de gauche, cliquez sur le lien ***Updates > Networked Computers > Manual Update*** (Mises à jour > Ordinateurs en réseau > Mise à jour manuelle).
10. Sélectionnez ***Manually select clients*** (Sélectionner le client manuellement) et cliquez sur ***Select*** (Sélectionner).
11. Cliquez sur le nom de domaine correspondant dans ***OfficeScan Server*** (Serveur OfficeScan).
12. Sélectionnez les systèmes clients un par un et cliquez sur ***Initiate Component Update*** (Lancer la mise à jour du composant).
13. Cliquez sur ***OK*** dans la zone de message.
14. Sur chaque système d'acquisition, procédez comme suit :
    a. Ouvrez l'éditeur du registre.
    b. Accédez à ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Assurez-vous que la valeur du registre ***RmvTmTDI*** est réglée à « **1** ».
    d. Accédez à ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Supprimez la clé de registre ***tmtdi*** si elle existe.
    f. Fermez l'éditeur de registre.
    g. Redémarrez les systèmes clients.
    h. Connectez-vous aux systèmes clients en tant qu'administrateur ou que membre de ce groupe.
    i. Sur chaque système client, ouvrez une invite de commande avec des droits d'administrateur, puis saisissez la commande « ***sc query tmtdi*** ».
    j. Assurez-vous que le message ***The specified service does not exist as an installed service*** (Le service spécifié n'existe pas en tant que service installé) s'affiche.
15. Sur le serveur de la console de gestion de l'antivirus, cliquez sur ***Log off*** (Déconnexion) et fermez la fenêtre OfficeScan Web Console (Console OfficeScan Web).

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Installez Trend Micro OfficeScan Client/Server Edition uniquement dans un environnement Mac-Lab/CardioLab en réseau. Le logiciel Trend Micro OfficeScan doit être installé sur le serveur de la console de gestion de l'antivirus avant d'être déployé en tant que client sur le serveur Centricity Cardiology INW et les postes de travail d'acquisition et de consultation. Suivez les instructions ci-après pour installer ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

La mise à jour des listes de virus incombe à l'établissement. Mettez régulièrement à jour les définitions afin de bénéficier de la toute dernière protection sur le système.

Consignes de pré-installation

1. La console de gestion de l'antivirus Trend Micro est censée avoir été installée conformément aux instructions de Trend Micro et être en bon état de fonctionnement.
2. Durant l'installation de Trend Micro OfficeScan, procédez comme indiqué ci-dessous sur le serveur de la console de gestion de l'antivirus :
   a. Désélectionnez ***Enable firewall*** (Activer le pare-feu) dans la fenêtre ***Anti-virus Feature*** (Fonction antivirus).
   b. Sélectionnez ***No, Please do not enable assessment mode*** (Ne pas activer le mode d'évaluation) dans la fenêtre ***Anti-spyware Feature*** (Fonction anti-logiciels espions).
   c. Désélectionnez ***Enable web reputation policy*** (Activer la stratégie d'e-réputation) dans la fenêtre ***Web Reputation Feature*** (Fonction e-réputation).
3. Trend Micro OfficeScan n'est pas recommandé lors de l'utilisation de la fonction CO_2 avec le PDM sur les systèmes Mac-Lab/CardioLab.
4. Si Trend Micro OfficeScan est nécessaire :
   a. Il est recommandé de configurer un serveur de la console de gestion de l'antivirus Trend Micro séparé pour les systèmes Mac-Lab/CardioLab. Une modification globale des paramètres de l'antivirus est nécessaire pour utiliser la fonction CO_2 avec le PDM sur les systèmes Mac-Lab/CardioLab.
   b. Si un serveur de la console de gestion de l'antivirus Trend Micro séparé ne peut pas être configuré, il est nécessaire d'effectuer une modification des paramètres globaux du serveur de la console de gestion de l'antivirus Trend Micro existant après l'installation. Dans la mesure où cette modification aura un impact sur tous les systèmes clients connectés au serveur de la console de gestion de l'antivirus Trend Micro existant, un technicien informatique doit être consulté avant de poursuivre.
5. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur tous les systèmes clients (acquisition, consultation et serveur INW) pour installer le logiciel antivirus.
6. Désactivez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Désactivation de la connexion de bouclage, page 6.
7. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs avant l'installation de l'antivirus, page 7.
8. Les certificats racine et intermédiaires suivants sont nécessaires pour l'installation sur les machines clientes acquisition, consultation et INW :
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
9. Répétez les sous-étapes suivantes pour installer les cinq certificats de niveau racine et intermédiaire énumérés à l'étape 8.
   a. Accédez à ***C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   REMARQUE : Dans INW, accédez à C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

b. Si le chemin de dossier indiqué ci-dessus n'est pas présent, obtenez manuellement les certificats de niveau racine et intermédiaire requis pour l'installation.

c. Double-cliquez sur ***AddTrustExternalCARoot.crt*** pour l'installer sur les systèmes MLCL (acquisition, consultation et INW).

d. Ouvrez le certificat, puis cliquez sur ***Install Certificate*** (Installer le certificat).

e. Cliquez sur ***Next*** (Suivant) lorsque le ***Certificate Import Wizard*** (Assistant d'importation de certificat) apparaît.

f. Dans la fenêtre ***Certificate Store***, sélectionnez ***Place all certificates in the following store*** (Placer tous les certificats sur le support suivant), puis cliquez sur ***Browse*** (Parcourir).

g. Cochez ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Afficher les supports physiques > Autorités de certification racine de confiance > Ordinateur local), puis cliquez sur ***OK***.

h. Cliquez sur ***Next*** (Suivant) dans le ***Certificate Import Wizard*** (Assistant d'importation de certificat).

i. Cliquez sur ***Finish*** (Terminer). Le message ***The import was successful*** (Importation réussie) doit apparaître.

j. Répétez l'étape 9 pour les autres certificats énumérés à l'étape 8.

REMARQUE : Chaque certificat possède une date d'expiration. Lorsque le certificat expire, il doit être renouvelé et mis à jour sur les systèmes MLCL afin de s'assurer que l'agent OfficeScan fonctionne comme prévu.

Trend Micro OfficeScan - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée pour la version 11.0 SP1)

1. Sélectionnez ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan - <nom du serveur> > Console Web OfficeScan).

REMARQUE : Sélectionnez ensuite ***Continue to this website (not recommended)*** (Rester sur ce site Internet [déconseillé]). Dans la fenêtre Security Alert (Alerte de sécurité), cochez ***In the future, do not show this warning*** (Ne plus afficher cet avertissement à l'avenir) et cliquez sur ***OK***.

2. Si vous recevez un certificat d'erreur indiquant qu'il ne s'agit pas d'un site de confiance, gérez vos certificats de manière à intégrer Trend Micro OfficeScan parmi les sites fiables.

3. Installez les additifs ***AtxEnc*** si le système vous y invite. L'écran Security Warning (Alerte de sécurité) s'affiche.

   a. Cliquez sur ***Install*** (Installer).

4. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).

5. Cliquez sur ***Update Now*** (Effectuer la mise à jour maintenant) pour installer de nouveaux widgets si le système vous y invite. Attendez que l'installation des nouveaux widgets soit terminée. L'écran Update is completed (Mise à jour terminée) s'affiche.

   a. Cliquez sur ***OK***.

6. Dans la barre de menus supérieure, cliquez sur ***Agents > Agent Installation > Remote*** (Agents > Installation d'un agent > À distance).

7. Installez les additifs ***AtxConsole*** si le système vous y invite. L'écran Security Warning (Alerte de sécurité) s'affiche.

   a. Cliquez sur ***Install*** (Installer).

8. Double-cliquez sur ***OfficeScan Server*** (Serveur OfficeScan) dans la fenêtre ***Remote Installation*** (Installation distante). Tous les domaines sont répertoriés dans ***OfficeScan Server*** (Serveur OfficeScan).

9. Double-cliquez sur le domaine (exemple : INW) dans la liste. Tous les systèmes connectés au domaine apparaissent.

REMARQUE : Si des domaines ou des systèmes ne sont pas répertoriés dans la fenêtre ***Domains and Endpoints*** (domaines et terminaux), consultez la section Résolution de problèmes des domaines ou systèmes non répertoriés dans la fenêtre Domains and Endpoints (Domaines et terminaux), page 74 pour les ajouter manuellement ou lancez directement l'installation depuis la machine cliente.

10. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) et cliquez sur ***Add*** (Ajouter).

11. Entrez le <domain name>\username (<nom de domaine>\nom d'utilisateur) et le mot de passe et cliquez sur ***Log on*** (Se connecter).

12. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) une par une dans le volet ***Selected Endpoints*** (Terminaux sélectionnés) et cliquez sur ***Install*** (Installer).

13. Cliquez sur ***OK*** dans la zone de confirmation.

14. Cliquez sur ***OK*** dans la zone de message ***Number of clients to which notifications were sent*** (Nombre de clients auxquels les notifications ont été envoyées).

15. Redémarrez toutes les machines clientes (acquisition, consultation et serveur INW), connectez-vous en tant qu'Administrateur ou membre de ce groupe sur toutes les machines clientes et attendez que l'icône Trend Micro OfficeScan présente dans la barre des tâches soit de couleur bleue avec une coche verte.

16. Cliquez sur le lien ***Log Off*** (Déconnexion) pour fermer la fenêtre ***OfficeScan Web Console*** (Console Web OfficeScan).

Configuration de la console Trend Micro OfficeScan Server pour la version 11.0 SP1

1. Cliquez sur ***Start > All Programs > TrendMicro OfficeScan server <servername> > OfficeScan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan <nomduserveur> > Console Web OfficeScan). L'écran de connexion ***Trend Micro OfficeScan Login*** (Connexion à Trend Micro OfficeScan) s'affiche.

2. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur ***Login*** (Ouvrir une session). L'écran ***Summary*** (Résumé) s'affiche.

3. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).

4. À gauche, sélectionnez le serveur ***OfficeScan***.

5. Parmi les options ***Settings*** *(Paramètres)*, sélectionnez ***Scan Settings*** *(Paramètres d'analyse) > Manual Scan Settings (Paramètres d'analyse manuelle)*. L'écran ***Manual Scan Settings*** (Paramètres d'analyse manuelle) s'affiche.

6. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
   - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
   - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
   - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
   - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
   - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
7. Cliquez sur l'onglet Scan Exclusion (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
   - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
   - ***Select Adds path*** (Sélectionner Ajouter le chemin vers) dans la liste déroulante sous ***Saving the officescan agent's exclusion list does the following:*** (L'enregistrement de la liste d'exclusion de l'agent officescan provoque l'action suivante :)
   - Saisissez les fichiers **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** et **G:** l'un après l'autre et cliquez sur **+**.
8. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
9. Cliquez sur ***OK*** lorsque vous recevez le message suivant : ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.*** (La liste d'exclusions affichée sur cet écran remplacera la liste d'exclusions des clients ou domaines que vous avez sélectionnée dans l'arborescence du client). ***Do you want to proceed?*** *(Souhaitez-vous continuer ?)* s'affiche.
10. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Manual Scan Settings*** (Paramètres d'analyse manuelle).
11. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
12. À gauche, sélectionnez le serveur ***OfficeScan***.
13. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Real-time Scan Settings*** (Paramètres d'analyse > Paramètres d'analyse en temps réel). L'écran ***Real-time Scan Settings*** (Paramètres d'analyse en temps réel) s'affiche.
14. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
   - ***Real-Time Scan Settings > Enable virus/malware scan*** *(Paramètres d'analyse en temps réel > Activer l'analyse antivirus/anti-malware).*
   - ***Real-Time Scan Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse en temps réel > Activer l'analyse anti-logiciels espions/anti-grayware).*
   - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*

- ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
- ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap*** *(Paramètres d'analyse antivirus/anti-logiciel malveillant uniquement > Activer IntelliTrap).*

15. Cliquez sur l'onglet Scan Exclusion (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
    - Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** et ***G:*** sont présents dans la ***Exclusion List*** (Liste d'exclusions).
16. Cliquez sur l'onglet ***Action***.
17. Conservez les paramètres par défaut et désélectionnez les options suivantes :
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected*** *(Virus/malware > Afficher un message de notification sur les terminaux lorsqu'un virus/malware est détecté).*
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected*** *(Logiciels espions/Grayware > Afficher un message de notification sur les terminaux lorsqu'un logiciel espion/grayware est détecté).*
18. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
19. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Real-time Scan Settings*** (Paramètres d'analyse en temps réel).
20. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
21. À gauche, sélectionnez le serveur ***OfficeScan***.
22. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Scheduled Scan Settings*** (Paramètres d'analyse > Paramètres d'analyse planifiée). L'écran ***Scheduled Scan Settings*** (Paramètres d'analyse planifiée) s'ouvre.
23. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scheduled Scan Settings > Enable virus/malware scan*** *(Paramètres d'analyse planifiée > Activer l'analyse antivirus/anti-malware).*
    - ***Scheduled Scan Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse planifiée > Activer l'analyse anti-logiciels espions/grayware).*
    - ***Schedule > Weekly, every Sunday, Start time:*** *(Planification > Hebdomadaire, tous les dimanches, Heure de début :)* ***00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*

- ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
- ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
- ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*

24. Cliquez sur l'onglet ***Scan Exclusion*** (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
    - Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** et ***G:*** sont présents dans la Exclusion List (Liste d'exclusions).
25. Cliquez sur l'onglet ***Action***.
26. Conservez les paramètres par défaut et désélectionnez les options suivantes :
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected*** *(Virus/malware > Afficher un message de notification sur les terminaux lorsqu'un virus/malware est détecté).*
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected*** *(Logiciels espions/Grayware > Afficher un message de notification sur les terminaux lorsqu'un logiciel espion/grayware est détecté).*
27. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
28. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Scheduled Scan Settings*** (Paramètres d'analyse planifiée).
29. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
30. À gauche, sélectionnez le serveur ***OfficeScan***.
31. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Scan Now Settings*** (Paramètres d'analyse > Paramètres d'analyse immédiate). L'écran ***Scan Now Settings*** (Paramètres d'analyse immédiate) s'affiche.
32. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Now Settings > Enable virus/malware scan*** *(Paramètres d'analyse immédiate > Activer l'analyse antivirus/anti-malware).*
    - ***Scan Now Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse immédiate > Activer l'analyse anti-logiciels espion/grayware).*
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
    - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*

33. Cliquez sur l'onglet ***Scan Exclusion*** (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
    - Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** et ***G:*** sont présents dans la Exclusion List (Liste d'exclusions).
34. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
35. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Scan Now Settings*** (Paramètres d'analyse immédiate).
36. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
37. À gauche, sélectionnez le serveur ***OfficeScan***.
38. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Web Reputation Settings*** (Paramètres d'e-réputation). L'écran ***Web Reputation Settings*** (Paramètres d'e-réputation) s'affiche.
39. Cliquez sur l'onglet ***External Agents*** (Agents externes) et désélectionnez ***Enable Web reputation policy on the following operating systems*** (Activer la stratégie d'e-réputation sur les systèmes d'exploitation suivants) si vous avez sélectionné cette option pendant l'installation.
40. Cliquez sur l'onglet ***Internal Agents*** (Agents internes) et désélectionnez ***Enable Web reputation policy on the following operating systems*** (Activer la stratégie d'e-réputation sur les systèmes d'exploitation suivants) si vous avez sélectionné cette option pendant l'installation.
41. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
42. Cliquez sur ***Close*** pour fermer l'écran ***Web Reputation*** (E-réputation).
43. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
44. À gauche, sélectionnez le serveur ***OfficeScan***.
45. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Behavior Monitoring Settings*** (Paramètres de surveillance des comportements). L'écran ***Behavior Monitoring Settings*** (Paramètres de surveillance des comportements) s'affiche.
46. Désélectionnez les options ***Enable Malware Behavior Blocking for known and potential threats*** (Activer le blocage des comportements de malware pour les menaces connues et potentielles) and ***Enable Event Monitoring*** (Activer la surveillance des événements).
47. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
48. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Behavior Monitoring*** (Surveillance des événements).
49. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
50. À gauche, sélectionnez le serveur ***OfficeScan***.

51. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Device Control Settings*** (Paramètres de contrôle des périphériques). L'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques) s'affiche.
52. Cliquez sur l'onglet ***External Agents*** (Agents externes) et désélectionnez les options suivantes :
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access*** *(Afficher un message de notification sur les terminaux lorsqu'OfficeScan détecte un accès par un périphérique non autorisé).*
    - ***Block the AutoRun function on USB storage devices*** *(Bloquer la fonction AutoRun [exécution automatique] sur les périphériques de stockage USB).*
53. Cliquez sur l'onglet ***Internal Agents*** (Agents internes) et désélectionnez les options suivantes :
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access*** *(Afficher un message de notification sur les terminaux lorsqu'OfficeScan détecte un accès par un périphérique non autorisé).*
    - ***Block the AutoRun function on USB storage devices*** *(Bloquer la fonction AutoRun [exécution automatique] sur les périphériques de stockage USB).*
54. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
55. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques).
56. Parmi les options ***Settings*** (Paramètres), sélectionnez de nouveau ***Device Control Settings*** (Paramètres de contrôle des périphériques). L'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques) s'affiche.
57. Cliquez sur l'onglet ***External Agents*** (Agents externes) et désélectionnez ***Enable Device Control*** (Activer le contrôle des périphériques).
58. Cliquez sur l'onglet ***Internal Agents*** (Agents internes) et désélectionnez ***Enable Device Control*** (Activer le contrôle des périphériques).
59. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
60. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques).
61. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
62. À gauche, sélectionnez le serveur ***OfficeScan***.
63. Parmi les options ***Settings*** *(Paramètres)*, sélectionnez ***Privileges and Other Settings*** *(Privilèges et autres paramètres)*.
64. Cliquez sur l'onglet ***Privileges*** (Privilèges) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan > Configure Manual Scan Settings*** *(Analyse > Configurer les paramètres de l'analyse manuelle).*
    - ***Scans > Configure Real-time Scan Settings (****Analyses > Configurer les paramètres de l'analyse en temps réel).*
    - ***Scans > Configure Scheduled Scan Settings*** *(Analyses > Configurer les paramètres d'analyse planifiée).*
    - ***Proxy Setting > Allow users to configure proxy settings*** *(Paramètre proxy > Autoriser les utilisateurs pour configurer les paramètres proxy).*
    - ***Uninstallation > Requires a password*** *(Désinstallation > Nécessite un mot de passe).* Saisissez un mot de passe valide et confirmez-le.
    - ***Unloading and Unlock > Requires a password*** *(Décharger et déverrouiller > Nécessite un mot de passe).* Saisissez un mot de passe valide et confirmez-le.

65. Cliquez sur l'onglet ***Other Settings*** (Autres paramètres).
66. Sélectionnez ***OfficeScan Agent Security Settings > Normal:*** (Paramètres de sécurité de l'agent OfficeScan > Normaux :) ***Allow users to access OfficeScan agent files and registries*** *(Autoriser les utilisateurs à accéder aux dossiers et répertoires de l'agent OfficeScan)* et désélectionnez les options restantes.

REMARQUE : Les options suivantes doivent impérativement être désactivées.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services*** *(Auto-protection de l'agent OfficeScan > Protéger les services de l'agent OfficeScan).*
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder*** *(Auto-protection de l'agent OfficeScan > Protéger les fichiers présents dans le dossier d'installation de l'agent OfficeScan).*
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys*** *(Auto-protection de l'agent OfficeScan > Protéger les clés de registre de l'agent OfficeScan).*
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes*** *(Auto-protection de l'agent OfficeScan > Protéger les processus de l'agent OfficeScan).*

67. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
68. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Privileges and Other Settings*** (Privilèges et autres paramètres).
69. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
70. À gauche, sélectionnez le serveur ***OfficeScan***.
71. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Additionnal Service Settings*** (Paramètres de service supplémentaires).
72. Désélectionnez l'option ***Enable service on the following operating systems*** (Activer le service sur les systèmes d'exploitation suivants).
73. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
74. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Additional Service Settings*** (Paramètres de service supplémentaires).
75. Dans le volet supérieur, sélectionnez le lien ***Agents > Global Agent Settings*** (Agents > Paramètres agent globaux).
76. Cochez uniquement les options suivantes et désélectionnez les autres options :

- ***Scan Settings for Large Compressed Files > Configure Scan settings for large compressed files*** *(Paramètres d'analyse des fichiers compressés volumineux > Configurer les paramètres d'analyse des fichiers compressés volumineux).*
- ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Paramètres d'analyse des fichiers compressés volumineux > Ne pas analyser les fichiers du fichier compressé si la taille est supérieure à 2 Mo). Suivez cette option pour ***Real-Time Scan*** (analyse en temps réel) et ***Manual Scan/Schedule Scan/Scan Now*** (analyse manuelle/analyse planifiée/analyse immédiate).
- ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files*** *(Paramètres d'analyse des fichiers compressés volumineux > Dans un fichier compressé, analyser uniquement les 100 premiers fichiers).* Suivre cette option pour ***Real-Time Scan*** (analyse en temps réel) et ***Manual Scan/Schedule Scan/Scan Now*** (analyse manuelle/analyse planifiée/analyse immédiate).
- ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan*** *(Paramètres de numérisation > Exclure le dossier de base de données du serveur OfficeScan de l'analyse en temps réel).*

- ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans*** *(Paramètres d'analyse > Exclure les dossiers et fichiers du serveur Microsoft Exchange de l'analyse).*
- ***Reserved Disk Space > Reserve 60 MB of disk space for updates*** *(Espace disque réservé > Réserver 60 Mo d'espace disque pour les mises à jour).*
- ***Proxy Configuration > Automatically detect settings*** *(Configuration du proxy > Paramètres de détection automatique).*

REMARQUE : Il est important de désélectionner ***Alert Settings*** (Paramètres d'alerte) -> ***Display a notification message*** (Afficher un message de notification) si le terminal doit redémarrer pour charger un pilote du noyau.

77. Cliquez sur ***Save*** (Enregistrer).
78. Dans le volet supérieur, cliquez sur le lien ***Updates > Agents > Manual Updates*** (Mises à jour > Agents > Mises à jour manuelles).
79. Sélectionnez ***Manually Select agents*** (Sélectionner les agents manuellement) et cliquez sur ***Select*** (Sélectionner).
80. Double-cliquez sur le nom de domaine correspondant dans ***OfficeScan Server*** (Serveur OfficeScan).
81. Sélectionnez les systèmes clients un par un et cliquez sur ***Initiate Update*** (Lancer la mise à jour).
82. Cliquez sur ***OK*** dans la zone de message.
83. Cliquez sur le lien ***Log Off*** (Déconnexion) et fermez la fenêtre OfficeScan Web Console (Console OfficeScan Web).

Configurations des paramètres globaux de Trend Micro

REMARQUE : Les instructions suivantes doivent être suivies uniquement lors de l'utilisation de la fonction CO_2 avec le PDM sur les systèmes Mac-Lab/CardioLab. Avant d'effectuer les étapes ci-dessous, assurez-vous d'avoir consulté un technicien informatique.

1. Sur le serveur de la console de gestion de l'antivirus, accédez au dossier ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. Ouvrez le fichier ***ofcscan.ini*** dans un éditeur de texte.
3. Dans la section Global Setting (Paramètre global), réglez la valeur de la clé suivante à **« 1 »** : [Global Setting] ***RmvTmTDI=1***
4. Enregistrez le fichier ofcscan.ini, puis fermez-le.
5. Sélectionnez ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan - <nom du serveur> > Console Web OfficeScan).
6. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter). L'écran ***Dashboard*** (Tableau de bord) s'affiche.
7. Cliquez sur ***Agents > Global Agent Settings*** (Agents > Paramètres agent globaux).
8. Cliquez sur ***Save*** (Enregistrer).
9. Dans le volet de gauche, cliquez sur le lien ***Updates > Agents > Manual Update*** (Mises à jour > Agents > Mise à jour manuelle).
10. Sélectionnez ***Manually select clients*** (Sélectionner le client manuellement) et cliquez sur ***Select*** (Sélectionner).

11. Cliquez sur le nom de domaine correspondant dans ***OfficeScan Server*** (Serveur OfficeScan).
12. Sélectionnez les systèmes clients un par un et cliquez sur ***Initiate Update*** (Lancer la mise à jour).
13. Cliquez sur ***OK*** dans la zone de message.
14. Sur chaque système d'acquisition, procédez comme suit :
    a. Ouvrez l'éditeur du registre.
    b. Accédez à ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***
    c. Assurez-vous que la valeur du registre ***RmvTmTDI*** est réglée à « ***1*** ».
    d. Accédez à ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Supprimez la clé de registre ***tmtdi*** si elle existe.
    f. Fermez l'éditeur de registre.
    g. Redémarrez les systèmes clients.
    h. Connectez-vous aux systèmes clients en tant qu'administrateur ou que membre de ce groupe.
    i. Sur chaque système client, ouvrez une invite de commande avec des droits d'administrateur, puis saisissez la commande « ***sc query tmtdi*** ».
    j. Assurez-vous que le message ***The specified service does not exist as an installed service*** (Le service spécifié n'existe pas en tant que service installé) s'affiche.
15. Sur le serveur de la console de gestion de l'antivirus, cliquez sur ***Log off*** (Déconnexion) et fermez la fenêtre OfficeScan Web Console (Console OfficeScan Web).

Après l'installation de Trend Micro OfficeScan

1. Activez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Activation de la connexion de bouclage, page 6.
2. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs après l'installation de l'antivirus, page 8.

Trend Micro OfficeScan Client/Server Edition XG 12.0 et XG SP1

Présentation de l'installation

Installez Trend Micro OfficeScan Client/Server Edition uniquement dans un environnement Mac-Lab/CardioLab en réseau. Le logiciel Trend Micro OfficeScan doit être installé sur le serveur de la console de gestion de l'antivirus avant d'être déployé en tant que client sur le serveur Centricity Cardiology INW et les postes de travail d'acquisition et de consultation. Suivez les instructions ci-après pour installer ***Trend Micro OfficeScan Client/Server Edition XG 12.0 et XG SP1***.

La mise à jour des listes de virus incombe à l'établissement. Mettez régulièrement à jour les définitions afin de bénéficier de la toute dernière protection sur le système.

Consignes de pré-installation

REMARQUE : Internet Explorer 10 est le navigateur IE minimal pour pouvoir exécuter le gestionnaire OfficeScan.

1. La console de gestion de l'antivirus Trend Micro est censée avoir été installée conformément aux instructions de Trend Micro et être en bon état de fonctionnement.
2. Durant l'installation de Trend Micro OfficeScan, procédez comme indiqué ci-dessous sur le serveur de la console de gestion de l'antivirus :
   a. Désélectionnez ***Enable firewall*** (Activer le pare-feu) dans la fenêtre ***Anti-virus Feature*** (Fonction antivirus).
   b. Sélectionnez ***No, Please do not enable assessment mode*** (Ne pas activer le mode d'évaluation) dans la fenêtre ***Anti-spyware Feature*** (Fonction anti-logiciels espions).
   c. Désélectionnez ***Enable web reputation policy*** (Activer la stratégie d'e-réputation) dans la fenêtre ***Web Reputation Feature*** (Fonction e-réputation).
3. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur tous les systèmes clients (acquisition, consultation et serveur INW) pour installer le logiciel antivirus.
4. Désactivez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Désactivation de la connexion de bouclage, page 6.
5. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs avant l'installation de l'antivirus, page 7.
6. Les certificats racine et intermédiaires suivants sont nécessaires pour l'installation sur les machines clientes acquisition, consultation et INW :
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
7. Répétez les sous-étapes suivantes pour installer les cinq certificats de niveau racine et intermédiaire énumérés à l'étape 6.
   a. Accédez à ***C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   REMARQUE : Dans INW, accédez à C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.
   b. Si le chemin de dossier indiqué ci-dessus n'est pas présent, obtenez manuellement les certificats de niveau racine et intermédiaire requis pour l'installation.
   c. Double-cliquez sur ***AddTrustExternalCARoot.crt*** pour l'installer sur les systèmes MLCL (acquisition, consultation et INW).
   d. Ouvrez le certificat, puis cliquez sur ***Install Certificate*** (Installer le certificat).
   e. Cliquez sur ***Next*** (Suivant) lorsque le ***Certificate Import Wizard*** (Assistant d'importation de certificat) apparaît.
   f. Dans la fenêtre ***Certificate Store***, sélectionnez ***Place all certificates in the following store*** (Placer tous les certificats sur le support suivant), puis cliquez sur ***Browse*** (Parcourir).
   g. Cochez ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Afficher les supports physiques > Autorités de certification racine de confiance > Ordinateur local), puis cliquez sur ***OK***.

h. Cliquez sur ***Next*** (Suivant) dans le ***Certificate Import Wizard*** (Assistant d'importation de certificat).

i. Cliquez sur ***Finish*** (Terminer). Le message ***The import was successful*** (Importation réussie) doit apparaître.

j. Répétez l'étape 7 pour les autres certificats énumérés à l'étape 6.

REMARQUE : Chaque certificat possède une date d'expiration. Lorsque le certificat expire, il doit être renouvelé et mis à jour sur les systèmes MLCL afin de s'assurer que l'agent OfficeScan fonctionne comme prévu.

Trend Micro OfficeScan - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée pour la version 12.0 et XG SP1)

1. Sélectionnez ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan - <nom du serveur> > Console Web OfficeScan).

REMARQUE : Sélectionnez ensuite ***Continue to this website (not recommended)*** (Rester sur ce site Internet [déconseillé]). Dans la fenêtre Security Alert (Alerte de sécurité), cochez ***In the future, do not show this warning*** (Ne plus afficher cet avertissement à l'avenir) et cliquez sur ***OK***.

2. Si vous recevez un certificat d'erreur indiquant qu'il ne s'agit pas d'un site de confiance, gérez vos certificats de manière à intégrer Trend Micro OfficeScan parmi les sites fiables.
3. Installez les additifs ***AtxEnc*** si le système vous y invite. L'écran Security Warning (Alerte de sécurité) s'affiche.
   a. Cliquez sur ***Install*** (Installer).
4. Entrez le nom d'utilisateur et le mot de passe et cliquez sur ***Log On*** (Se connecter).
5. Cliquez sur ***Update Now*** (Effectuer la mise à jour maintenant) pour installer de nouveaux widgets si le système vous y invite. Attendez que l'installation des nouveaux widgets soit terminée. L'écran Update is completed (Mise à jour terminée) s'affiche.
   a. Cliquez sur ***OK***.
6. Dans la barre de menus supérieure, cliquez sur ***Agents > Agent Installation > Remote*** (Agents > Installation d'un agent > À distance).
7. Installez les additifs ***AtxConsole*** si le système vous y invite. L'écran Security Warning (Alerte de sécurité) s'affiche.
   a. Cliquez sur ***Install*** (Installer).
8. Double-cliquez sur ***My Company*** (Ma société) dans la fenêtre ***Remote Installation*** (Installation distante). Tous les domaines sont répertoriés dans ***OfficeScan Server*** (Serveur OfficeScan).
9. Double-cliquez sur le domaine (exemple : INW) dans la liste. Tous les systèmes connectés au domaine apparaissent.

REMARQUE : Si des domaines ou des systèmes ne sont pas répertoriés dans la fenêtre ***Domains and Endpoints*** (Domaines et terminaux), consultez la section Résolution de problèmes des domaines ou systèmes non répertoriés dans la fenêtre Domains and Endpoints (Domaines et terminaux), page 74, pour les ajouter manuellement ou lancez directement l'installation depuis la machine cliente.

10. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) et cliquez sur ***Add*** (Ajouter).

11. Entrez le <domain name>\username (<nom de domaine>\nom d'utilisateur) et le mot de passe et cliquez sur ***Log on*** (Se connecter).
12. Sélectionnez les machines clientes (acquisition, consultation et serveur INW) une par une dans le volet ***Selected Endpoints*** (Terminaux sélectionnés) et cliquez sur ***Install*** (Installer).
13. Cliquez sur ***Yes*** (Oui) dans la zone de confirmation.
14. Cliquez sur ***OK*** dans la zone de message ***Number of agents to which notifications were sent*** (Nombre d'agents auxquels les notifications ont été envoyées).
15. Redémarrez toutes les machines clientes (acquisition, consultation et serveur INW), connectez-vous en tant qu'Administrateur ou membre de ce groupe sur toutes les machines clientes et attendez que l'icône Trend Micro OfficeScan présente dans la barre des tâches soit de couleur bleue avec une coche verte.
16. Cliquez sur le lien ***Log Off*** (Déconnexion) pour fermer la fenêtre ***OfficeScan Web Console*** (Console Web OfficeScan).

Configuration de la console Trend Micro OfficeScan pour la version 12.0

1. Cliquez sur ***Start > All Programs > TrendMicro OfficeScan server <servername> > OfficeScan Web Console*** (Démarrer > Tous les programmes > Serveur TrendMicro OfficeScan <nomduserveur> > Console Web OfficeScan). L'écran de connexion ***Trend Micro OfficeScan Login*** (Connexion à Trend Micro OfficeScan) s'affiche.
2. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur ***Login*** (Ouvrir une session). L'écran ***Summary*** (Résumé) s'affiche.
3. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
4. À gauche, sélectionnez le serveur ***OfficeScan***.
5. Parmi les options ***Settings*** *(Paramètres)*, sélectionnez ***Scan Settings*** *(Paramètres d'analyse)* ***> Manual Scan Settings*** *(Paramètres d'analyse manuelle)*. L'écran ***Manual Scan Settings*** (Paramètres d'analyse manuelle) s'affiche.
6. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
   - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
   - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
   - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
   - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
   - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
7. Cliquez sur l'onglet Scan Exclusion (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
   - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*

- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list*** (Liste d'exclusion de l'analyse [répertoires] > Exclure les répertoires dans lesquels les produits Trend Micro sont installés et sélectionner Ajouter le chemin à la liste d'exclusion des ordinateurs agents).
- ***Select Adds path*** (Sélectionner Ajouter le chemin vers) dans la liste déroulante sous ***Saving the officescan agent's exclusion list does the following:*** (L'enregistrement de la liste d'exclusion de l'agent officescan provoque l'action suivante :)
- Saisissez les fichiers **C:\Program Files (x86)\GE Healthcare\MLCL\, C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** et **G:** l'un après l'autre et cliquez sur ***Add*** (Ajouter).

8. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
9. Cliquez sur ***OK*** lorsque vous recevez le message suivant : ***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier.*** (La liste d'exclusions affichée sur cet écran remplacera la liste d'exclusions des agents ou domaines que vous avez sélectionnée dans l'arborescence du client). ***Do you want to proceed?*** *(Souhaitez-vous continuer ?)* s'affiche.
10. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Manual Scan Settings*** (Paramètres d'analyse manuelle).
11. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
12. À gauche, sélectionnez le serveur ***OfficeScan***.
13. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Real-time Scan Settings*** (Paramètres d'analyse > Paramètres d'analyse en temps réel). L'écran ***Real-time Scan Settings*** (Paramètres d'analyse en temps réel) s'affiche.
14. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Real-Time Scan Settings > Enable virus/malware scan*** *(Paramètres d'analyse en temps réel > Activer l'analyse antivirus/anti-malware).*
    - ***Real-Time Scan Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse en temps réel > Activer l'analyse anti-logiciels espions/anti-grayware).*
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings Only > Enable IntelliTrap*** *(Paramètres d'analyse antivirus/anti-logiciel malveillant uniquement > Activer IntelliTrap).*
15. Cliquez sur l'onglet Scan Exclusion (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*

- Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** et ***G:*** sont présents dans la ***Exclusion List*** (Liste d'exclusions).

16. Cliquez sur l'onglet ***Action***.
17. Conservez les paramètres par défaut et désélectionnez les options suivantes :
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected*** *(Virus/malware > Afficher un message de notification sur les terminaux lorsqu'un virus/malware est détecté).*
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected*** *(Logiciels espions/Grayware > Afficher un message de notification sur les terminaux lorsqu'un logiciel espion/grayware est détecté).*
18. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
19. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Real-time Scan Settings*** (Paramètres d'analyse en temps réel).
20. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
21. À gauche, sélectionnez le serveur ***OfficeScan***.
22. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Scheduled Scan Settings*** (Paramètres d'analyse > Paramètres d'analyse planifiée). L'écran ***Scheduled Scan Settings*** (Paramètres d'analyse planifiée) s'ouvre.
23. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scheduled Scan Settings > Enable virus/malware scan*** *(Paramètres d'analyse planifiée > Activer l'analyse antivirus/anti-malware).*
    - ***Scheduled Scan Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse planifiée > Activer l'analyse anti-logiciels espions/grayware).*
    - ***Schedule > Weekly, every Sunday, Start time:*** *(Planification > Hebdomadaire, tous les dimanches, Heure de début :)* ***00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
    - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
24. Cliquez sur l'onglet Scan Exclusion (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*

- Vérifiez que les chemins des dossiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***\ et ***G:***\ sont présents dans la Exclusion List (Liste d'exclusions).

25. Cliquez sur l'onglet ***Action***.
26. Conservez les paramètres par défaut et désélectionnez les options suivantes :
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected*** *(Virus/malware > Afficher un message de notification sur les terminaux lorsqu'un virus/malware est détecté).*
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected*** *(Logiciels espions/Grayware > Afficher un message de notification sur les terminaux lorsqu'un logiciel espion/grayware est détecté).*
27. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
28. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Scheduled Scan Settings*** (Paramètres d'analyse planifiée).
29. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
30. À gauche, sélectionnez le serveur ***OfficeScan***.
31. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Scan Settings > Scan Now Settings*** (Paramètres d'analyse > Paramètres d'analyse immédiate). L'écran ***Scan Now Settings*** (Paramètres d'analyse immédiate) s'affiche.
32. Cliquez sur l'onglet ***Target*** (Cible) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Now Settings > Enable virus/malware scan*** *(Paramètres d'analyse immédiate > Activer l'analyse antivirus/anti-malware).*
    - ***Scan Now Settings > Enable spyware/grayware scan*** *(Paramètres d'analyse immédiate > Activer l'analyse anti-logiciels espion/grayware).*
    - ***Files to Scan > File types scanned by IntelliScan*** *(Fichiers à analyser >Types de fichiers analysés par IntelliScan).*
    - ***Scan Settings > Scan compressed files*** *(Paramètres d'analyse > Analyser les fichiers compressés).*
    - ***Scan Settings > Scan OLE objects*** *(Paramètres d'analyse > Analyser les objets OLE).*
    - ***Virus/Malware Scan Settings only > Scan boot Area*** *(Paramètres d'analyse antivirus/anti-malware uniquement > Analyser la zone d'amorçage).*
    - ***CPU Usage > Low*** *(Utilisation de l'UC > Faible).*
33. Cliquez sur l'onglet ***Scan Exclusion*** (Exclusion de l'analyse) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Exclusion > Enable scan exclusion*** *(Exclusion de l'analyse > Activer l'exclusion de l'analyse).*
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types*** *(Exclusion de l'analyse > Appliquer les paramètres d'exclusion de l'analyse à tous les types d'analyses).*
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed*** *(Liste d'exclusion de l'analyse [répertoires]) > Exclure les répertoires dans lesquels les produits Trend Micro sont installés).*
    - Vérifiez que les fichiers ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***\ et ***G:***\

34. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
35. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Scan Now Settings*** (Paramètres d'analyse immédiate).
36. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
37. À gauche, sélectionnez le serveur ***OfficeScan***.
38. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Web Reputation Settings*** (Paramètres d'e-réputation). L'écran ***Web Reputation Settings*** (Paramètres d'e-réputation) s'affiche.
39. Cliquez sur l'onglet ***External Clients*** (Clients externes) et désélectionnez ***Enable Web reputation policy on the following operating systems*** (Activer la stratégie d'e-réputation sur les systèmes d'exploitation suivants) si vous avez sélectionné cette option pendant l'installation.

REMARQUE : Pour XG 12 SP1, cliquez sur l'onglet **External Agent** (Agent externe)

40. Cliquez sur l'onglet ***Internal Agents*** (Agents internes) et désélectionnez ***Enable Web reputation policy on the following operating systems*** (Activer la stratégie d'e-réputation sur les systèmes d'exploitation suivants) si vous avez sélectionné cette option pendant l'installation.
41. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
42. Cliquez sur ***Close*** pour fermer l'écran ***Web Reputation*** (E-réputation).
43. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
44. À gauche, sélectionnez le serveur ***OfficeScan***.
45. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Behavior Monitoring Settings*** (Paramètres de surveillance des comportements). L'écran ***Behavior Monitoring Settings*** (Paramètres de surveillance des comportements) s'affiche.
46. Désélectionnez les options ***Enable Malware Behavior Blocking*** (Activer le blocage des comportements de malware) et ***Enable Event Monitoring*** (Activer la surveillance des événements).
47. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
48. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Behavior Monitoring*** (Surveillance des événements).
49. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
50. À gauche, sélectionnez le serveur ***OfficeScan***.
51. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Device Control Settings*** (Paramètres de contrôle des périphériques). L'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques) s'affiche.
52. Cliquez sur l'onglet ***External Agents*** (Agents externes) et désélectionnez les options suivantes :
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access*** *(Afficher un message de notification sur les terminaux lorsqu'OfficeScan détecte un accès par un périphérique non autorisé).*
    - ***Block the AutoRun function on USB storage devices*** *(Bloquer la fonction AutoRun [exécution automatique] sur les périphériques de stockage USB).*
    - ***Enable Device Control*** *(Activer le contrôle des périphériques).*

53. Cliquez sur l'onglet ***Internal Agents*** (Agents internes) et désélectionnez les options suivantes :
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access*** *(Afficher un message de notification sur les terminaux lorsqu'OfficeScan détecte un accès par un périphérique non autorisé).*
    - ***Block the AutoRun function on USB storage devices*** *(Bloquer la fonction AutoRun [exécution automatique] sur les périphériques de stockage USB).*
    - *Enable Device Control (Activer le contrôle des périphériques).*
54. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
55. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques).
56. Parmi les options ***Settings*** (Paramètres), sélectionnez de nouveau ***Device Control Settings*** (Paramètres de contrôle des périphériques). L'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques) s'affiche.
57. Cliquez sur l'onglet ***External Agents*** (Agents externes) et désélectionnez ***Enable Device Control*** (Activer le contrôle des périphériques).
58. Cliquez sur l'onglet ***Internal Agents*** (Agents internes) et désélectionnez ***Enable Device Control*** (Activer le contrôle des périphériques).
59. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
60. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Device Control Settings*** (Paramètres de contrôle des périphériques).
61. Dans le volet situé à gauche, cliquez sur le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
62. À gauche, sélectionnez le serveur ***OfficeScan***.
63. Parmi les options ***Settings*** *(Paramètres)*, sélectionnez ***Privileges and Other Settings*** *(Privilèges et autres paramètres)*.
64. Cliquez sur l'onglet ***Privileges*** (Privilèges) et sélectionnez uniquement les options suivantes (les autres options doivent être désélectionnées) :
    - ***Scan Privileges > Configure Manual Scan Settings*** *(Privilèges d'analyse > Configurer les paramètres de l'analyse manuelle).*
    - ***Scan Privileges > Configure Real-time Scan Settings*** *(Privilèges d'analyse > Configurer les paramètres de l'analyse en temps réel).*
    - ***Scan Privileges > Configure Scheduled Scan Settings*** *(Privilèges d'analyse > Configurer les paramètres d'analyse planifiée).*
    - ***Proxy Setting Privileges > Allow the agent user to configure proxy settings*** *(Privilèges de paramètre proxy > Autoriser l'utilisateur agent pour configurer les paramètres proxy).*
    - ***Uninstallation > Requires a password*** *(Désinstallation > Nécessite un mot de passe).* Saisissez un mot de passe valide et confirmez-le.
    - ***Unload and Unlock > Requires a password*** *(Décharger et déverrouiller > Nécessite un mot de passe).* Saisissez un mot de passe valide et confirmez-le.
65. Cliquez sur l'onglet ***Other Settings*** (Autres paramètres).
66. Décochez toutes les options.

REMARQUE : Les options suivantes doivent impérativement être désactivées.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services*** *(Auto-protection de l'agent OfficeScan > Protéger les services de l'agent OfficeScan).*

- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder*** *(Auto-protection de l'agent OfficeScan > Protéger les fichiers présents dans le dossier d'installation de l'agent OfficeScan).*
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys*** *(Auto-protection de l'agent OfficeScan > Protéger les clés de registre de l'agent OfficeScan).*
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes*** *(Auto-protection de l'agent OfficeScan > Protéger les processus de l'agent OfficeScan).*

67. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
68. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Privileges and Other Settings*** (Privilèges et autres paramètres).
69. Dans le volet supérieur, sélectionnez le lien ***Agents > Agent Management*** (Agents > Gestion des agents).
70. À gauche, sélectionnez le serveur ***OfficeScan***.
71. Parmi les options ***Settings*** (Paramètres), sélectionnez ***Additionnal Service Settings*** (Paramètres de service supplémentaires).
72. Désélectionnez l'option ***Enable service on the following operating systems*** (Activer le service sur les systèmes d'exploitation suivants).

REMARQUE : Pour la version XG SP1, décochez toutes les options

73. Cliquez sur ***Apply to All Agents*** (Appliquer à tous les agents).
74. Cliquez sur ***Close*** (Fermer) pour fermer l'écran ***Additional Service Settings*** (Paramètres de service supplémentaires).
75. Dans le volet supérieur, sélectionnez le lien ***Agents > Global Agent Settings*** (Agents > Paramètres agent globaux).
76. Cochez uniquement les options suivantes et désélectionnez les autres options :
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Paramètres d'analyse des fichiers compressés volumineux > Ne pas analyser les fichiers du fichier compressé si la taille est supérieure à 2 Mo). Suivez cette option pour ***Real-Time Scan*** (analyse en temps réel) et ***Manual Scan/Schedule Scan/Scan Now*** (analyse manuelle/analyse planifiée/analyse immédiate).
    - ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files*** *(Paramètres d'analyse des fichiers compressés volumineux > Dans un fichier compressé, analyser uniquement les 100 premiers fichiers).* Suivre cette option pour ***Real-Time Scan*** (analyse en temps réel) et ***Manual Scan/Schedule Scan/Scan Now*** (analyse manuelle/analyse planifiée/analyse immédiate).
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan*** *(Paramètres de numérisation > Exclure le dossier de base de données du serveur OfficeScan de l'analyse en temps réel).*
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans*** *(Paramètres d'analyse > Exclure les dossiers et fichiers du serveur Microsoft Exchange de l'analyse).*
77. Cliquez sur ***Save*** (Enregistrer).
78. Dans le volet supérieur, cliquez sur le lien ***Updates > Agents > Manual Updates*** (Mises à jour > Agents > Mises à jour manuelles).
79. Sélectionnez ***Manually Select agents*** (Sélectionner les agents manuellement) et cliquez sur ***Select*** (Sélectionner).
80. Double-cliquez sur le nom de domaine correspondant dans ***OfficeScan Server*** (Serveur OfficeScan).

81. Sélectionnez les systèmes clients un par un et cliquez sur ***Initiate Update*** (Lancer la mise à jour).
82. Cliquez sur ***OK*** dans la zone de message.
83. Cliquez sur le lien ***Log Off*** (Déconnexion) et fermez la fenêtre OfficeScan Web Console (Console OfficeScan Web).

Après l'installation de Trend Micro OfficeScan

1. Activez la connexion de bouclage. Pour plus d'informations, reportez-vous à la section Activation de la connexion de bouclage, page 6.
2. Configurez le service Explorateur d'ordinateurs. Pour plus d'informations, reportez-vous à la section Configuration du service Explorateur d'ordinateurs après l'installation de l'antivirus, page 8.

Résolution de problèmes des domaines ou systèmes non répertoriés dans la fenêtre Domains and Endpoints (Domaines et terminaux)

Dans le cadre des méthodes d'installation « Push » pour Trend Micro OfficeScan Client/Server Édition 11.0 SP1 et Trend Micro OfficeScan Client/Server Édition XG 12.0, les domaines et les systèmes doivent être répertoriés pour lancer l'installation du système. Ces étapes vous donnent deux méthodes pour installer le logiciel antivirus sur les machines clientes (acquisition, consultation et INW).

Pour la version 11.0 SP1, reportez-vous à la section Trend Micro OfficeScan - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée pour la version 11.0 SP1), page 55.
Pour la version 12.0, reportez-vous à la section Trend Micro OfficeScan - Étapes de déploiement d'une nouvelle installation (Méthode d'installation « Push » préférée pour la version 12.0), page 66.

1. Utilisez l'adresse IP des machines clientes (acquisition, consultation et INW) dans la console de gestion et effectuez les actions suivantes :
   a. Saisissez l'IP de chaque système client dans la zone ***Search for endpoints*** (Rechercher les terminaux) l'une après l'autre, puis appuyez sur ***Enter*** (Entrer).
   b. Saisissez le ***<domain name>\username*** (<nom de domaine>\nom d'utilisateur) et le mot de passe puis cliquez sur ***Log on*** (Se connecter).
   c. Choisissez l'une des étapes suivantes en fonction de la version de Trend Micro que vous possédez :
      i. Pour la version 11.0 SP1, revenez à l'étape 10 de la page 47.
      ii. Pour les versions 12.0 et XG SP1, revenez à l'étape 10 de la page 56.
2. Si vous ne connaissez pas l'adresse IP des systèmes ou que la méthode précédente n'a pas fonctionné, allez sur chaque machine client (acquisition, consultation et serveur INW) et effectuez les actions suivantes :
   a. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur toutes les machines clientes.
   b. Cliquez sur ***Start > Run*** (Démarrer > Exécuter).
   c. Entrez ***\\<Anti-Virus Management Console_server_IP_address>*** et appuyez sur la touche ***Entrée***. Saisissez le nom d'utilisateur et le mot de passe de l'administrateur lorsque le système vous y invite.

d. Allez sur ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** et double-cliquez sur ***AutoPcc.exe***. Saisissez le nom d'utilisateur et le mot de passe de l'administrateur lorsque le système vous y invite.

e. Redémarrez les systèmes clients une fois l'installation terminée.

f. Connectez-vous en tant qu'**Administrator** (Administrateur) ou membre de ce groupe sur toutes les machines clientes et attendez que l'icône Trend Micro OfficeScan présente dans la barre des tâches soit de couleur bleue.

g. Choisissez l'une des étapes suivantes en fonction de la version de Trend Micro que vous possédez :

   i. Pour la version 11.0 SP1, reportez-vous à la section Configuration de la console Trend Micro OfficeScan pour la version 11.0 SP1, page 56.

   ii. Pour la version 12.0, reportez-vous à la section Configuration de la console Trend Micro OfficeScan pour la version 12.0 et XG SP1, page 67.