



10.0

Worry-Free™ Business Security Éditions Standard et Advanced Service Pack 1

Guide d'installation et de mise à niveau

Securing Your Journey to the Cloud



Protected Cloud



Web Security

Trend Micro Incorporated se réserve le droit de modifier ce document et le produit décrit ici sans notification préalable. Avant d'installer et d'utiliser le produit, veuillez consulter les fichiers Lisez-moi, les notes de mise à jour et/ou la dernière version de la documentation utilisateur applicable que vous trouverez sur le site Web de Trend Micro à l'adresse suivante :

<http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx>

Trend Micro, le logo t-ball de Trend Micro, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan et ScanMail sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de produits ou de sociétés peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Copyright © 2019 Trend Micro Incorporated. Tous droits réservés.

Document n° : WFEM108678/190617

Date de publication : Juin 2019

Protégé par le brevet américain n°: 5 951 698 et 7 188 369

Cette documentation présente les fonctionnalités principales du produit et/ou fournit les instructions d'installation pour un environnement de production. Lisez attentivement cette documentation avant d'installer ou d'utiliser le produit.

Pour plus d'informations concernant l'utilisation des fonctionnalités spécifiques de produit, consultez notre Trend Micro Centre d'aide en ligne et/ou notre Trend Micro base de connaissances.

Trend Micro cherche constamment à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Évaluez cette documentation sur le site Web suivant :

<http://www.trendmicro.com/download/documentation/rating.asp>

Table des matières

Préface

Préface	v
Documentation relative à Worry-Free Business Security	vi
Public visé	vii
Conventions typographiques du document	vii

Chapitre 1: Préparation de l'installation et de la mise à niveau

Éditions du produit	1-2
Licences, enregistrement et activation	1-3
Le réseau Worry-Free Business Security	1-6
Serveur Security Server	1-6
Agents	1-8
Console Web	1-8

Chapitre 2: Installation de Security Server

Configuration requise pour l'installation et la mise à niveau ..	2-2
Considérations d'installation de Security Server	2-2
Conditions requises pour la prise en charge d'IPv6 sur Security Server	2-2
Emplacement du serveur Security Server	2-3
Nombre de clients	2-4
Trafic réseau	2-4
Serveur dédié	2-6
Problèmes de compatibilité	2-6
Ports Worry-Free Business Security	2-8
Liste de contrôle de l'installation	2-9
Installation de Security Server	2-13
Phase 1 : Démarrage de l'installation de Security Server	2-16

Phase 2 : Configuration des paramètres selon le type d'installation	2-26
Configuration des paramètres pour une installation type ou minimale	2-26
Configuration des paramètres d'installation personnalisée	2-32
Phase 3 : processus d'installation	2-54
Installation de plusieurs serveurs Security Server en mode silencieux	2-58
Enregistrement d'une session d'installation	2-58
Démarrage de l'installation en mode silencieux	2-60
Vérification de l'installation	2-60

Chapitre 3: Mise à niveau du serveur Security Server et des agents

Configuration requise pour l'installation et la mise à niveau ..	3-2
Éléments à prendre en compte pour la mise à niveau	3-2
Exigences IPv6 pour les mises à niveau	3-2
Pratiques recommandées pour la mise à niveau	3-3
Mises à niveau des versions antérieures	3-4
Méthode de mise à niveau 1 : Mise à niveau à l'aide du pack d'installation	3-5
Méthode de mise à niveau 2 : déplacement des agents Security Agent vers le serveur Security Server 10.0 Service Pack 1	3-7
Mises à niveau vers la version complète ou l'Édition Advanced	3-9
Mises à niveau vers la version complète ou Advanced	3-10

Annexe A: Assistance technique

Ressources de dépannage	A-2
Utilisation du portail d'assistance	A-2
Encyclopédie des menaces	A-2

Comment contacter Trend Micro	A-3
Optimisation de la demande d'assistance	A-4
Envoi de contenu suspect à Trend Micro	A-5
services de réputation de messagerie (Email Reputation Services)	A-5
Services de File Reputation	A-5
Services de réputation de sites Web	A-5
Autres ressources	A-6
Centre de téléchargement	A-6
Commentaires relatifs à la documentation	A-6

Index

Index	IN-1
-------------	------

Préface

Préface

Bienvenue dans le *Guide d'installation et de mise à niveau* de Trend Micro™ Worry-Free™ Business Security. Ce document aborde les exigences et procédures relatives à :

- L'installation de Security Server
- Mise à niveau du serveur Security Server et des agents

Pour plus d'informations sur l'installation des agents, voir le *Manuel de l'administrateur*.

Documentation relative à Worry-Free Business Security

La documentation relative à Worry-Free Business Security inclut les éléments suivants :

TABLEAU 1. Documentation relative à Worry-Free Business Security

DOCUMENTATION	DESCRIPTION
Guide d'installation et de mise à niveau	document PDF qui aborde les éléments requis et les procédures d'installation du serveur Security Server, ainsi que les informations nécessaires pour la mise à niveau du serveur et des agents.
Manuel de l'administrateur	document PDF qui aborde les informations relatives au démarrage, les procédures d'installation client et l'administration du serveur Security Server et des agents.
Aide	Fichiers HTML compilés au format WebHelp ou CHM contenant des descriptions de procédures, des conseils d'utilisation et des informations relatives aux champs
Fichier Lisez-moi	Contient une liste des problèmes connus et les étapes d'installation de base. Il peut aussi contenir des informations relatives au produit qui n'ont pas pu être intégrées à temps à l'aide ou à la documentation imprimée.
Base de connaissances	Base de données en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les dernières informations sur les problèmes connus identifiés pour les produits. Pour accéder à la base de connaissances, consultez le site Web suivant: http://esupport.trendmicro.com

Téléchargez la dernière version des documents PDF et du fichier Lisez-moi à l'adresse suivante:

<http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx>

Public visé

La documentation relative à Worry-Free Business Security est destinée aux utilisateurs suivants :

- **Administrateurs de sécurité** : responsable de l'administration de Worry-Free Business Security, y compris de la gestion et de l'installation de Security Server et de l'agent. Ces utilisateurs doivent disposer d'une connaissance approfondie de la mise en réseau et de la gestion des serveurs.
- **Utilisateurs finaux** : utilisateurs qui ont installé Security Agent sur leurs ordinateurs. Leur niveau de compétence informatique varie: débutant, expérimenté, etc.

Conventions typographiques du document

Pour faciliter la recherche et la compréhension des informations, la documentation relative à Worry-Free Business Security utilise les conventions suivantes :

TABLEAU 2. Conventions typographiques du document

NOMENCLATURE	DESCRIPTION
MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets, options et tâches
<i>Italique</i>	Références à d'autres documents ou composants de nouvelles technologies
<Texte>	Indique que le texte entre crochets doit être remplacé par les données réelles. Par exemple, C:\Program Files \<file_name> peut correspondre à C:\Program Files \sample.jpg.

NOMENCLATURE	DESCRIPTION
 Remarque	Introduit des remarques ou recommandations relatives à la configuration
 Conseil	Fournit des informations sur les pratiques recommandées concernant Trend Micro
 AVERTISSEMENT!	Fournit des avertissements sur les activités pouvant nuire aux ordinateurs de votre réseau

Chapitre 1

Préparation de l'installation et de la mise à niveau

Ce chapitre explique les préparations nécessaires avant l'installation ou la mise à niveau de Worry-Free™ Business Security.

Éditions du produit

Trend Micro propose les éditions suivantes :

- Worry-Free Business Security **Standard** : conçue pour protéger les endpoints (postes de travail, ordinateurs portables et serveurs) sur votre réseau local. Cette édition inclut le pare-feu et le scan antivirus/anti-programme espion. Elle inclut également le support technique, les téléchargements de fichiers de signatures de programmes malveillants/virus, le scan en temps réel et les mises à jour du programme pour une durée d'un an.
- Worry-Free Business Security **Advanced** : conçue pour protéger les endpoints et les serveurs Microsoft Exchange sur votre réseau. Outre les fonctionnalités de Worry-Free Business Security Standard, cette édition inclut l'anti-spam, le filtrage de contenu, la prévention contre la perte de données et le blocage des pièces jointes.

Le tableau ci-dessous répertorie les fonctions prises en charge par chaque édition.

TABLEAU 1-1. Fonctions disponibles par édition de produit

FONCTIONNALITÉS	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Mises à jour des composants	Oui	Oui
Contrôle des dispositifs	Oui	Oui
Antivirus/anti-programme espion	Oui	Oui
Pare-feu.	Oui	Oui
Réputation de sites Web	Oui	Oui
Filtrage d'URL	Oui	Oui
Apprentissage automatique prédictif	Oui	Oui

FONCTIONNALITÉS	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Surveillance des comportements	Oui	Oui
Outils utilisateur	Oui	Oui
Scan de la messagerie (POP3)	Oui	Oui
Anti-Spam (POP3)	Oui	Oui
Scan de la messagerie (IMAP)	Non	Oui
Anti-Spam (IMAP)	Non	Oui
Filtrage du contenu des messages électroniques	Non	Oui
Prévention contre la perte de données de message électronique	Non	Oui
Blocage des pièces jointes	Non	Oui

Licences, enregistrement et activation

Lorsque vous achetez Worry-Free Business Security, vous recevez une licence pour le(s) produit(s) et un contrat de maintenance standard. Le contrat de maintenance standard est un contrat entre votre organisation et Trend Micro concernant votre droit à bénéficier d'une assistance technique et de mises à jour de produits moyennant le paiement des frais en vigueur.

La licence concédée avec les logiciels Trend Micro comprend généralement l'accès aux mises à jour des produits, aux fichiers de signatures, ainsi qu'une assistance technique de base pendant une période d'un (1) an à compter de la date d'achat. Après la première année, vous devez renouveler le contrat de maintenance tous les ans moyennant les frais de maintenance alors en vigueur chez Trend Micro.



Remarque

Votre contrat de maintenance expire, mais ce n'est pas le cas de votre contrat de licence. Lorsque votre contrat de maintenance expire, les scans ont toujours lieu, mais vous n'êtes plus en mesure de mettre à jour les fichiers de signatures de virus/programmes malveillants, le moteur de scan ni les fichiers de programme (même manuellement). Vous ne pouvez plus non plus bénéficier de l'assistance technique Trend Micro.

Enregistrez et activez votre licence Worry-Free Business Security pour activer toutes les fonctionnalités du produit.

Clé d'enregistrement

Une clé d'enregistrement est fournie avec votre achat de Worry-Free Business Security. Elle comporte 22 caractères (tirets compris) et est présentée au format suivant :

Worry-Free Business Security Standard : CS-xxxx-xxxxx-xxxxx-xxxxx

Worry-Free Business Security Advanced : CM-xxxx-xxxxx-xxxxx-xxxxx

Utilisez une clé d'enregistrement complète pour enregistrer Worry-Free Business Security sur le site Web de Trend Micro à l'adresse <https://clp.trendmicro.com>.

Code d'activation

Après l'enregistrement, vous recevrez un code d'activation de version complète par courrier électronique. Un code d'activation contient 37 caractères (tirets compris) et est présenté au format suivant :

Worry-Free Business Security Standard : CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Worry-Free Business Security Advanced : CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Au cours de l'installation de Security Server, saisissez le code d'activation lorsque vous y êtes invité. Si vous laissez le champ vide, Worry-Free Business Security installe la version d'évaluation de 30 jours. Effectuez la mise à niveau vers la version complète avant l'expiration de la version d'évaluation.

État de la licence

Le tableau suivant répertorie les fonctions prises en charge en fonction de l'état de la licence.

TABLEAU 1-2. État de la licence

FONCTION	LICENCE COMPLÈTE	VERSION D'ÉVALUATION (30 JOURS)	EXPIRÉ
Notification de l'expiration	Oui	Oui	Oui
Mises à jour des composants	Oui	Oui	Non
Mises à jour du programme	Oui	Oui	Non
Assistance technique	Oui	Non	Non
Scan en temps réel	Oui	Oui	Oui, mais le scan en temps réel utilisera des composants obsolètes

Lorsqu'un code d'activation de version complète expire, vous ne pouvez plus télécharger de mises à jour du moteur de scan ou des fichiers de signatures. Cependant, à la différence d'un code d'activation de version d'évaluation, lorsqu'un code d'activation de version complète expire, toutes les configurations existantes et autres paramètres restent applicables. Cela permet de conserver un niveau de protection au cas où vous laisseriez accidentellement expirer votre licence.

Vous pouvez renouveler une version complète de Worry-Free Business Security en achetant un renouvellement de votre contrat de maintenance. Vous avez besoin d'un code d'activation pour installer les versions complètes.

Si vous avez des questions à propos du processus d'enregistrement, veuillez consulter le site d'assistance de Trend Micro à l'adresse :

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326>

Le réseau Worry-Free Business Security

Worry-Free Business Security comprend les éléments suivants :

- *Serveur Security Server à la page 1-6*
- *Agents à la page 1-8*
- *Console Web à la page 1-8*

Serveur Security Server

Security Server est au cœur de la solution Worry-Free Business Security. Le serveur Security Server héberge la console Web, la console Web de gestion centralisée pour la solution Worry-Free Business Security. Security Server installe les agents sur les clients du réseau et, avec ces agents, établit une relation agent-serveur. Security Server permet d'afficher les informations relatives à l'état de sécurité, d'afficher les agents, de configurer la sécurité système et de télécharger des composants à partir d'un emplacement centralisé. Security Server contient aussi une base de données dans laquelle il stocke les journaux des menaces Web détectées qui lui sont signalées par les agents.

Security Server exécute les tâches essentielles suivantes :

- Il installe, surveille et gère les agents.
- Il télécharge la plupart des composants dont les clients ont besoin. Par défaut, le serveur Security Server télécharge les composants depuis le serveur ActiveUpdate de Trend Micro, puis les distribue aux agents.

Serveur de scan

Le serveur Security Server possède un service dénommé Scan Server (Serveur de scan), qui est installé automatiquement lors de l'installation du serveur Security Server. Il n'est ainsi pas nécessaire de l'installer séparément. Le serveur de scan s'exécute sous le nom de processus iCRCService.exe et s'affiche sous l'intitulé **Service Trend Micro Smart Scan** dans Microsoft Management Console.

Lorsque des agents Security Agent utilisent une méthode de scan dénommée **smart scan**, le serveur de scan optimise leur exécution. Le processus smart scan peut être décrit comme suit :

- L'agent Security Agent analyse la présence de menaces de sécurité sur le client à l'aide de **Signatures de l'agent Smart Scan**, une version légère du fichier de signatures de virus traditionnel. Signatures de l'agent Smart Scan contient la plupart des signatures de menaces présentes dans le fichier de signatures de virus.
- Un agent Security Agent dans l'impossibilité de déterminer le risque du fichier lors du scan vérifie ce risque en envoyant une requête au serveur de scan. Le serveur de scan vérifie le risque à l'aide de **Signatures Smart Scan**, qui contient les signatures de menaces non disponibles sur Signatures de l'agent Smart Scan.
- Security Agent met en mémoire cache le résultat de la requête fournie par le serveur de scan afin d'améliorer ses performances.

En hébergeant certaines des définitions de menaces, le serveur de scan permet de réduire la consommation de bande passante des agents Security Agent lors du téléchargement des composants. Au lieu de télécharger le fichier de signatures de virus, les agents Security Agent téléchargent signatures de l'agent Smart Scan, qui est d'une taille considérablement inférieure.

Lorsque les agents Security Agent ne peuvent pas se connecter au serveur de scan, ils envoient leurs requêtes de scan à Trend Micro Smart Protection Network, qui possède la même fonction que le serveur de scan.

Il est impossible de désinstaller le serveur de scan séparément du serveur Security Server. Si vous ne souhaitez pas utiliser le serveur de scan :

1. Sur l'ordinateur de Security Server, ouvrez Microsoft Management Console et désactivez **Service Trend Micro Smart Scan**.
2. Dans la console Web, basculez les agents Security Agent en mode de scan traditionnel en accédant à **Administration > Paramètres généraux > Poste de travail/serveur** et en sélectionnant l'option **Désactiver le service Smart Scan**.

Agents

Les agents protègent les clients contre les menaces de sécurité. Les clients incluent les postes de travail, les serveurs et les serveurs Microsoft Exchange. Les agents Worry-Free Business Security sont :

TABLEAU 1-3. Agents Worry-Free Business Security

AGENT	DESCRIPTION
Security Agent	Protège les postes de travail et les serveurs des menaces de sécurité et des intrusions
Messaging Security Agent (Advanced uniquement)	Protège les serveurs Microsoft Exchange contre les menaces de sécurité liées à la messagerie

Un agent dépend du serveur Security Server à partir duquel il a été installé. L'agent envoie les informations relatives à l'état et aux événements en temps réel pour fournir à Security Server les informations les plus récentes concernant le client. Les agents signalent des événements tels que la détection d'une menace, le démarrage, l'arrêt, le lancement d'un scan et la réalisation d'une mise à jour.

Console Web

La console Web est le point central pour la surveillance des agents Security Agent sur le réseau de l'entreprise. Elle présente des paramètres et des valeurs par défaut que vous pouvez configurer en fonction de vos spécifications et exigences de sécurité. La console Web utilise des technologies Internet standard telles que Java, CGI, HTML et HTTP.

Utilisez la console Web pour :

- Déployer des agents sur les endpoints ;
- Organiser les agents par groupes logiques pour les configurer et les gérer tous ensemble ;
- Configurer les paramètres de produits et exécuter un scan manuel sur les endpoints ;

- Recevoir des notifications et consulter les journaux d'activité liées aux menaces ;
- Recevoir des notifications et envoyer des alertes d'épidémies par email lorsque des menaces sont détectées sur les endpoints.

Chapitre 2

Installation de Security Server

Ce chapitre fournit des informations que vous devrez connaître afin d'installer Security Server.

Configuration requise pour l'installation et la mise à niveau

Visitez le site Web suivant pour obtenir une liste complète des configurations requises pour une installation ou une mise à niveau :

<http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx>

Considérations d'installation de Security Server

Tenez compte des points suivants lors de l'installation de Security Server :

- *Conditions requises pour la prise en charge d'IPv6 sur Security Server à la page 2-2*
- *Emplacement du serveur Security Server à la page 2-3*
- *Nombre de clients à la page 2-4*
- *Trafic réseau à la page 2-4*
- *Serveur dédié à la page 2-6*
- *Problèmes de compatibilité à la page 2-6*

Conditions requises pour la prise en charge d'IPv6 sur Security Server

Les conditions requises pour la prise en charge d'IPv6 dans le serveur Security Server sont les suivantes :

- Si le serveur peut gérer les agents IPv4 et IPv6, il doit contenir les adresses IPv4 et IPv6 et doit être identifié par son nom d'hôte. Si un serveur est identifié par son adresse IPv4, les agents IPv6 purs ne peuvent pas s'y connecter. La même erreur se produit si les clients utilisant exclusivement IPv4 se connectent à un serveur identifié par ses adresses IPv6.

- Si le serveur ne gère que des agents IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6. Lorsque le serveur est identifié par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.
- Vérifiez que l'adresse IPv6 ou IPv4 de l'ordinateur hôte peut être récupérée en utilisant, par exemple, la commande « `ping` » ou « `nslookup` ».
- Si vous installez le serveur Security Server sur un ordinateur IPv6 pur, installez un serveur proxy à double pile qui peut convertir les adresses IPv4 et IPv6 (par exemple, DeleGate). Positionnez le serveur proxy entre le serveur Security Server et Internet pour permettre au serveur de se connecter aux services hébergés de Trend Micro, tels que le serveur ActiveUpdate, le site Web d'enregistrement en ligne et Smart Protection Network.

Emplacement du serveur Security Server

Worry-Free Business Security s'adapte à un grand nombre d'environnements réseau. Par exemple, vous pouvez placer un pare-feu entre Trend Micro Security Server et les clients exécutant Security Agent ou installer à la fois Trend Micro Security Server et tous les clients derrière un pare-feu réseau unique.

Si vous gérez plusieurs sites, il est conseillé d'installer Security Server sur le site principal, ainsi que sur chaque site géré, pour réduire l'utilisation de la bande passante entre le site principal et les sites gérés et pour accélérer les taux de déploiement des modèles.

Si le pare-feu de Windows est activé sur les clients, Worry-Free Business Security l'ajoute automatiquement à la liste d'exceptions.



Remarque

Si un pare-feu est situé entre Trend Micro Security Server et ses clients, vous devez configurer le pare-feu pour autoriser le trafic entre le port d'écoute du client et le port d'écoute de Trend Micro Security Server.

Nombre de clients

Un client est un ordinateur sur lequel vous prévoyez d'installer un agent Security Agent ou Messaging Security Agent. Cela inclut les postes de travail, les serveurs, les ordinateurs portables, y compris ceux qui appartiennent aux utilisateurs qui travaillent à distance.

Une seule installation de Security Server peut gérer jusqu'à 2 500 clients. Si votre nombre de clients est supérieur, Trend Micro vous suggère d'installer plus d'un serveur Security Server.

Trafic réseau

Worry-Free Business Security génère un trafic réseau lorsque le serveur Security Server et les agents communiquent.

Security Server et le serveur de scan génèrent du trafic dans les situations suivantes :

- Notification des agents à propos des changements de configuration qui ont eu lieu
- Notification des agents de télécharger des composants mis à jour
- Connexion au serveur ActiveUpdate de Trend Micro afin de vérifier et de télécharger les composants mis à jour
- Réponse aux requêtes de scan envoyées par les agents utilisant smart scan
- Envoi d'une sauvegarde à Trend Micro Smart Protection Network

Les agents génèrent du trafic dans les situations suivantes :

- Démarrage
- Arrêt
- Génération des journaux
- Exécution de mises à jour programmées
- Exécution de mises à jour manuelles (« Mettre à jour »)
- Connexion au serveur de scan pour les requêtes de scan

**Remarque**

À l'exception des mises à jour, toutes les autres actions génèrent un niveau de trafic négligeable.

Trafic réseau pendant les mises à jour de composants

Lorsqu'il met à jour un composant, Security Server génère un trafic réseau important. Pour réduire le trafic réseau généré au cours des mises à jour des composants, Security Server réalise une duplication des composants. Au lieu de télécharger un fichier de signatures complet mis à jour, Security Server télécharge uniquement les fichiers de signatures «[°]incrémentiels» (versions moins volumineuses du fichier de signatures complet) puis les fusionne avec l'ancien fichier de signatures une fois le téléchargement effectué.

Un serveur Security Server mis à jour régulièrement télécharge uniquement le fichier de signatures incrémentiel. Sinon, il télécharge le fichier de signatures complet.

Trend Micro publie régulièrement de nouveaux fichiers de signatures. Trend Micro publie également un nouveau fichier de signatures dès la découverte d'un virus/programme malveillant destructeur circulant activement.

Utilisation des agents de mise à jour pour réduire la bande passante du réseau

Si vous identifiez des sections de votre réseau entre les agents Security Agent et le serveur Security Server comme étant « à faible bande passante » ou « à trafic élevé », vous pouvez décider que les agents agissent comme sources de mise à jour (agents de mise à jour) pour d'autres agents. Cela aide à répartir

la charge de travail en ce qui concerne le déploiement des composants vers tous les agents.

Par exemple, si votre réseau est segmenté par emplacement et si le lien réseau entre les segments présente un trafic élevé, Trend Micro recommande d'autoriser au moins un agent Security Agent sur chaque segment à agir comme agent de mise à jour.

Serveur dédié

Lors de la sélection du client pour héberger le serveur Worry-Free Business Security, tenez compte des éléments suivants :

- La charge du processeur que le client doit gérer
- Si le client assure d'autres fonctions

Si le client cible assure d'autres fonctions, choisissez un client qui n'exécute pas d'applications stratégiques ou consommant beaucoup de ressources.

Problèmes de compatibilité

Cette section évoque les problèmes de compatibilité pouvant survenir avec certaines applications tierces. Reportez-vous toujours à la documentation de toutes les applications tierces installées sur le même ordinateur que celui sur lequel vous souhaitez installer Security Server et les autres composants Worry Free.

Autres logiciels de sécurité de terminaux

Avant d'installer le serveur Security Server, Trend Micro recommande de supprimer manuellement les autres logiciels de sécurité d'endpoints de l'ordinateur cible, car ceux-ci peuvent bloquer l'installation ou affecter les performances du serveur Security Server après l'installation.

Applications de sécurité dans SBS et EBS 2008

Worry-Free Business Security est compatible avec Windows Small Business Server (SBS) 2008 et avec Windows Essential Business Server (EBS) 2008.

Toutefois, certaines applications de sécurité dont l'installation ou la gestion se font à partir de ces systèmes d'exploitation peuvent être à l'origine de conflits avec Worry-Free Business Security. C'est la raison pour laquelle vous devrez peut-être supprimer ces applications de sécurité.

Messaging Security Agent et Forefront

Messaging Security Agent ne peut pas être installé sur les serveurs Microsoft Exchange disposant de Forefront (Microsoft Forefront Security for Exchange Server). Désinstallez Forefront et assurez-vous que le service Microsoft Exchange Information Store est démarré avant l'installation de Messaging Security Agent.

Messaging Security Agent et Microsoft Server Enterprise

Messaging Security Agent ne prend pas en charge certaines fonctionnalités de Microsoft Exchange Server Enterprise, telles que le Groupe de disponibilité de données (DAG).

Agents Security Agent et Windows Defender

L'installation de l'agent Security Agent désactive Windows Defender.

Bases de données

Les performances des applications qui accèdent à ces bases de données risquent d'être diminuées à cause du scan de bases de données. Trend Micro recommande d'exclure les bases de données et leurs dossiers de sauvegarde du scan en temps réel. Si vous avez besoin de scanner une base de données, exécutez un scan manuel ou programmez un scan en dehors des heures de pointe pour réduire l'impact du scan.

Autres applications de pare-feu

Trend Micro recommande la suppression ou la désactivation des autres applications de pare-feu avant d'installer le pare-feu Worry-Free Business Security, y compris :

- Windows Internet Connection Firewall (ICF)
- Windows Firewall (WF)

Toutefois, si vous souhaitez utiliser ICF ou tout autre pare-feu tiers, ajoutez les ports d'écoute de Trend Micro Security Server à la liste des exceptions du

pare-feu (voir *Ports Worry-Free Business Security à la page 2-8* pour obtenir des informations sur les ports d'écoute puis consultez votre documentation sur le pare-feu pour obtenir des informations détaillées sur la configuration des listes d'exceptions).

Ports Worry-Free Business Security

Worry-Free Business Security utilise les ports suivants :

- **Port d'écoute du serveur (port HTTP)** : Utilisé pour accéder au serveur Security Server. Par défaut, Worry-Free Business Security utilise l'un des ports suivants :
 - **Site Web du serveur IIS par défaut** : le même numéro de port TCP que votre serveur HTTP.
 - **Site Web virtuel du serveur IIS** : 8059
 - **Serveur Apache** : 8059
- **Port d'écoute client** : numéro de port généré de façon aléatoire par le biais duquel les agents Security Agent et Messaging Security Agent reçoivent les commandes du serveur Security Server.

Vous pouvez uniquement modifier les ports d'écoute au cours de l'installation.



AVERTISSEMENT!

Les cyber criminels d'aujourd'hui utilisent HTTP et dirigent leurs attaques vers les ports 80 et/ou 8080 – fréquemment utilisés dans la plupart des entreprises comme ports TCP par défaut pour les communications HTTP. Si votre entreprise utilise actuellement l'un de ces ports comme port HTTP, Trend Micro vous recommande d'utiliser un autre numéro de port.



Remarque

Pour connaître les ports utilisés par vos agents Security Agent pour se connecter au serveur de scan, ouvrez le fichier SSCFG.ini dans le dossier d'installation du serveur.

- **Ports du serveur de scan** : utilisés par le serveur de scan pour communiquer avec les agents Security Agent pour les requêtes de scan.

TABLEAU 2-1. Ports du serveur de scan

TYPE DE PORT	IIS PAR DÉFAUT	IIS VIRTUEL	SERVEUR APACHE PRÉINSTALLÉ	NOUVELLE INSTALLATION D'APACHE
Port non-SSL	Port non-SSL sur serveur Web	Premier port ouvert entre 8082 et 65536	Port non-SSL sur serveur Web	Port non-SSL sur serveur Web
Port SSL Utilisation de SSL	Port SSL sur serveur Web	Premier port ouvert entre 4345 et 65536	N/A	Port SSL sur serveur Web
Port SSL Pas d'utilisation de SSL	Premier port ouvert entre 4345 et 65536	Premier port ouvert entre 4345 et 65536	N/A	Premier port ouvert entre 4345 et 65536

- **Port de communication Trend Micro Security (pour Mac)** : Utilisé par le serveur Trend Micro Security (pour Mac) pour communiquer avec les clients Mac. Le port par défaut est 61617.
- **Port SMTP** : Utilisé par le serveur Security Server pour envoyer des rapports et des notifications aux administrateurs par courrier électronique. Le port par défaut est 25.
- **Port de proxy** : Utilisé pour réaliser les connexions par le biais d'un serveur proxy.

Liste de contrôle de l'installation

Le programme d'installation vous invite à fournir les informations suivantes lorsque vous installez le serveur Security Server.

TABLEAU 2-2. Liste de contrôle de l'installation

INFORMATION	VALEURS PAR DÉFAUT	VOTRE VALEUR
Serveur Security Server (inclus Scan Server)		
Code d'activation	Fourni par Trend Micro	
Chemin d'installation	L'un des suivants (selon le système d'exploitation) : <ul style="list-style-type: none"> • C:\Program Files\TrendMicro\Security Server • C:\Program Files (x86)\Trend Micro\Security Server 	
Chemin de la base de données du serveur de scan	Identique au chemin d'installation du serveur Security Server (personnalisable)	
Adresse IPv4/IPv6	Défini par l'utilisateur	
Nom de domaine complet (FQDN)	Défini par l'utilisateur	
Nom (d'hôte) NetBIOS	Défini par l'utilisateur	
Serveur Web	Choisissez-en un : <ul style="list-style-type: none"> • Apache • IIS (site Web par défaut) • IIS (site Web virtuel) 	
Port d'écoute (HTTP)	8059	
Port d'écoute (HTTPS)	4343	
Mot de passe de la console	Défini par l'utilisateur	

INFORMATION	VALEURS PAR DÉFAUT	VOTRE VALEUR
Mot de passe de des installations/déchargement de Security Agent	Défini par l'utilisateur	
(Facultatif) Paramètres SMTP des rapports et des notifications du serveur Security Server envoyés par e-mail		
Adresse IPv4/IPv6	Défini par l'utilisateur	
Nom de domaine complet (FQDN)	Défini par l'utilisateur	
Nom (d'hôte) NetBIOS	Défini par l'utilisateur	
Port	25	
Destinataires	Défini par l'utilisateur	
(Facultatif) Paramètres proxy pour la connexion du serveur Security Server aux services hébergés Trend Micro		
Adresse IPv4/IPv6	Défini par l'utilisateur	
Nom de domaine complet (FQDN)	Défini par l'utilisateur	
Nom (d'hôte) NetBIOS	Défini par l'utilisateur	
Nom d'utilisateur d'authentification	Défini par l'utilisateur	
Mot de passe d'authentification	Défini par l'utilisateur	
Agents Security Agent		
Port d'écoute	Généré de façon aléatoire par le programme d'installation	

INFORMATION	VALEURS PAR DÉFAUT	VOTRE VALEUR
Chemin d'installation	<p>L'un des suivants (selon le système d'exploitation) :</p> <ul style="list-style-type: none"> • C:\Program Files\TrendMicro\Security Agent • C:\Program Files (x86)\Trend Micro\Security Agent 	
(Facultatif) Authentification proxy pour les fonctionnalités des agents Security Agent (surveillance des comportements, réputation de sites Web et Smart Scan)		
 Remarque Les agents Security Agent utilisent les paramètres de proxy configurés dans Internet Explorer.		
Nom d'utilisateur d'authentification	Défini par l'utilisateur	
Mot de passe d'authentification	Défini par l'utilisateur	
(Facultatif) Agents Messaging Security Agent		
Adresse IPv4/IPv6 de Microsoft Exchange Server	Défini par l'utilisateur	
Nom de domaine complet (FQDN) de Microsoft Exchange Server	Défini par l'utilisateur	
Nom (d'hôte) NetBIOS de Microsoft Exchange Server	Défini par l'utilisateur	

INFORMATION	VALEURS PAR DÉFAUT	VOTRE VALEUR
Compte et mot de passe d'administrateur de domaine permettant de se connecter à Microsoft Exchange Server	Défini par l'utilisateur	
Port d'écoute	16372	
Chemin d'installation	L'un des suivants (selon le système d'exploitation) : <ul style="list-style-type: none">• C:\Program Files\TrendMicro\Messaging Security Agent• C:\Program Files (x86)\Trend Micro\Messaging Security Agent	
Dossier Temp (Le programme d'installation extrait les fichiers d'installation dans ce dossier)	C\$\	

Installation de Security Server

L'installation de Security Server implique trois phases :

PHASES	TÂCHES ESSENTIELLES
Phase 1 : Démarrage de l'installation de Security Server	<ul style="list-style-type: none">• Lisez les instructions pré-installation.• Lancez le pack d'installation.• Acceptez les termes du contrat de licence.• Sélectionnez un type d'installation.<ul style="list-style-type: none">• Type (recommandé)• Minimale• Personnalisé• Indiquez votre code d'activation.

PHASES	TÂCHES ESSENTIELLES
Phase 2 : configuration des paramètres selon votre type d'installation sélectionné	<p>Pour une installation type ou minimale, configurez les paramètres de base, notamment :</p> <ul style="list-style-type: none"> • Emplacement de l'installation de Security Server • Mots de passe du compte administrateur • Paramètres du serveur SMTP et destinataires des notifications • Smart Protection Network <p>Pour une installation personnalisée, configurez tous les paramètres personnalisables, notamment :</p> <ul style="list-style-type: none"> • Paramètres de base <ul style="list-style-type: none"> • Emplacement de l'installation de Security Server • Emplacement de la base de données du serveur de scan • Installer ou non Security Agent ou Messaging Security Agent sur le même ordinateur que Security Server • Paramètres du serveur Security Server <ul style="list-style-type: none"> • Serveur Web • Mot de passe du compte administrateur • Paramètres du serveur SMTP et destinataires des notifications • Smart Protection Network • Paramètres généraux de proxy • Paramètres de Security Agent <ul style="list-style-type: none"> • Chemin d'installation de Security Agent • Fonctions de Security Agent à activer • Paramètres de proxy pour les services complémentaires • Paramètres de Messaging Security Agent <ul style="list-style-type: none"> • Paramètres du serveur Microsoft Exchange • Emplacement d'installation de Messaging Security Agent

PHASES	TÂCHES ESSENTIELLES
Phase 3 : processus d'installation	Attendez que l'installation se termine, puis fermez-la.

Phase 1 : Démarrage de l'installation de Security Server

Avant de commencer

- Ouvrez une session sur l'ordinateur en tant qu'administrateur de domaine ou qu'administrateur local.
- Fermez toutes les applications en cours avant d'installer Worry-Free Business Security. Si vous procédez à l'installation alors que d'autres applications sont en cours d'exécution, le processus d'installation peut prendre plus de temps.
- Assurez-vous que vous n'installez pas Security Server sur un ordinateur qui exécute des applications pouvant bloquer IIS. Cela risquerait de faire échouer l'installation. Pour obtenir des informations complémentaires, consultez la documentation relative à IIS.
- L'installation de Trend Micro Security Server ne nécessite pas le redémarrage de l'ordinateur. Une fois l'installation terminée, configurez immédiatement les paramètres sur la console Web puis installez l'agent Security Agent sur les clients.

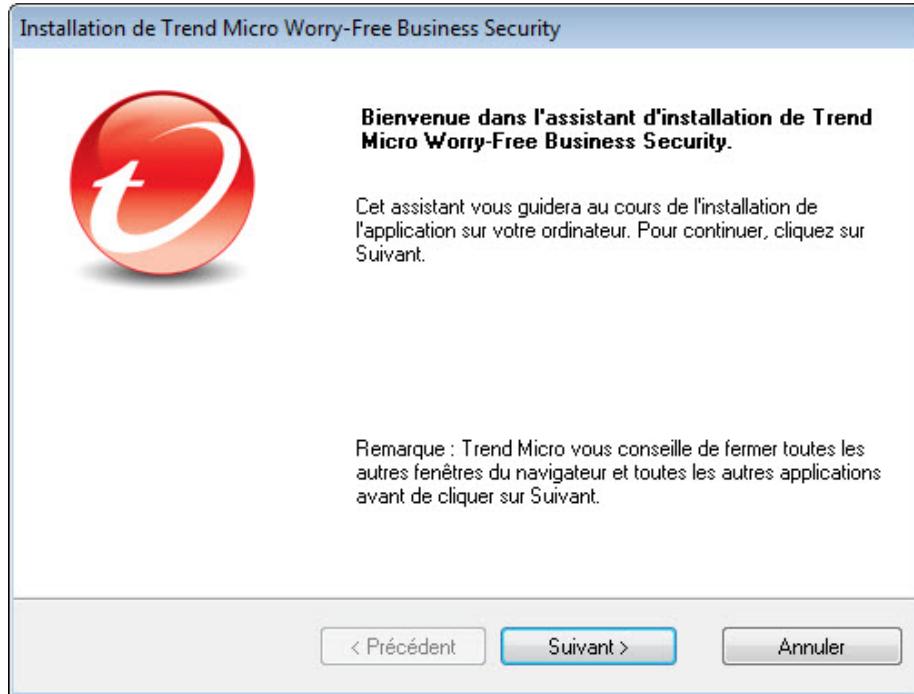
Lancement du pack d'installation

Cliquez deux fois sur le pack d'installation (fichier .exe).

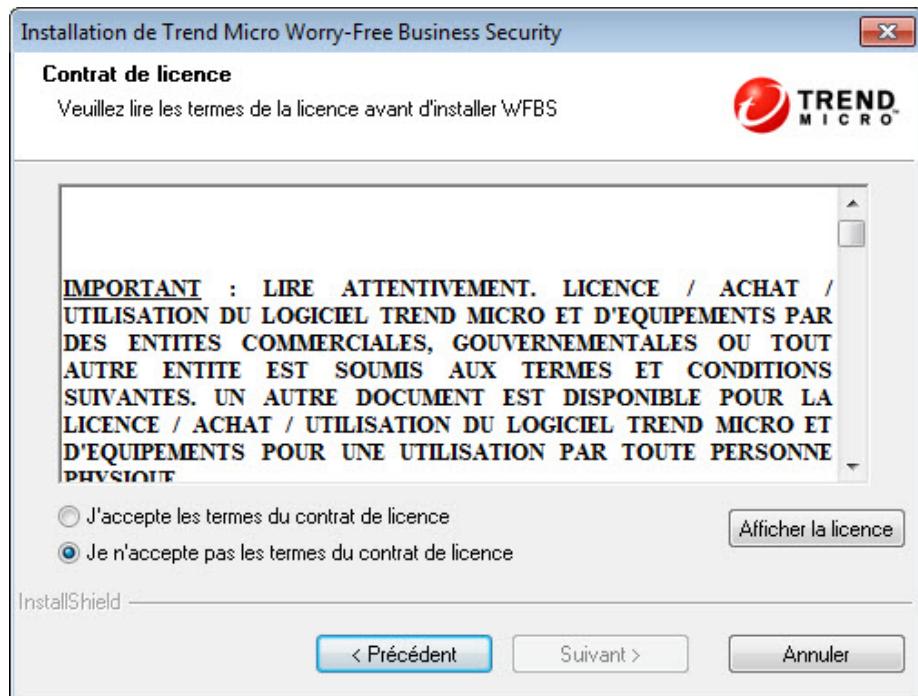


Les fichiers d'installation sont extraits dans le même répertoire que celui du fichier .exe. Pour modifier le chemin, cliquez sur **Parcourir**, puis recherchez le répertoire.

Lorsque vous cliquez sur **Démarrer**, le programme d'installation commence à extraire les fichiers. L'état d'extraction s'affiche dans la barre d'état située au bas de l'écran. Une fois d'extraction terminée, l'écran Bienvenue s'affiche.

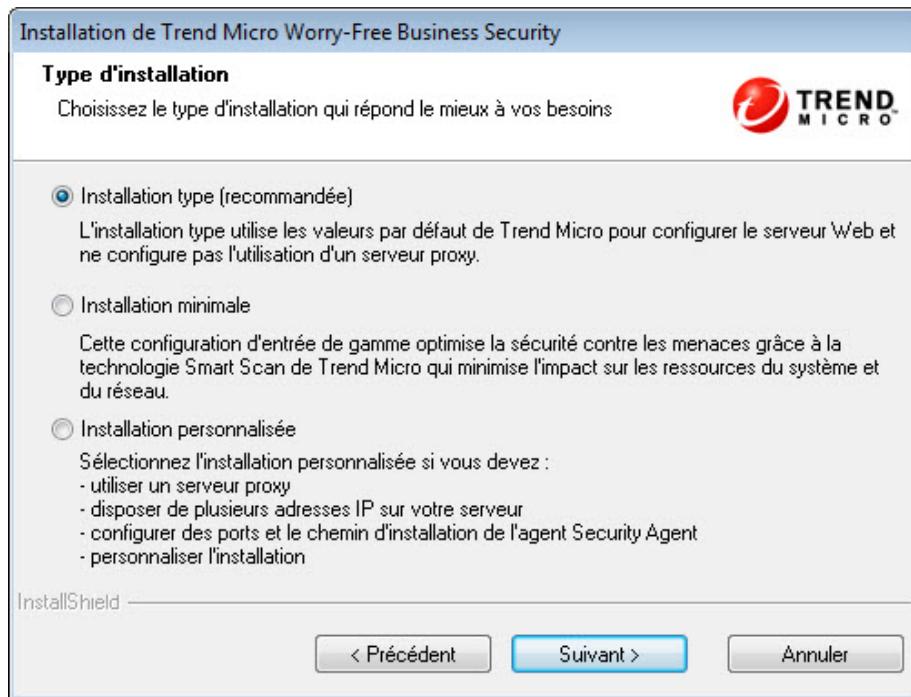


Contrat de licence



Lisez le contrat de licence. Si vous acceptez ces termes, sélectionnez **J'accepte les conditions du contrat de licence.**

Type d'installation



Choisissez l'une des options suivantes :

Installation type (recommandée)

Cette méthode est destinée à une instance de Security Server gérant jusqu'à 100 agents.

Lors d'une installation type :

- Les fonctionnalités suivantes sont automatiquement activées à l'issue de l'installation :
 - Antivirus/anti-programme espion

- Surveillance des comportements (uniquement sur les postes de travail, tels que Windows 10)
- Réputation de sites Web
- Filtrage d'URL
- Smart Scan



Remarque

Les agents Security Agent doivent respecter la configuration minimale requise pour exécuter smart scan. La configuration requise est détaillée à la page <http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx>.

- S'il n'est pas présent, Security Agent est automatiquement installé sur le même ordinateur que le serveur Security Server.



Remarque

Installez Security Agent sur d'autres clients du réseau et gérez-les à partir de la console Web. Pour plus d'informations sur les différentes méthodes d'installation de Security Agent, consultez le Manuel de l'administrateur.

- Si un autre programme de sécurité de point final est installé sur l'ordinateur, le programme d'installation désinstalle préalablement ce dernier avant d'installer Security Agent.



Remarque

Certains logiciels de sécurité de point final peuvent être uniquement détectés, mais pas désinstallés. Dans ce cas, désinstallez d'abord manuellement le logiciel.

Visitez le site Web suivant pour obtenir une liste de logiciels de sécurité de point final ne pouvant pas être désinstallés ou détectables, mais pas désinstallables :

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

Installation minimale

Lors d'une installation minimale :

- seule la fonctionnalité antivirus/anti-programme espion est activée après l'installation.
- S'il n'est pas présent, Security Agent est automatiquement installé sur le même ordinateur que le serveur Security Server.



Remarque

Installez Security Agent sur d'autres clients du réseau et gérez-les à partir de la console Web. Pour plus d'informations sur les différentes méthodes d'installation de Security Agent, consultez le Manuel de l'administrateur.

- Si un autre programme de sécurité de point final est installé sur l'ordinateur, le programme d'installation désinstalle préalablement ce dernier avant d'installer Security Agent.



Remarque

Certains logiciels de sécurité de point final peuvent être uniquement détectés, mais pas désinstallés. Dans ce cas, désinstallez d'abord manuellement le logiciel.

Visitez le site Web suivant pour obtenir une liste de logiciels de sécurité de point final ne pouvant pas être désinstallés ou détectables, mais pas désinstallables :

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

Installation personnalisée

L'installation personnalisée vous offre une flexibilité accrue de configuration des paramètres du serveur Security Server et des agents en fonction de votre stratégie de sécurité réseau. Cette méthode convient parfaitement si le serveur Security Server doit gérer un grand nombre d'agents.

Lors d'une installation personnalisée, les paramètres suivants sont **facultatifs** :

- S'il n'est pas présent, installez Security Agent sur le même ordinateur que le serveur Security Server.

**Remarque**

Installez Security Agent sur d'autres clients du réseau et gérez-les à partir de la console Web. Pour plus d'informations sur les différentes méthodes d'installation de Security Agent, consultez le Manuel de l'administrateur.

- Si un autre programme de sécurité de point final est installé sur l'ordinateur, le programme d'installation désinstalle préalablement ce dernier avant d'installer Security Agent.

**Remarque**

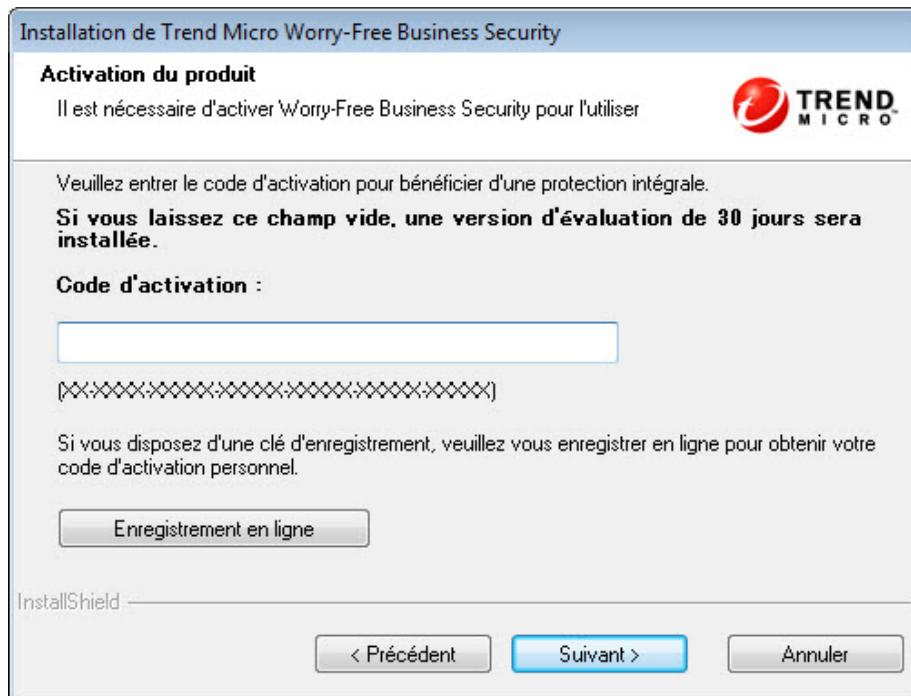
Certains logiciels de sécurité de point final peuvent être uniquement détectés, mais pas désinstallés. Dans ce cas, désinstallez d'abord manuellement le logiciel.

Visitez le site Web suivant pour obtenir une liste de logiciels de sécurité de point final ne pouvant pas être désinstallés ou détectables, mais pas désinstallables :

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

- Installez Messaging Security Agent sur le même ordinateur que le serveur Security Server (s'il existe un serveur Microsoft Exchange) ou sur des clients distants.

Activation du produit



Dans le champ **Code d'activation**, saisissez votre code d'activation.

Si vous n'avez pas de code d'activation, vous n'avez peut-être pas encore enregistré votre version de Worry-Free Business Security. Cliquez sur le bouton **Enregistrement en ligne** pour ouvrir une nouvelle fenêtre de navigateur. Suivez les instructions de l'écran Enregistrement. Vous pouvez également cliquer sur **Suivant** pour installer la version d'évaluation. Si vous effectuez une mise à niveau vers la version complète avant expiration de la période d'évaluation de 30 jours, vous ne perdez aucun paramètre.

Présentation de l'installation



L'écran Présentation de l'installation affiche les composants que vous devez configurer pour installer Trend Micro Security Server, Security Agent ou Messaging Security Agent.

Après avoir cliqué sur **Suivant** :

- Si vous choisissez Installation type/minimale, poursuivez par :
 - *Configuration des paramètres pour une installation type ou minimale à la page 2-26*
 - *Phase 3 : processus d'installation à la page 2-54*

- Si vous choisissez Installation personnalisée, poursuivez par :
 - *Configuration des paramètres d'installation personnalisée à la page 2-32*
 - *Phase 3 : processus d'installation à la page 2-54*

Phase 2 : Configuration des paramètres selon le type d'installation

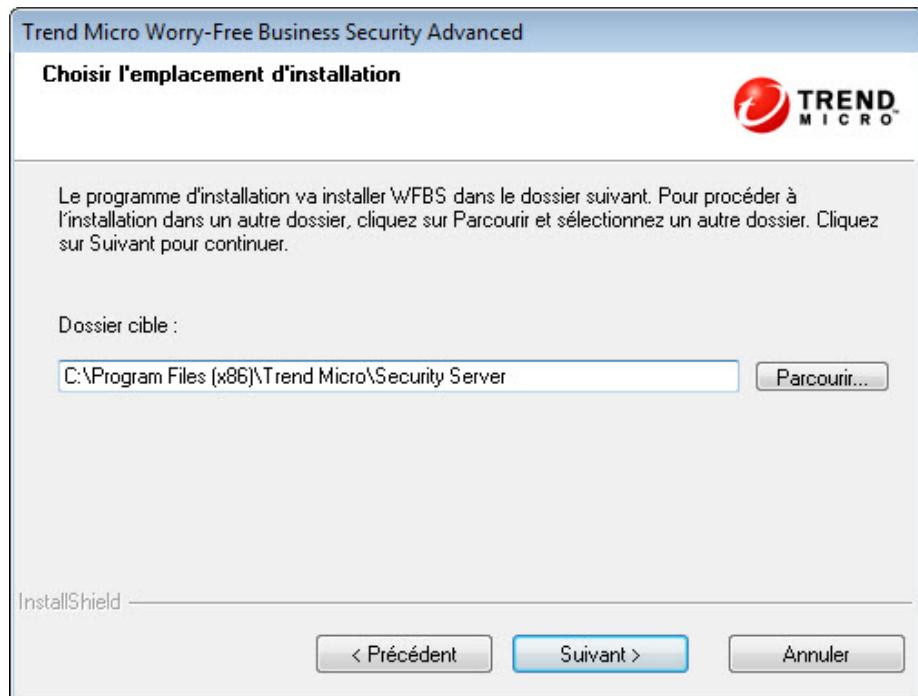
Les paramètres à configurer dans la phase 2 dépendent du type d'installation choisie au cours de la phase 1.

- *Configuration des paramètres pour une installation type ou minimale à la page 2-26*
- *Configuration des paramètres d'installation personnalisée à la page 2-32*

Configuration des paramètres pour une installation type ou minimale

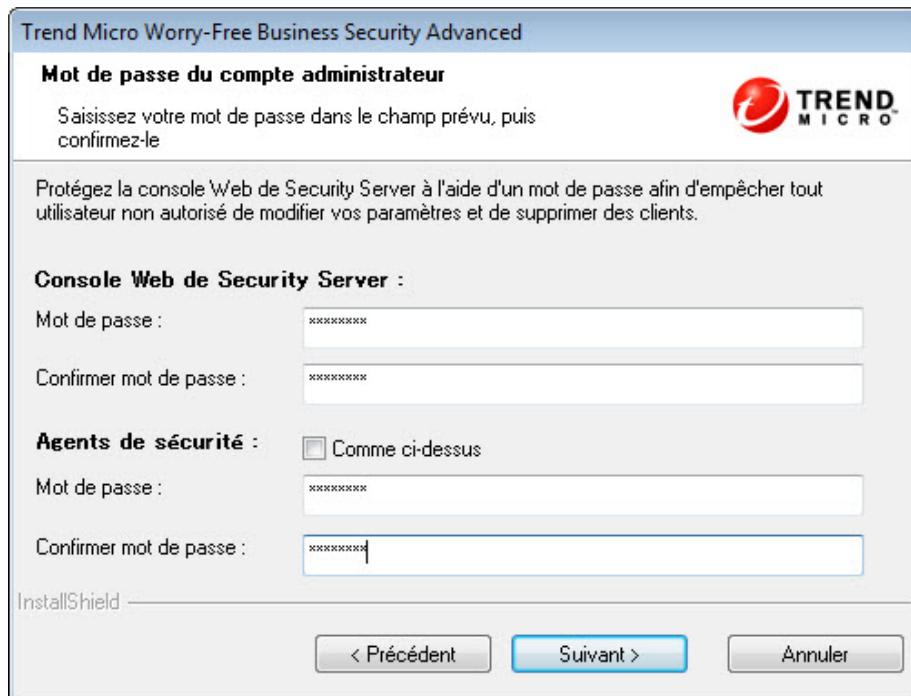
Lorsque vous effectuez une installation type ou minimale, les écrans suivants s'affichent successivement :

Emplacement d'installation



Le dossier d'installation par défaut de Worry-Free Business Security est C:\Program Files\Trend Micro\Security Server ou C:\Program Files (x86)\Trend Micro\Security Server. Cliquez sur **Parcourir** si vous voulez installer Worry-Free Business Security dans un autre dossier.

Mot de passe du compte administrateur



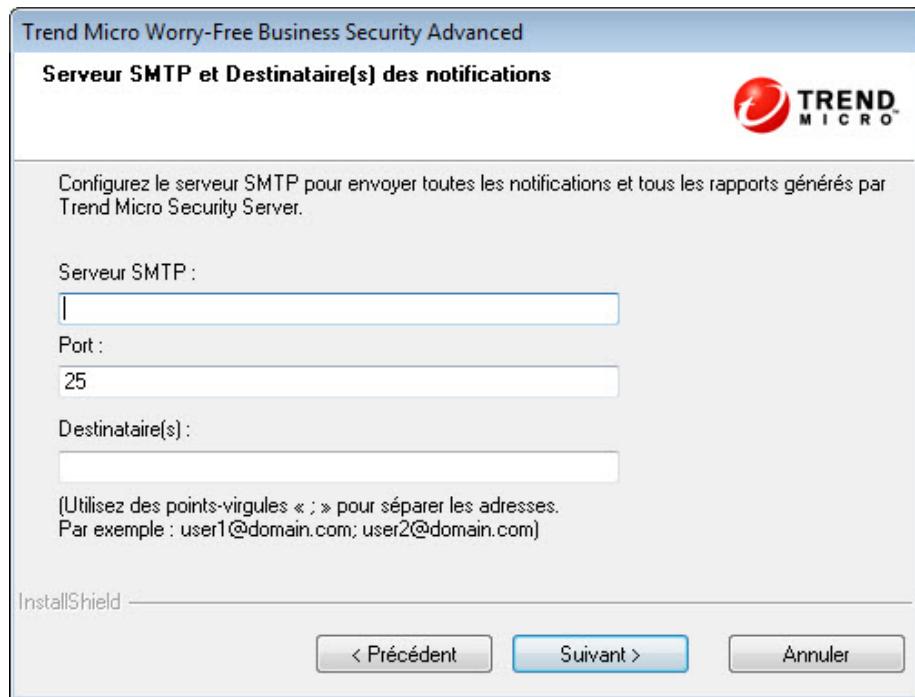
Spécifiez différents mots de passe pour la console Web du serveur Security Server et de Security Agent.

- **Console Web du serveur Security Server** : Requis pour se connecter à la console Web
- **Agents Security Agent** : Requis pour la désinstallation ou le déchargement des agents Security Agent des clients

**Remarque**

Le champ de mot de passe peut contenir entre 1 et 24 caractères et est sensible à la casse.

Serveur SMTP et Destinataires des notifications



Indiquez les informations suivantes :

- **Serveur SMTP** : adresse IP de votre serveur de messagerie



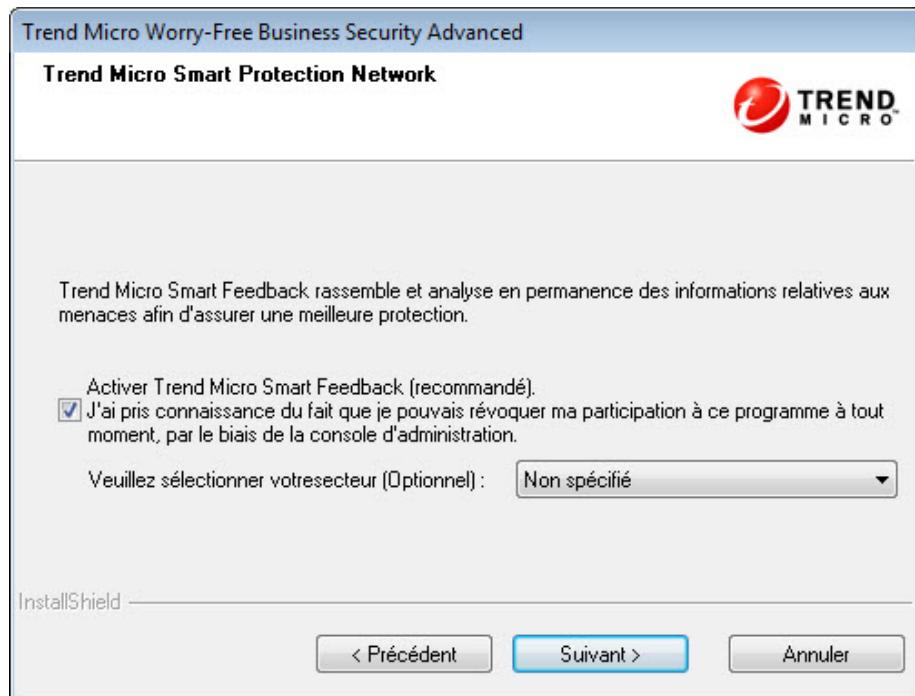
Remarque

Si le serveur SMTP se trouve sur le même ordinateur que WFBS et utilise le port 25, le programme d'installation détecte le nom du serveur SMTP et met à jour les champs Serveur SMTP et Port.

- **Port** : port utilisé par le serveur SMTP pour les communications
- **Destinataire(s)** : adresse(s) électronique(s) utilisée(s) par le serveur SMTP pour envoyer des notifications d'alerte. Vous pouvez entrer plusieurs adresses électroniques si plusieurs personnes doivent recevoir des notifications.

Reportez-vous aux paramètres du serveur de messagerie de votre FAI. Si vous ne connaissez pas ces paramètres, passez à l'étape suivante. Vous pouvez mettre à jour les paramètres SMTP après l'installation. Pour obtenir des instructions, consultez le manuel de l'administrateur.

Smart Protection Network



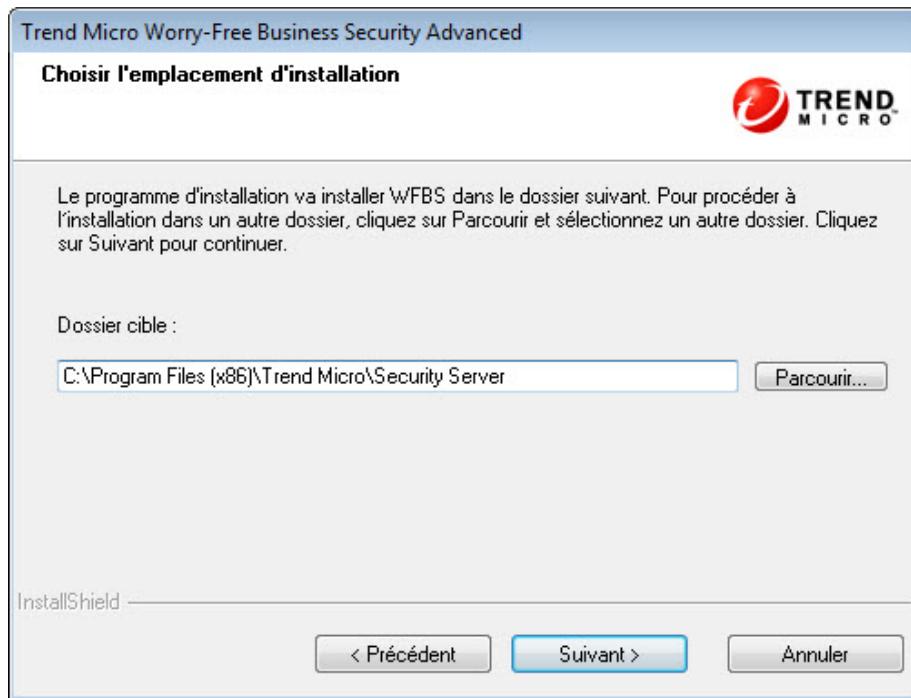
Choisissez de faire partie ou non du programme de commentaires de Trend Micro Smart Protection Network.

Cette fonction facultative vous permet de fournir des commentaires à Trend Micro sur les infections de programmes malveillants. Trend Micro vous recommande de conserver la valeur par défaut activée. En effet, elle lui permet d'utiliser les données de commentaires Worry-Free Business Security à l'échelle mondiale pour renforcer l'efficacité de ses solutions anti-programmes malveillants. Vous pouvez annuler votre participation ultérieurement par le biais de la console Web.

Configuration des paramètres d'installation personnalisée

Si vous effectuez une installation personnalisée, les écrans suivants s'affichent les uns après les autres :

Emplacement d'installation



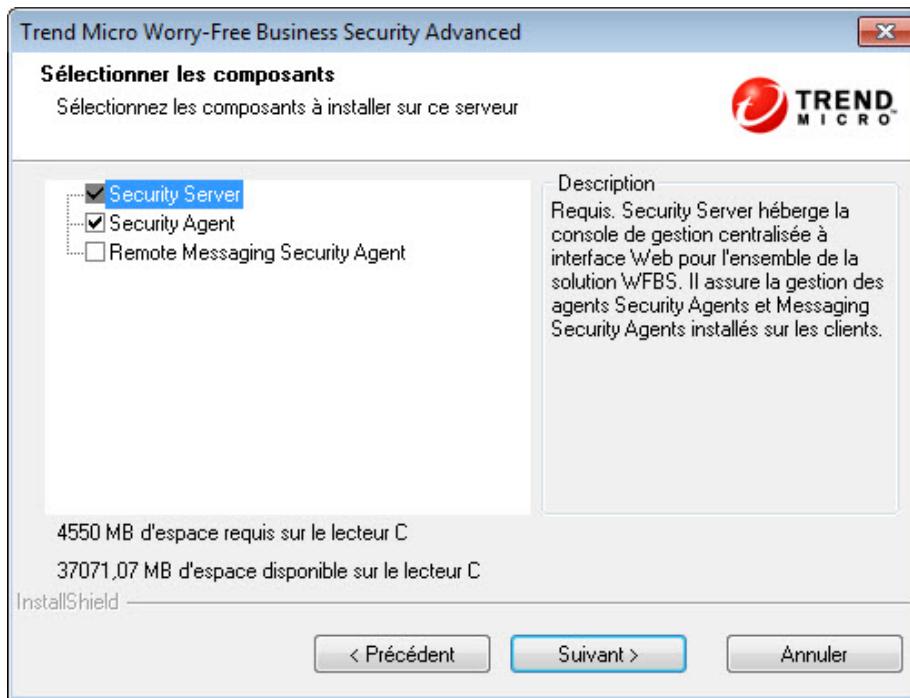
Le dossier d'installation par défaut de Worry-Free Business Security est C:\Program Files\Trend Micro\Security Server ou C:\Program Files (x86)\Trend Micro\Security Server. Cliquez sur **Parcourir** si vous voulez installer Worry-Free Business Security dans un autre dossier.

Emplacement de la base de données du serveur de scan



Sélectionnez **Utiliser l'emplacement d'installation** pour stocker la base de données du serveur de scan dans le même dossier que le serveur Security Server ou sélectionnez **Spécifier un autre emplacement** et saisissez le chemin absolu vers un autre emplacement sur le serveur Security Server. Il est impossible de spécifier un lecteur mappé ou un chemin UNC.

Sélectionner les composants



Sélectionnez les composants que vous voulez installer sur l'ordinateur cible :

- **Serveur Security Server** (Requis) : Le serveur Security Server héberge la console Web centralisée
- **Security Agent** (Facultatif) : agent protégeant les postes de travail et les serveurs
- **Messaging Security Agent** (facultatif) : Lors de l'installation du serveur Security Server sur un ordinateur sur lequel le serveur Microsoft Exchange est installé, le programme d'installation vous invite à installer un agent Messaging Security Agent local (Advanced uniquement).

- **Remote Messaging Security Agent** (facultatif) : Lors de l'installation du serveur Security Server sur un ordinateur qui ne peut pas détecter l'existence de serveurs Microsoft Exchange locaux, le programme d'installation vous invite à installer l'agent Messaging Security Agent distant sur les serveurs distants (Advanced uniquement).



Remarque

S'il existe un serveur Exchange sur l'ordinateur sur lequel vous installez Security Server, Remote Messaging Security Agent n'apparaît pas sur l'écran Sélectionner les composants ; seul l'agent Messaging Security Agent local s'affiche.

Configurer le serveur Security Server



L'écran Configuration du serveur Security Server présente les paramètres du serveur Security Server que vous devez configurer.

Serveur Web



Pour une nouvelle installation, le programme d'installation vérifie si un serveur Web figure déjà sur l'ordinateur cible.

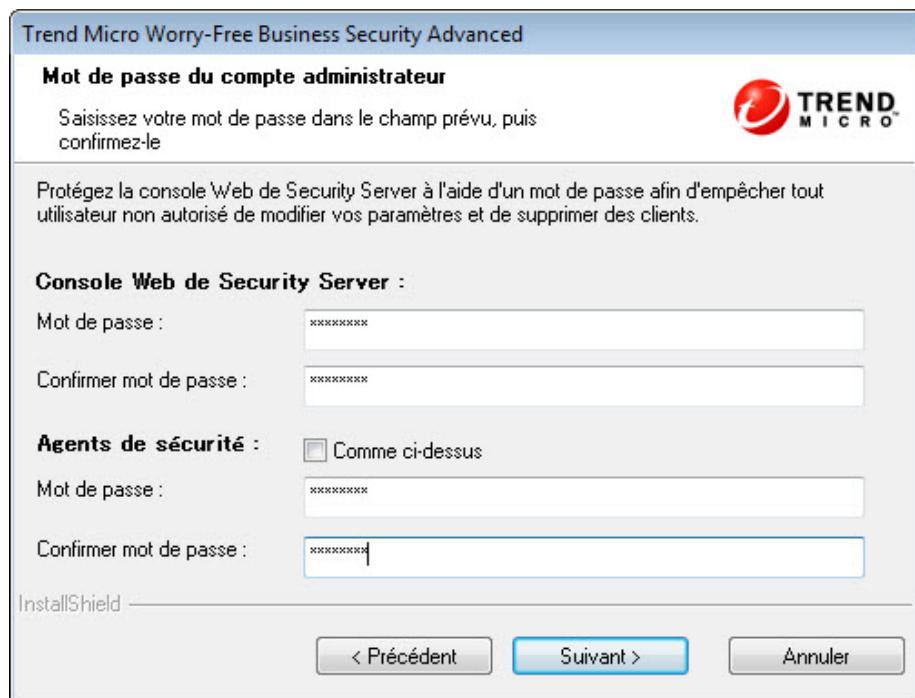
SCÉNARIO	RÉSULTAT	REMARQUES
Le programme d'installation détecte les serveurs Web IIS et Apache	<ul style="list-style-type: none"> Pour une installation standard ou minimale, le programme d'installation utilise automatiquement IIS. Pour une installation personnalisée : <ul style="list-style-type: none"> Le programme d'installation utilise automatiquement IIS si la version du serveur Web Apache n'est pas prise en charge. Vous pouvez choisir l'un ou l'autre serveur Web si la version du serveur Web Apache est prise en charge. 	Si l'ordinateur s'exécute sous Windows 7, 8.1 ou 10, Trend Micro recommande d'effectuer une installation personnalisée et de choisir Apache comme serveur Web.
Le programme d'installation détecte uniquement le serveur Web IIS	<ul style="list-style-type: none"> Pour une installation standard ou minimale, le programme d'installation utilise automatiquement IIS. Pour une installation personnalisée, vous pouvez choisir l'un ou l'autre des deux serveurs Web. Si vous choisissez Apache, le programme d'installation installe automatiquement la version 2.4. 	

SCÉNARIO	RÉSULTAT	REMARQUES
Le programme d'installation détecte uniquement le serveur Web Apache	<ul style="list-style-type: none"> Le programme d'installation utilise le serveur Apache si sa version est la 2.4. L'installation ne peut pas se poursuivre s'il s'agit d'une autre version d'Apache. Tenez compte des actions suivantes : <ul style="list-style-type: none"> Désinstallez Apache si aucune application ne l'utilise. Mettez à niveau Apache vers la version 2.4. Choisissez un autre ordinateur sur lequel installer le Security Server. 	<p>Les plates-formes suivantes contiennent IIS et sont prises en charge par le Security Server :</p> <ul style="list-style-type: none"> Windows Server 2008/2008 R2 Windows SBS 2008 Windows EBS 2008 Windows SBS 2011 Standard/Essentials Windows Server 2012/2012 R2 Windows Server 2016 <p>Si le programme d'installation ne parvient pas à détecter IIS sur ces plates-formes, il est possible que IIS ait été désactivé (par défaut ou par l'administrateur système). Dans ce cas, activez IIS.</p>
Le programme d'installation ne détecte aucun serveur Web	Le programme d'installation installe automatiquement le serveur Web Apache 2.4.	

Pour les mises à niveau, si Apache est déjà utilisé en tant que serveur Web :

- Le programme d'installation effectue une mise à niveau automatique d'Apache vers la version 2.4 si le serveur Web Apache a été installé par le programme d'installation de Worry-Free Business Security 8.x/9.x.
- Le programme d'installation conserve la version existante d'Apache si elle a été installée par un autre programme.

Mot de passe du compte administrateur



Spécifiez différents mots de passe pour la console Web du serveur Security Server et de Security Agent.

- **Console Web du serveur Security Server** : Requis pour se connecter à la console Web
- **Agents Security Agent** : Requis pour la désinstallation ou le déchargement des agents Security Agent des clients



Remarque

Le champ de mot de passe peut contenir entre 1 et 24 caractères et est sensible à la casse.

Serveur SMTP et Destinataires des notifications



Indiquez les informations suivantes :

- **Serveur SMTP** : adresse IP de votre serveur de messagerie

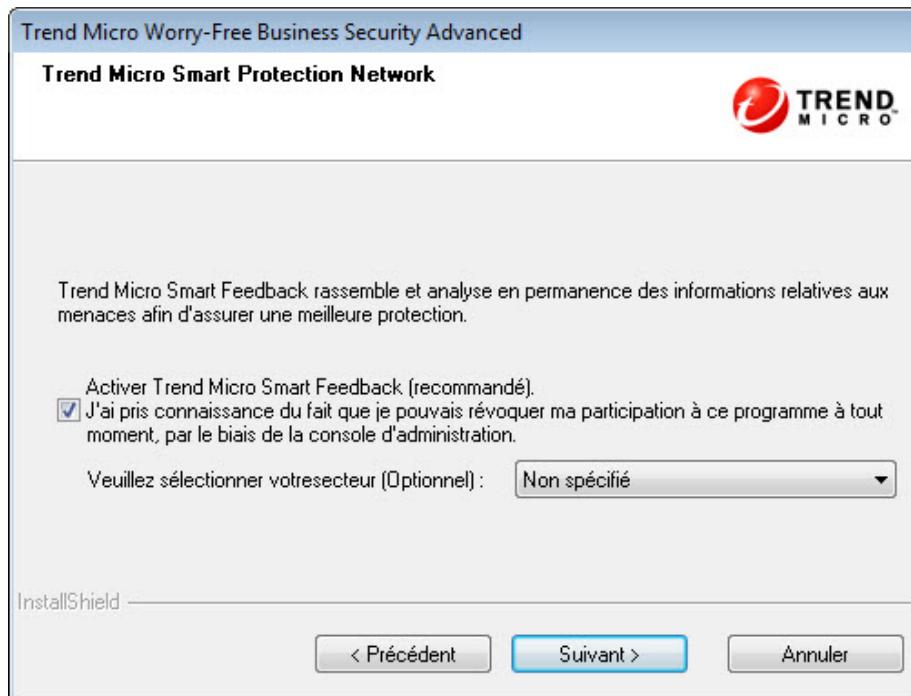
**Remarque**

Si le serveur SMTP se trouve sur le même ordinateur que WFBS et utilise le port 25, le programme d'installation détecte le nom du serveur SMTP et met à jour les champs Serveur SMTP et Port.

- **Port** : port utilisé par le serveur SMTP pour les communications
- **Destinataire(s)** : adresse(s) électronique(s) utilisée(s) par le serveur SMTP pour envoyer des notifications d'alerte. Vous pouvez entrer plusieurs adresses électroniques si plusieurs personnes doivent recevoir des notifications.

Reportez-vous aux paramètres du serveur de messagerie de votre FAI. Si vous ne connaissez pas ces paramètres, passez à l'étape suivante. Vous pouvez mettre à jour les paramètres SMTP après l'installation. Pour obtenir des instructions, consultez le manuel de l'administrateur.

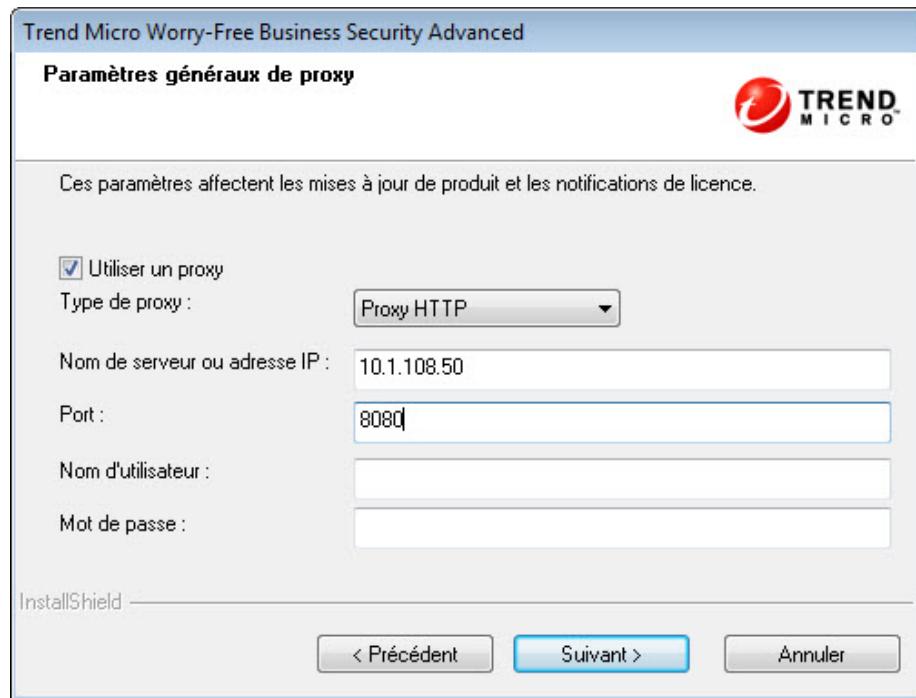
Smart Protection Network



Choisissez de faire partie ou non du programme de commentaires de Trend Micro Smart Protection Network.

Cette fonction facultative vous permet de fournir des commentaires à Trend Micro sur les infections de programmes malveillants. Trend Micro vous recommande de conserver la valeur par défaut activée. En effet, elle lui permet d'utiliser les données de commentaires Worry-Free Business Security à l'échelle mondiale pour renforcer l'efficacité de ses solutions anti-programmes malveillants. Vous pouvez annuler votre participation ultérieurement par le biais de la console Web.

Paramètres généraux de proxy



Si un serveur proxy est requis pour accéder à Internet, cochez la case **Utiliser un proxy** et saisissez les informations suivantes :

- **Type de serveur proxy**
- **Nom de serveur ou adresse IP**
- **Port**
- **Nom d'utilisateur et mot de passe** : requis uniquement si le serveur proxy nécessite une authentification.

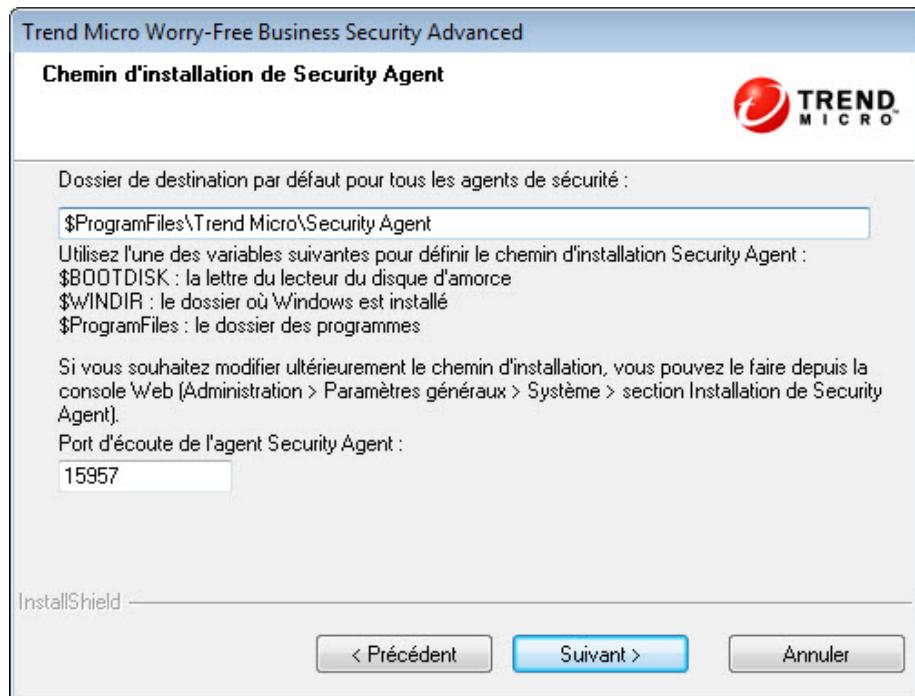
Configuration de Security Agent



L'écran Configuration de Security Agent présente les paramètres de Security Agent que vous devez configurer.

À l'issue de l'installation du serveur Security Server, installez Security Agent sur les clients du réseau. Pour plus d'informations sur les différentes méthodes d'installation de Security Agent, consultez le Manuel de l'administrateur.

Chemin d'installation de Security Agent



Définissez les éléments suivants :

- **Chemin d'installation** : dossier de destination dans lequel les fichiers de Security Agent sont installés
- **Port d'écoute de Security Agent** : numéro de port utilisé pour les communications entre Security Agent et le serveur Security Server

Paramètres de Security Agent



Configurez les paramètres de Security Agent pour les serveurs et les postes de travail.

- **Serveurs** : Les agents Security Agent exécutés sur des plates-formes serveur Windows (telles que Windows Server 2016) seront ajoutés aux groupes de serveurs par défaut lorsque vous les ajouterez pour la première fois à la console Web. Vous pouvez activer différentes technologies pour ce groupe selon vos besoins particuliers.
- **Postes de travail** : les agents Security Agent exécutés sur des plates-formes de bureau Windows (telles que Windows 10) seront ajoutés aux groupes de postes de travail par défaut lorsque vous les ajouterez pour la

première fois à la console Web. Vous pouvez activer différentes technologies pour ce groupe selon vos besoins particuliers.

Dans chaque groupe, vous pouvez configurer les composants suivants :

- **Smart scan** : Smart scan utilise un serveur de scan central sur votre réseau pour prendre en charge une partie du scan des clients.
- **Antivirus et Anti-programme espion** : scanne les fichiers à la recherche de code malveillant lors de leur ouverture ou création
- **Pare-feu** : protège les clients contre les attaques de programmes malveillants et les virus de réseau en créant une barrière entre les clients et le réseau
- **Réputation de sites Web** : bloque les sites Web malveillants en vérifiant la crédibilité des domaines Web et en leur attribuant un score de réputation basé sur plusieurs facteurs d'identification
- **Filtrage d'URL** : bloque des sites Web de catégories particulières (pornographiques, réseaux sociaux, etc.) selon la politique de votre entreprise
- **Surveillance des comportements** : analyse le comportement du programme afin de détecter proactivement les menaces connues et inconnues.
- **Contrôle des dispositifs** : régule l'accès aux dispositifs de stockage externes et aux ressources du réseau.
- **Apprentissage automatique prédictif** : utilise une technologie avancée d'apprentissage automatique pour mettre en corrélation les informations sur les menaces et effectuer une analyse approfondie des fichiers afin de détecter de nouveaux risques de sécurité inconnus via l'empreinte d'ADN numérique, le mappage d'API et d'autres fonctionnalités de fichier.

Paramètres de proxy pour les services complémentaires



Les services **Smart Scan**, **Réputation de sites Web** et **Surveillance des comportements** utilisent l'adresse et le port du serveur proxy employés par Internet Explorer sur les ordinateurs clients. Si ce serveur proxy nécessite une authentification, utilisez cet écran pour saisir vos informations de connexion.

Configuration de l'agent Messaging Security Agent

Installez Messaging Security Agent lors de l'installation du serveur Security Server.

Remarques et rappels d'installation :

- Vous n'avez pas besoin d'arrêter ou de démarrer les services Microsoft Exchange avant ou après l'installation.
- Si l'endpoint contient des informations d'une installation précédente de Messaging Security Agent, vous ne pourrez pas installer correctement la nouvelle version. Utilisez l'**utilitaire de résolution des problèmes d'installation et de désinstallation du programme** pour nettoyer les résidus de l'installation précédente.

Pour plus d'informations sur l'**utilitaire de résolution des problèmes d'installation et de désinstallation du programme**, reportez-vous à <https://support.microsoft.com/en-us/help/17588/>.

- Si vous installez Messaging Security Agent sur un serveur qui exécute des outils de blocage, supprimez l'outil de blocage pour qu'il ne désactive pas le service IIS et fasse échouer l'installation.
- Messaging Security Agent peut aussi être installé à partir de la console Web à l'issue de l'installation de Security Server. Pour plus de détails, reportez-vous au Manuel de l'administrateur.

Le programme d'installation vous invite à installer Messaging Security Agent à l'un des moments suivants :

- Lors de l'installation du serveur Security Server sur un ordinateur sur lequel le serveur Microsoft Exchange est installé, le programme

d'installation vous invite à installer un agent Messaging Security Agent local.

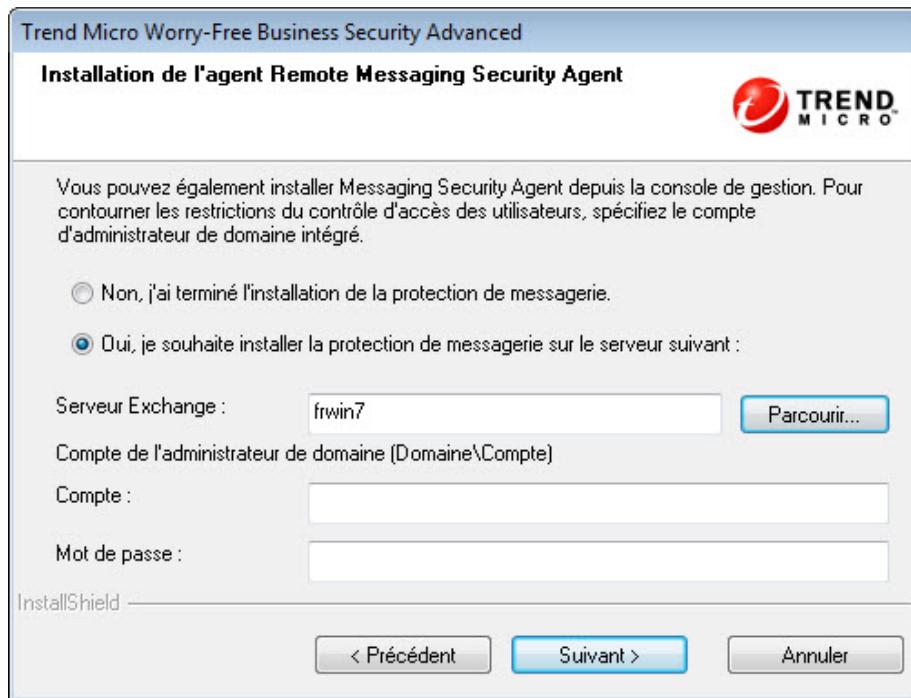


- Lors de l'installation du serveur Security Server sur un ordinateur qui ne peut pas détecter l'existence de serveurs Microsoft Exchange locaux, le

programme d'installation vous invite à installer un agent Messaging Security Agent **distant** sur les serveurs distants.



Installation de Messaging Security Agent



Saisissez les informations suivantes :

- **Serveur Exchange**



Remarque

Le programme d'installation détecte automatiquement le nom du serveur Exchange local et renseigne le champ Serveur Exchange si le serveur Exchange est situé sur l'ordinateur sur lequel Security Server est installé. Si un serveur Exchange est installé sur le même ordinateur et si le champ correspondant à son nom n'est pas automatiquement renseigné, vérifiez si l'environnement Messaging Security Agent respecte la configuration requise.

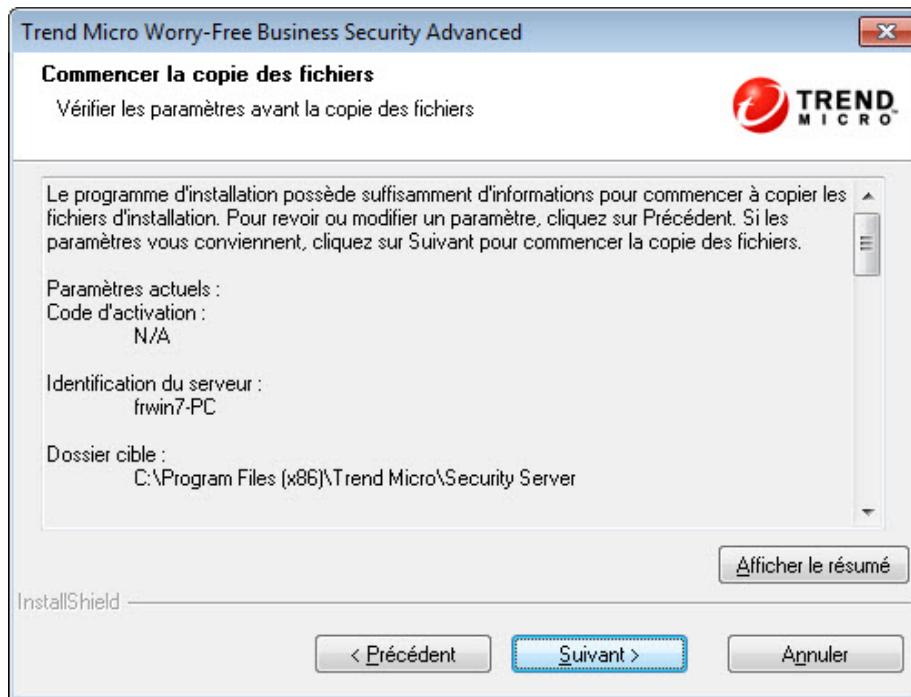
- **Compte de l'administrateur de domaine**
- **Mot de passe**

**Remarque**

Le programme d'installation peut ne pas transmettre les mots de passe contenant des caractères spéciaux et/ou non-alphanumériques à l'ordinateur de serveur Exchange. Cela empêchera l'installation de Messaging Security Agent. Pour contourner ce problème, vous pouvez soit modifier provisoirement le mot de passe du compte de l'administrateur du domaine intégré, soit installer Messaging Security Agent directement sur le serveur Microsoft Exchange.

Phase 3 : processus d'installation

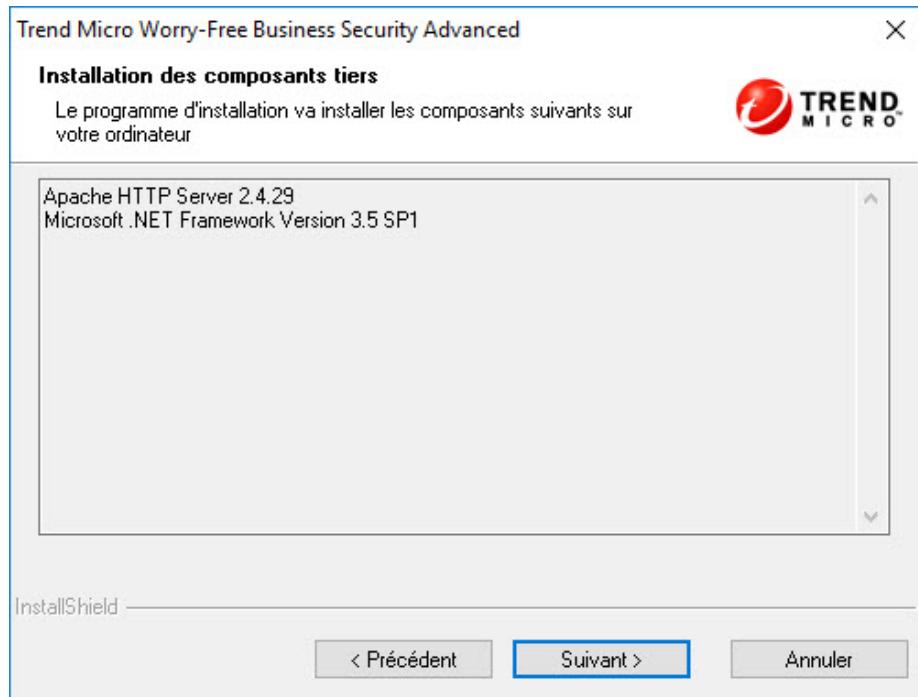
Commencer la copie des fichiers



L'écran Commencer la copie des fichiers affiche un récapitulatif de tous les paramètres qui seront utilisés durant l'installation de Worry-Free Business Security.

Cliquez sur **Retour** pour vérifier les paramètres d'installation précédents ou sur **Suivant** pour procéder à l'installation effective.

Installer des composants tiers



Cet écran indique les composants tiers qui seront installés. Cliquez sur **Suivant** pour lancer l'installation des composants sélectionnés.

État de l'installation

Trend Micro Worry-Free Business Security Advanced

État de l'installation



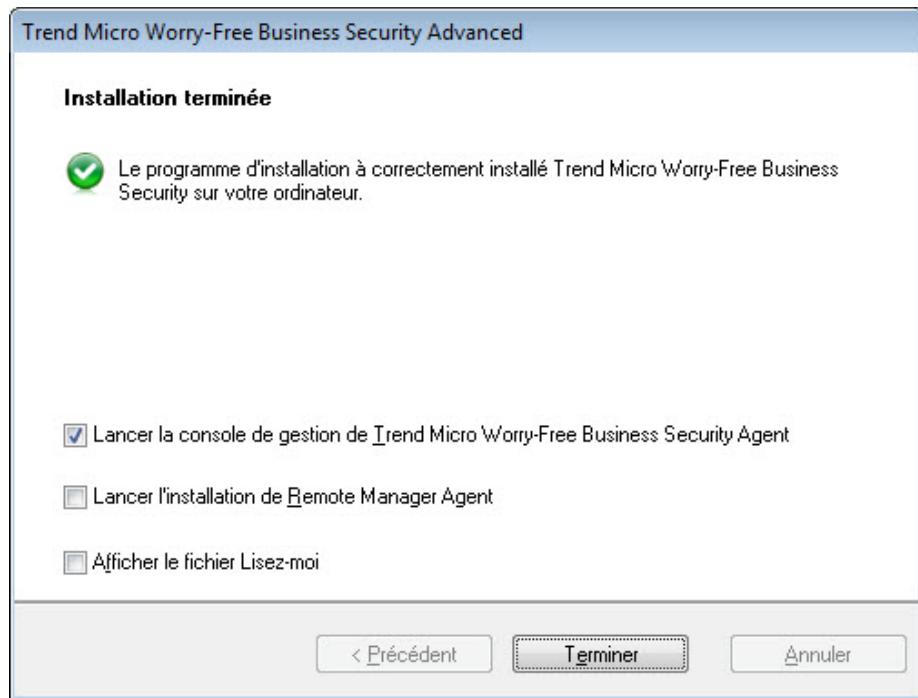
Le programme d'installation installe Trend Micro Worry-Free Business Security sur votre ordinateur. Cette procédure peut prendre quelques minutes...

Le programme d'installation installe Microsoft .NET Framework 3.5...

InstallShield

Le processus d'installation peut prendre un certain temps. Durant l'installation, un écran d'état affiche la progression du processus.

Installation terminée



Cochez éventuellement les cases pour :

- Ouvrir la console d'administration à interface Web (sélectionné par défaut)
- Installer Remote Manager Agent (consultez le *Manuel de l'administrateur* pour connaître la procédure)
- Afficher le fichier Lisez-moi

Cliquez sur **Terminer** pour quitter la procédure d'installation.

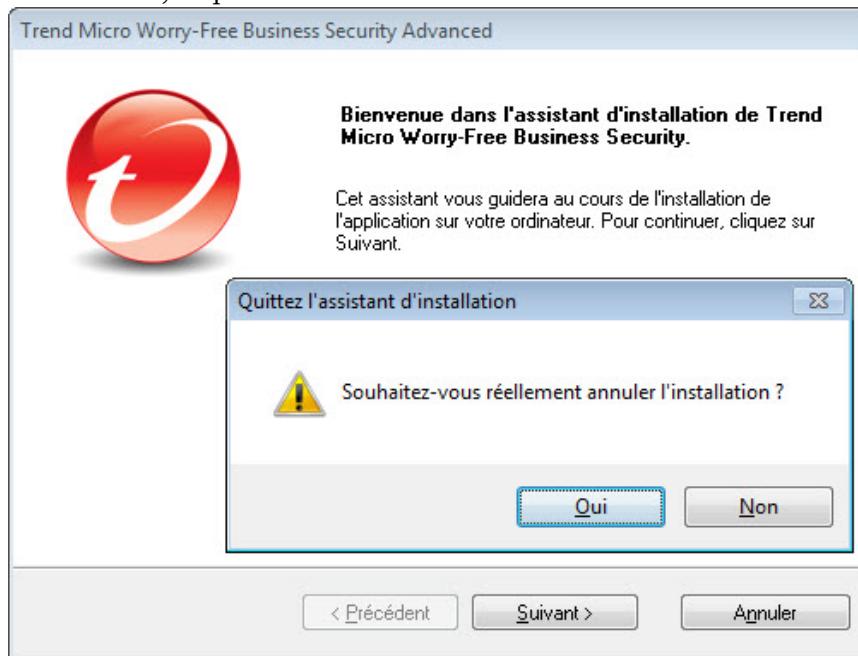
Installation de plusieurs serveurs Security Server en mode silencieux

Utilisez l'installation en mode silencieux pour exécuter plusieurs installations identiques sur des réseaux distincts. Vous pouvez enregistrer les paramètres d'installation dans une session de l'assistant d'installation, puis les utiliser pour générer des installations automatisées.

Enregistrement d'une session d'installation

Procédure

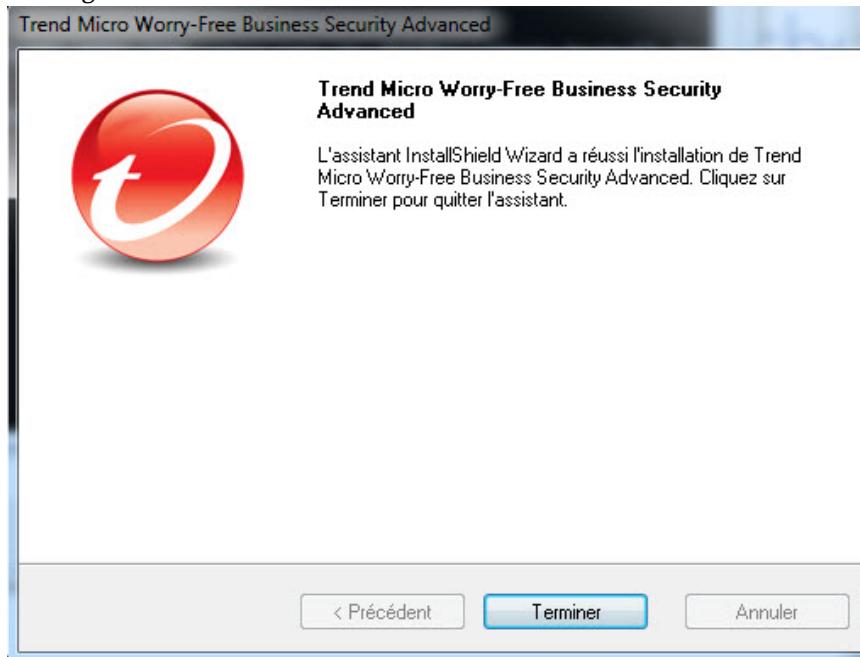
1. Téléchargez et extrayez les fichiers WFBS sur votre disque dur. Lorsque l'assistant d'installation commence à collecter les paramètres d'installation, cliquez sur **Annuler** > **Oui** > **Terminer**.



2. En mode d'invite de commande, accédez au répertoire dans lequel se situent les fichiers d'installation extraits de WFBS, par exemple : C:\Extract\WFBS\CSM
3. À l'invite de commande, saisissez `Setup.exe /r /f1"\\silent-install.iss"`, puis cliquez sur **Entrée**.

L'assistant d'installation redémarre. Les données que vous entrez seront enregistrées dans le fichier silent-install.iss sur le lecteur C.

4. Suivez les instructions indiquées à l'écran. Ces instructions sont les mêmes que celles décrites dans *Installation de Security Server à la page 2-13*.
5. À la fin de la session d'enregistrement, l'écran de confirmation suivant s'affiche. Cliquez sur **Terminer** pour terminer la session d'enregistrement et revenir en mode d'invite de commande.



Démarrage de l'installation en mode silencieux

Procédure

1. En mode d'invite de commande, accédez au répertoire dans lequel se situent les fichiers d'installation extraits de WFBS, par exemple : C:\Extract\WFBS\CSM
2. À l'invite de commande, saisissez `Setup.exe /s /f1"c:\silent-install.iss"`, puis cliquez sur **Entrée**.

L'installation de WFBS en mode silencieux démarre automatiquement et dure environ le même temps qu'une installation normale.

Lors de l'installation en mode silencieux, aucun indicateur de progression n'apparaît à l'écran.

3. Pour vérifier si l'installation a abouti, ouvrez le fichier `c:\setup.log`. Si `ResultCode=0` s'affiche, l'installation a réussi.
4. Reprenez les opérations 1 à 3 sur tous les autres ordinateurs de votre réseau.

Vérification de l'installation

Procédure

- Cliquez sur **Démarrer > Tous les programmes** afin de voir si Security Server et Security Agent figurent dans la liste.



- Cliquez sur **Démarrer > Panneau de configuration > Programmes > Désinstaller un programme** pour vérifier si le programme WFBS et Security Agent figurent dans la liste.
- Pour vous connecter à la console d'administration à l'aide de l'URL du serveur : `https://{nom_serveur}:{numéro de port}/SMB`

**Remarque**

Si vous n'utilisez pas SSL (Security Socket Layer), saisissez `http` au lieu de `https`.

Chapitre 3

Mise à niveau du serveur Security Server et des agents

Ce chapitre fournit des informations que vous devrez comprendre pour mettre à niveau Security Server et les agents.

Configuration requise pour l'installation et la mise à niveau

Visitez le site Web suivant pour obtenir une liste complète des configurations requises pour une installation ou une mise à niveau :

<http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx>

Éléments à prendre en compte pour la mise à niveau

Tenez compte des points suivants lors de la mise à niveau du serveur Security Server et des agents.

- *Exigences IPv6 pour les mises à niveau à la page 3-2*
- *Pratiques recommandées pour la mise à niveau à la page 3-3*

Exigences IPv6 pour les mises à niveau

Les conditions requises pour la prise en charge d'IPv6 dans le serveur Security Server sont les suivantes :

- Le serveur Security Server à mettre à niveau doit être installé sur Windows 7, 8.1, 10, Server 2008, 2012, 2012 R2, 2016, 2019 ou SBS 2008/2011. La mise à niveau des serveurs Security Server est impossible sur Windows XP, Server 2003 et SBS 2003, car ces systèmes d'exploitation ne prennent que partiellement en charge l'adressage IPv6.
- Affectez une adresse IPv6 au serveur Security Server. De plus, le serveur doit être identifié par son nom d'hôte, de préférence son nom de domaine complet (FQDN ou (Fully Qualified Domain Name). Si le serveur est identifié par son adresse IPv6, tous les clients actuellement gérés par le serveur perdront la connexion à celui-ci. Si le serveur est identifié par son adresse IPv4, il ne pourra pas déployer l'agent sur des clients IPv6 purs.

- Vérifiez que l'adresse IPv6 ou IPv4 de l'ordinateur hôte du serveur Security Server peut être récupérée en utilisant, par exemple, la commande « ping » ou « nslookup ».

Pratiques recommandées pour la mise à niveau

Vous pouvez conserver vos paramètres clients lorsque vous passez à la version la plus récente de WFBS. Pour pouvoir facilement restaurer vos paramètres existants en cas d'échec de la mise à niveau, Trend Micro vous recommande les actions suivantes :

- Sauvegarde de la base de données du serveur Security Server
- Suppression de tous les fichiers journaux du serveur Security Server

Sauvegarde de la base de données du serveur Security Server

Procédure

1. Arrêtez Trend Micro Security Server Master Service
 2. Dans Windows Explorer, accédez au dossier Security Server et copiez le contenu du dossier \PCCSRV\HTTPDB à un autre emplacement (par exemple, sur le même serveur, mais dans un dossier différent, sur un autre ordinateur ou encore sur un lecteur amovible).
-

Suppression des fichiers journaux du serveur Security Server

Procédure

1. Accédez à **Rapports > Maintenance > Suppression manuelle de journaux**.
2. Pour les types de journaux que vous souhaitez supprimer, définissez **Supprimer journaux antérieurs à** sur 0.

3. Choisissez l'une des méthodes suivantes pour supprimer les journaux :
 - Cliquez sur **Supprimer** dans chaque type de journal.
 - Cliquez sur **Tout supprimer** pour supprimer tous les journaux.
-

Mises à niveau des versions antérieures

Cette version de produit prend en charge les mises à niveau depuis les versions Worry-Free Business Security ou Worry-Free Business Security-Advanced suivantes :

- 10,0
- 9.x (y compris tous les Service Packs)
- 8.x (8.0 et 8.0 SP1)

Cette version du produit ne prend pas en charge les mises à niveau suivantes :

- Worry-Free Business Security ou Worry-Free Business Security-Advanced 7.x
- Worry-Free Business Security ou Worry-Free Business Security-Advanced 6.x
- Worry-Free Business Security ou Worry-Free Business Security-Advanced 5.x
- Toutes les mises à niveau qui prenaient en charge Windows 2000
- Client/Server Messaging Security 3.6 (à l'exception de la version japonaise)
- Client/Server/Messaging Security 3.5
- Client/Server/Messaging Security 3.0
- Client/Server Security 3.0

- Client/Server Suite 2.0
- Client/Server/Messaging Suite 2.0
- OfficeScan ou ScanMail pour Microsoft Exchange
- D'une langue à l'autre

Selon la bande passante du réseau et le nombre d'agents gérés par le serveur Security Server, effectuez une mise à niveau échelonnée des agents par groupes ou mettez à niveau tous les agents immédiatement après la mise à niveau du serveur.

Méthode de mise à niveau 1 : Mise à niveau à l'aide du pack d'installation

Procurez-vous le pack d'installation de cette version du produit, puis exécutez Setup.exe sur l'ordinateur du serveur Security Server. Lorsqu'il détecte une installation existante du serveur Security Server sur l'ordinateur,

le programme d'installation vous invite à effectuer une mise à niveau, tel qu'indiqué dans l'image suivante.



Suivez les instructions s'affichant à l'écran pour effectuer la mise à niveau du serveur Security Server.

Après la mise à niveau :

- Les agents Security Agent en ligne sont mis à niveau immédiatement.
- Les agents Security Agent hors ligne sont mis à niveau lorsqu'ils passent en mode en ligne.

Demandez aux utilisateurs de se connecter au réseau afin que les agents Security Agent passent en mode en ligne. Si un agent Security Agent est en mode hors ligne pendant une période prolongée, demandez aux

utilisateurs de le désinstaller du point final, puis d'utiliser une méthode d'installation d'agent adaptée (par exemple Client Packager), décrite dans le *Manuel de l'administrateur* pour le réinstaller.



Remarque

Tous les paramètres d'agent précédents, hormis les priviléges d'agent de mise à jour, seront conservés après la mise à niveau sur cette version. Ce qui signifie que les agents de mise à jour redeviendront des Security Agent après la mise à niveau. Réaffectez-les en tant qu'agents de mise à jour depuis la console de gestion.

Voir <http://esupport.trendmicro.com/solution/en-US/1057531.aspx> pour plus de détails.

Méthode de mise à niveau 2 : déplacement des agents Security Agent vers le serveur Security Server 10.0 Service Pack 1

Effectuez une nouvelle installation de Security Server et déplacez les agents Security Agent vers ce serveur. Lorsque vous déplacez les agents Security Agent, ceux-ci sont automatiquement mis à niveau vers la version 10.0 Service Pack 1.

Partie 1 : nouvelle installation du serveur Security Server 10.0 Service Pack 1

Procédure

1. Effectuez une nouvelle installation du serveur Security Server sur un ordinateur. Pour plus de détails, voir *Installation de Security Server à la page 2-13*.
2. Enregistrez les informations du serveur Security Server 10.0 Service Pack 1. Lors du déplacement des agents, spécifiez ces informations sur le serveur Security Server pris en charge.
 - Nom ou adresse IP de l'hôte

- Port d'écoute du serveur

Le nom d'hôte et le port d'écoute se trouvent sur l'écran Paramètres de sécurité du serveur Security Server, au-dessus du panneau Tâches.

Partie 2 : mise à niveau des agents

Procédure

1. Sur la console Web Security Server prise en charge, accédez à **Paramètres de sécurité**.
2. Pour déplacer des agents Security Agent, cliquez sur un groupe puis sélectionnez les agents à déplacer.



Conseil

Pour sélectionner plusieurs agents Security Agent adjacents, cliquez sur le premier agent de la plage, maintenez la touche MAJ enfoncee, puis cliquez sur le dernier agent de la plage. Pour sélectionner plusieurs agents non adjacents, cliquez sur le premier agent de la plage, maintenez la touche CTRL enfoncee, puis cliquez sur les agents que vous souhaitez sélectionner.

3. Cliquez sur **Gérer l'arborescence des clients > Déplacer le client**.
Un nouvel écran s'affiche.
 4. Saisissez le nom d'hôte et le port d'écoute du serveur Security Server 10.0 Service Pack 1 vers lequel déplacer les agents.
 5. Cliquez sur **Déplacer**.
-

Résultats de la mise à niveau

- Le déplacement et la mise à niveau des agents en ligne commencent. Après la mise à niveau, les agents Security Agent se trouveront sous le

groupe **Postes de travail (par défaut)** ou **Serveurs (par défaut)** du serveur Security Server 10.0 Service Pack 1, selon le système d'exploitation de l'endpoint. L'agent hérite des paramètres du nouveau groupe.

- La mise à niveau des agents hors ligne s'opère lorsque ceux-ci passent en mode en ligne. Demandez aux utilisateurs de se connecter au réseau afin que les agents passent en mode en ligne. Si un agent Security Agent est en mode hors ligne pendant une période prolongée, demandez aux utilisateurs de le désinstaller du point final, puis d'utiliser une méthode d'installation d'agent adaptée (par exemple Client Packager), décrite dans le *Manuel de l'administrateur* pour le réinstaller.

Mises à niveau vers la version complète ou l'Édition Advanced

Utilisez l'écran Licence de la console Web pour :

- Effectuer une mise à niveau de la version d'évaluation vers la version complète du produit
- Effectuer une mise à niveau de la version standard vers la version avancée du produit

Versions d'évaluation et complètes

Lorsque votre version d'évaluation est sur le point d'expirer, un message de notification s'affiche sur l'écran État actuel de la console Web. Vous pouvez effectuer la mise à niveau d'une version d'évaluation vers une version sous licence à l'aide de la console Web. Vos paramètres de configuration actuels seront conservés. Lors de l'achat d'une version avec licence complète, vous recevez une clé d'enregistrement ou un code d'activation.

Éditions Advanced et Standard

Trend Micro propose deux produits similaires pour protéger vos clients et votre réseau : Worry-Free Business Security Standard et Worry-Free Business Security Advanced.

TABLEAU 3-1. Versions du produit

VERSION DU PRODUIT	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Solution côté client	Oui	Oui
Solution côté serveur	Oui	Oui
Solution Microsoft Exchange Server	Non	Oui

Vous pouvez procéder à la mise à niveau de Worry-Free Business Security Standard vers Worry-Free Business Security Advanced en obtenant un code d'activation auprès de Trend Micro.

Mises à niveau vers la version complète ou Advanced

Procédure

1. Dans la console Web, accédez à **Administration > Licence du produit**.
2. Si vous disposez d'un code d'activation, cliquez sur **Entrer un nouveau code**, saisissez-le dans le champ **Nouveau code d'activation**, puis cliquez sur **Activer**.

Si vous ne disposez pas d'un code d'activation, visitez le site Web de Trend Micro <http://olr.trendmicro.com> pour procéder à l'enregistrement en ligne et obtenir votre code d'activation.

Annexe A

Assistance technique

Découvrez les rubriques suivantes :

Ressources de dépannage

Avant de contacter le service d'assistance technique, consultez les ressources d'aide en ligne suivantes fournies par Trend Micro.

Utilisation du portail d'assistance

Le portail d'assistance de Trend Micro est une ressource en ligne disponible 24 h/24 et 7 j/7 qui contient les informations les plus récentes à la fois sur les problèmes courants et exceptionnels.

Procédure

1. Accédez à <http://esupport.trendmicro.com>.
2. Sélectionnez un des produits disponibles ou cliquez sur le bouton approprié pour chercher des solutions.
3. Utilisez la zone **Recherche de support** pour rechercher les solutions disponibles.
4. Si aucune solution n'est trouvée, cliquez sur **Contactez l'Assistance** et sélectionnez le type d'assistance dont vous avez besoin.



Conseil

Pour envoyer une demande d'assistance en ligne, visitez l'adresse suivante :

<http://esupport.trendmicro.com/srf/srfmain.aspx>

Un ingénieur d'assistance Trend Micro étudie le cas et répond en 24 heures maximum.

Encyclopédie des menaces

De nos jours, la plupart des programmes malveillants sont des menaces combinées : deux technologies ou plus qui sont combinées afin de

contourner les protocoles de sécurité des ordinateurs. Trend Micro lutte contre ces programmes malveillants complexes grâce à des produits qui créent une stratégie de défense personnalisée. L'Encyclopédie des menaces fournit une liste complète des noms et des symptômes de plusieurs menaces combinées, y compris les programmes malveillants, spams, URL malveillantes et failles connues.

Accédez à <http://about-threats.trendmicro.com/fr/threatencyclopedia#malware> pour en savoir plus sur :

- Les programmes malveillants et les codes mobiles malveillant actuellement actifs ou « en circulation »
- Les pages contenant des informations relatives aux menaces rassemblées pour former un historique complet des attaques Web
- Les informations sur les menaces Internet concernant les attaques ciblées et les menaces de sécurité
- Les informations sur les attaques Web et sur les tendances sur Internet
- Rapports hebdomadaires sur les programmes malveillants.

Comment contacter Trend Micro

Les revendeurs Trend Micro peuvent être contactés par téléphone ou courrier électronique :

Adresse	Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Téléphone	+33 (0) 1 76 68 65 00
Site Web	http://www.trendmicro.fr

Adresse
électronique

sales@trendmicro.fr

- Sites d'assistance à travers le monde :
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Comment contacter Trend Micro :
<http://www.trendmicro.fr/apropos/contact/index.html>
- Documentation sur les produits Trend Micro :
<http://docs.trendmicro.com/fr-fr/home.aspx>

Optimisation de la demande d'assistance

Pour améliorer la résolution de vos problèmes, préparez les informations suivantes :

- Étapes permettant de reproduire le problème
- Informations concernant l'appareil ou le réseau
- Marque de l'ordinateur, modèle et tout matériel complémentaire ou périphériques connectés
- Quantité de mémoire et d'espace disque disponible
- Version du système d'exploitation et du Service Pack
- Version de l'agent installé
- Numéro de série ou code d'activation
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché

Envoi de contenu suspect à Trend Micro

Plusieurs façons d'envoyer du contenu suspect à Trend Micro pour une analyse plus poussée sont à votre disposition.

services de réputation de messagerie (Email Reputation Services)

Lancez une interrogation de la réputation d'une adresse IP spécifique et indiquez un agent de transfert de messages à inclure dans la liste globale des éléments approuvés :

<https://ers.trendmicro.com/>

Reportez-vous à l'entrée suivante de la Base de connaissances pour envoyer des échantillons de messages à Trend Micro :

<https://success.trendmicro.com/solution/1112106>

Services de File Reputation

Collectez des informations système et envoyez le contenu de fichiers suspects à Trend Micro :

<https://success.trendmicro.com/solution/1059565>

Notez le numéro de dossier à des fins de suivi.

Services de réputation de sites Web

Lancez une interrogation de l'évaluation de sécurité et du type de contenu d'une URL que vous pensez correspondre à un site de phishing ou un autre « vecteur de menaces » (source de menaces Internet intentionnelles telles que les spywares et programmes malveillants) :

<http://global.sitesafety.trendmicro.com/>

Si l'évaluation attribuée est incorrecte, envoyez une demande de reclassification à Trend Micro.

Autres ressources

Outre les solutions et l'assistance disponibles en ligne, d'autres ressources, dont le but est de maintenir à jour vos systèmes, de vous informer des innovations les plus récentes et de vous faire connaître les dernières tendances en matière de sécurité, sont également consultables.

Centre de téléchargement

Trend Micro est susceptible de publier, de temps à autre, un patch corrigeant un problème connu ou une mise à niveau s'appliquant à un produit ou service particulier. Pour savoir si des patches sont disponibles, rendez-vous sur le site :

<http://downloadcenter.trendmicro.com/index.php?regs=fr>

Si l'un des patches disponibles n'a pas été appliqué (les patches sont datés), ouvrez le fichier Lisez-moi afin de déterminer s'il convient à votre environnement. Le fichier Lisez-moi contient également des instructions d'installation.

Commentaires relatifs à la documentation

Trend Micro cherche toujours à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez consulter le site suivant^o:

<http://www.trendmicro.com/download/documentation/rating.asp>

Index

A

assistance

 résout les problèmes plus
 rapidement, A-4

C

commentaires relatifs à la
documentation, A-6

console Web, 1-8
 à propos de..., 1-8

D

documentation, vi

P

port

 port d'écoute du serveur, 3-8

S

Serveur OfficeScan
 fonctions, 2-6

W

WFBS

 documentation, vi



TREND MICRO INCORPORATED

Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Tél. : +33 (0)176 68 65 00 info@trendmicro.com

www.trendmicro.com

Item Code: WFFM108709/190701