TREND MICRO™

3.1

TREND MICRO™ Smart Protection Server

Manuel de l'administrateur

Une sécurité plus intelligente

Endpoint Security

Messaging Security

Protected Cloud

Web Security

N° de référence du document : APFM37522/160819

Date de publication : Octobre 2016

Protégée par le brevet américain n°: Brevets en instance.

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

Vous trouverez des informations détaillées sur la façon d'utiliser des fonctionnalités spécifiques du produit/service dans le centre d'aide en ligne Trend Micro et/ou dans la base de connaissances Trend Micro.

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 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

Chapitre 1: Introduction

Chapitre 2: Utilisation de Smart Protection Server

Chapitre 3: Surveillance de Smart Protection Server

Chapitre 4: Intégration à Trend Micro Control Manager

Chapitre 5: Obtenir de l'aide

Annexe A: Commandes de l'interface de ligne de commande (CLI)

Index

Préface

Préface

Bienvenue dans le Manuel de l'administrateur Smart Protection Server™. Ce document contient des informations sur les paramètres du produit.

Les rubriques sont les suivantes :

À propos de Trend Micro

Trend Micro Incorporated fournit des logiciels et des services de sécurité de protection antivirus, anti-spam et de filtrage de contenu. Trend Micro permet à ses clients du monde entier d'empêcher du code malveillant d'endommager leurs ordinateurs.

Documentation du produit

La documentation de Smart Protection Server comprend les éléments suivants :

DOCUMENTATION	DESCRIPTION
Guide d'installation et de mise à niveau	Il vous aide à planifier l'installation, les mises à niveau et le déploiement.
Manuel de l'administrateur	Il vous aide à configurer tous les paramètres du produit.
Aide en ligne	Elle fournit des instructions détaillées sur chaque champ et sur la manière de configurer toutes les fonctions via l'interface utilisateur.
Fichier Lisez-moi	Il contient des informations récentes relatives au produit qui n'ont peut-être pas été intégrées les autres documents. Les rubriques contiennent une description des fonctionnalités, des conseils d'installation, des problèmes connus, ainsi que l'historique des versions du produit.

La documentation est disponible à l'adresse suivante :

http://downloadcenter.trendmicro.com/?regs=FR

Public cible

La documentation relative à Smart Protection Server™ s'adresse aux responsables informatiques et aux administrateurs. Elle suppose que le lecteur dispose d'une connaissance approfondie des réseaux informatiques.

Par contre, elle ne considère pas que le lecteur ait des connaissances en matière de prévention contre les virus/programmes malveillants ou de technologie anti-spam.

Conventions typographiques du document

Le Guide de l'utilisateur Smart Protection Server™ utilise les conventions suivantes.

TABLEAU 1. 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 et options
Chemin > **de navigation**	Chemin de navigation permettant d'accéder à un écran particulier Par exemple, **Fichier** > **Enregistrer** signifie que vous devez cliquer sur **Fichier**, puis sur **Enregistrer** dans l'interface.
 **Remarque**	Remarques sur la configuration
 **Conseil**	Recommandations ou suggestions
 **AVERTISSEMENT!**	Actions critiques et options de configuration

Chapitre 1

Introduction

Ce chapitre présente et décrit les fonctions de Trend Micro™ Smart Protection Server™.

Les rubriques sont les suivantes:

Mode de fonctionnement de Trend Micro Smart Protection Server

Trend Micro™ Smart Protection Server™ est une solution de protection avancée de nouvelle génération basée sur le Web. Au cœur de cette solution réside une architecture de scan avancée qui exploite les signatures anti-programmes malveillants stockées en ligne.

Cette solution tire parti des technologies File Reputation et de réputation de sites Web pour détecter les risques de sécurité. Cette technologie opère en transférant un nombre important de listes et de signatures anti-programmes malveillants auparavant stockées sur des points finaux vers le serveur Trend Micro Smart Protection Server.

Cette démarche réduit considérablement l'impact sur les systèmes et sur le réseau du volume sans cesse croissant de mises à jour de signatures vers les points finaux.

Le besoin d'une nouvelle solution

Dans l'approche actuelle de la gestion des menaces basées sur les fichiers, les signatures (ou les définitions) requises pour protéger un point final sont, pour la plupart, fournies sur la base d'une planification. Trend Micro envoie les signatures par lots vers les points finaux. À la réception d'une nouvelle mise à jour, le logiciel de protection contre les virus/programme malveillants du point final recharge en mémoire ce lot de définitions de signatures de nouveaux risques. En cas de nouveau virus/programme malveillant, cette signature doit à nouveau être mise à jour partiellement ou entièrement et rechargée sur le point final pour assurer une protection continue.

Avec le temps, le volume des nouvelles menaces a connu une augmentation significative. Une progression du nombre de menaces quasi-exponentielle est prévue dans les années à venir. Avec un tel taux de croissance, le nombre de risques de sécurité actuellement connus sera prochainement largement dépassé. À l'avenir, le volume des risques de sécurité représentera en soi un nouveau type de risque de sécurité. Il peut avoir un impact sur les performances des serveurs et des postes de travail, l'utilisation de la bande passante du réseau et, en général, le temps nécessaire pour fournir une protection efficace (« délai de protection »).

Trend Micro a adopté une nouvelle approche dans la gestion du volume des menaces. Elle vise à protéger les utilisateurs de Trend Micro contre le risque que représente ce

volume lui-même. Cet effort d'innovation tire parti d'une technologie et d'une architecture qui permettent de transférer en ligne le stockage des signatures de virus/programmes malveillants. Trend Micro est ainsi à même de mieux protéger les clients contre le volume de nouveaux risques de sécurité.

Solutions Smart Protection Network

Le processus de requête en ligne utilise deux technologies basées sur le réseau :

- Trend Micro™ Smart Protection Network™ : infrastructure Internet d'envergure mondiale visant à fournir des services aux utilisateurs qui ne bénéficient pas d'un accès direct à leur réseau d'entreprise
- Smart Protection Server : Le serveur Smart Protection Server appartient au réseau local. Ils sont mis à la disposition des utilisateurs qui ont accès à leur réseau d'entreprise local. Ces serveurs sont conçus dans le but de localiser les opérations sur le réseau d'entreprise afin d'assurer une efficacité optimale

Remarque

Installez plusieurs serveurs Smart Protection Server pour assurer la continuité de la protection dans le cas où la connexion à un serveur Smart Protection Server n'est pas possible.

Ces deux solutions basées sur le réseau hébergent la plupart des définitions de virus/programmes malveillants et des scores de réputation Web. Trend Micro™ Smart Protection Network™ et Smart Protection Server mettent ces définitions à la disposition des autres points finaux du réseau afin de vérifier les menaces potentielles. Les requêtes ne sont envoyées aux serveurs Smart Protection que si le point final ne parvient pas à déterminer le risque du fichier ou de l'URL.

Les points finaux utilisent les technologies File Reputation et de réputation de sites Web pour envoyer des requêtes aux serveurs Smart Protection Server dans le cadre de leurs activités régulières de protection du système. Dans cette solution, les agents envoient aux serveurs Smart Protection Server, à titre de requête, des informations d'identification déterminées par la technologie Trend Micro. Les agents n'envoient jamais le fichier entier lorsqu'ils utilisent la technologie File Reputation. Le risque du fichier est déterminé à l'aide des informations d'identification.

Fichiers de signatures

Les fichiers de signatures Smart protection sont utilisés pour les services de File Reputation et de réputation de sites Web. Trend Micro publie ces fichiers de signatures par le biais du serveur ActiveUpdate de Trend Micro.

Les éléments suivants sont les fichiers de signatures :

TABLEAU 1-1. Fichiers de signatures de Smart Protection Server

SERVICE DE RÉPUTATION	SIGNATURES	DÉTAILS
Services de File Reputation	**Fichier de signatures Smart Scan**	Le processus de requête en ligne utilise le fichier de signatures Smart Scan associé à un système de requête en ligne en temps réel. Le système de requête en ligne vérifie les fichiers, les URL et autres composants par rapport à un serveur Smart Protection Server au cours du processus de vérification. Les serveurs Smart Protection Server utilisent divers algorithmes pour garantir un processus efficace qui utilise un minimum de bande passante réseau. Le fichier de signatures Smart Scan est mis à jour automatiquement toutes les heures.

SERVICE DE RÉPUTATION	SIGNATURES	DÉTAILS
Services de réputation de sites Web	**Signatures de blocage Web**	Les produits qui utilisent les services de réputation de sites Web (tels qu'OfficeScan et Deep Security) vérifient la réputation d'un site Web par rapport aux signatures de blocage Web en envoyant des requêtes de réputation de sites Web à Smart Protection Server. Ces produits mettent en corrélation les données de réputation reçues de la source Smart Protection avec la stratégie de réputation de sites Web appliquée sur l'endpoint. Selon la stratégie, ils autorisent ou bloquent l'accès au site. **Remarque** Pour obtenir la liste des produits qui utilisent les services de réputation de sites Web, consultez le document : *Intégration aux produits et services Trend Micro à la page 2-30*

Processus de mise à jour des signatures

Les mises à jour de signatures sont une réponse aux menaces de sécurité. Smart Protection Network et les serveurs Smart Protection Server téléchargent le fichier Smart Scan Pattern à partir de serveurs ActiveUpdate. Les produits Trend Micro qui prennent

en charge les serveurs Smart Protection Server téléchargent les fichiers Smart Scan Agent Pattern à partir de serveurs ActiveUpdate.

Les points finaux au sein de votre intranet téléchargent les fichiers Smart Scan Agent Pattern depuis les produits Trend Micro qui prennent en charge les serveurs Smart Protection Server. Les points finaux externes sont des points finaux situés hors de l'intranet et qui ne peuvent pas se connecter aux serveurs Smart Protection Server ou à des produits Trend Micro prenant en charge les serveurs Smart Protection Server.

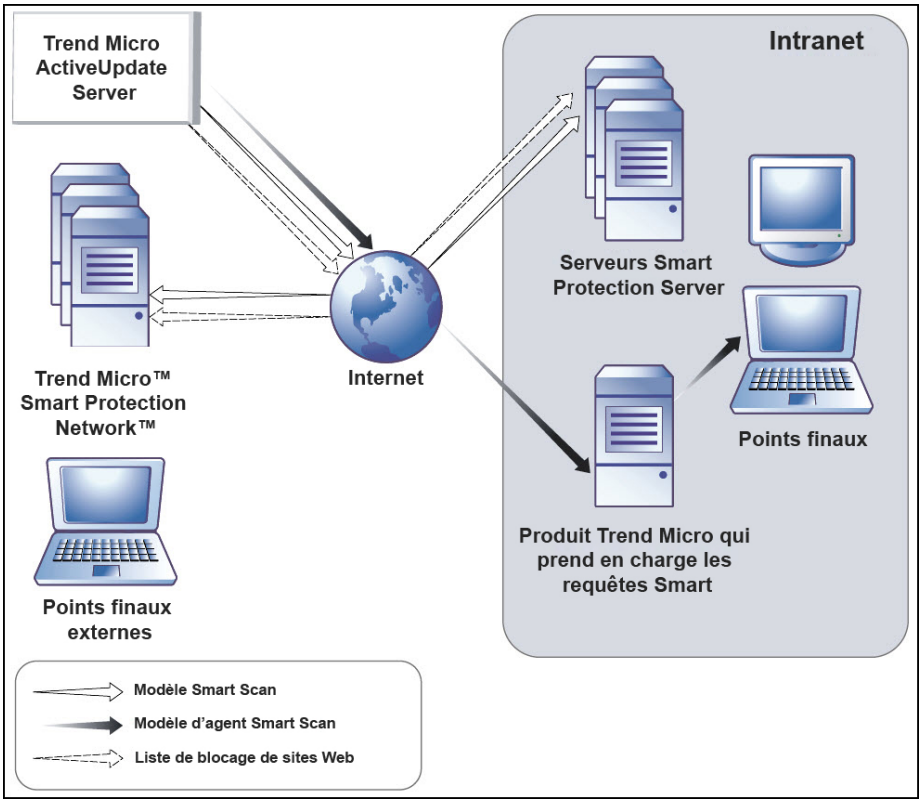


FIGURE 1-1. Processus de mise à jour des signatures

Processus de requête

Les points finaux qui sont actuellement dans votre intranet utilisent des serveurs Smart Protection Server pour les requêtes. Ceux qui ne se trouvent pas dans votre intranet peuvent se connecter à Trend Micro Smart Protection Network dans ce but.

Si une connexion réseau est requise pour utiliser des serveurs Smart Protection Server, les points finaux sans accès à une connexion réseau bénéficient néanmoins de la technologie Trend Micro. Smart Scan Agent Pattern et la technologie de scan qui résident sur les points finaux protègent ceux d'entre eux qui n'ont pas accès à une connexion réseau.

Les agents installés sur les points finaux effectuent d'abord un scan du point final. S'ils ne parviennent pas à déterminer le risque que présente le fichier ou l'URL, ils vérifient ce risque en envoyant une requête à un serveur Smart Protection Server.

TABLEAU 1-2. Comportements de protection en fonction de l'accès à l'intranet

EMPLACEMENT	FICHIER DE SIGNATURES ET COMPORTEMENT DE REQUÊTE
Accès à l'intranet	• **Fichiers de signatures** : les points finaux téléchargent le fichier Smart Scan Agent Pattern depuis les produits Trend Micro qui prennent en charge les serveurs Smart Protection Server. • **Requêtes** : les points finaux se connectent à Smart Protection Server pour les requêtes.

EMPLACEMENT	FICHIER DE SIGNATURES ET COMPORTEMENT DE REQUÊTE
Sans accès à intranet	• **Fichiers de signatures** : les points finaux ne téléchargent pas le dernier fichier Smart Scan Agent Pattern, à moins qu'une connexion à un produit Trend Micro prenant en charge les serveurs Smart Protection Server ne soit disponible. • **Requêtes** : les points finaux scannent les fichiers de ressources locales telles que le fichier Smart Scan Agent Pattern.

La technologie de filtre avancée permet à l'agent de « mettre en mémoire cache » le résultat de la requête. Cela améliore les performances de scan et évite d'envoyer plusieurs fois la même requête aux serveurs Smart Protection Server.

Un agent qui ne peut pas vérifier localement le risque lié à un fichier et qui ne peut pas se connecter à un serveur Smart Protection Server après plusieurs tentatives marque le fichier pour vérification et le rend temporairement accessible. Lorsque la connexion à un serveur Smart Protection Server est restaurée, tous les fichiers marqués d'un indicateur sont scannés à nouveau. L'action de scan appropriée est ensuite menée sur les fichiers qui constituent une menace avérée pour votre réseau.

Conseil

Installez plusieurs serveurs Smart Protection Server pour assurer la continuité de la protection dans le cas où la connexion à un serveur Smart Protection Server n'est pas possible.

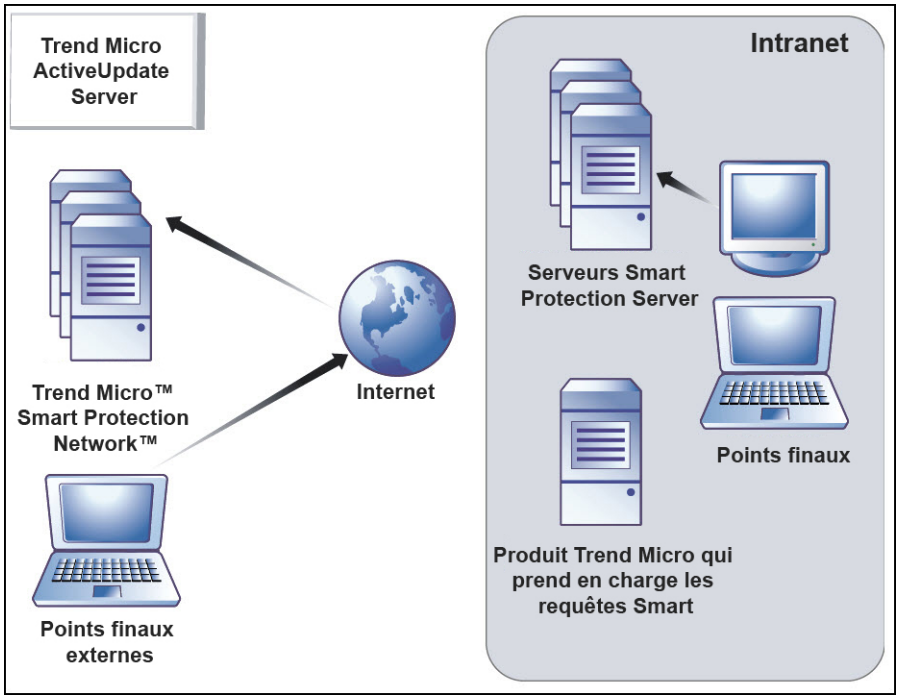


FIGURE 1-2. Processus de requête

Nouveautés de cette version

Trend Micro Smart Protection Server inclut les nouvelles fonctionnalités et améliorations suivantes :

TABLEAU 1-3. Nouveautés de la version 3.1

FONCTION	DESCRIPTION
Proxy du service Smart Protection d'OfficeScan	Smart Protection Server redirige les demandes de requêtes d'apprentissage automatique prédictif et de surveillance des comportements d'OfficeScan vers Smart Protection Network.

FONCTION	DESCRIPTION
Protocole du serveur ActiveUpdate	Les communications du serveur ActiveUpdate utilisent par défaut le protocole HTTPS. **Remarque** Les communications ActiveUpdate prennent toujours en charge le protocole HTTP.
Modifications de la configuration par défaut	• La fréquence de synchronisation par défaut de la liste d'objets suspects est passée de 60 minutes à 10 minutes. • La fréquence de synchronisation par défaut du serveur ActiveUpdate est passée de 60 minutes à 15 minutes.

Fonctionnalités et avantages principaux

Trend Micro Smart Protection Server offre les fonctionnalités et les avantages suivants :

- Technologie File Reputation
  - Le réseau d'entreprise sera mieux en mesure de faire face au risque que constitue le volume des menaces.
  - Le « délai de protection » global contre les nouvelles menaces diminue considérablement.
  - La mémoire utilisée par le noyau sur les postes de travail est extrêmement réduite et augmente peu dans le temps.
  - Rationalise l'administration et simplifie la gestion. Au lieu d'être diffusée sur de nombreux postes de travail, la masse des mises à jour des définitions de signatures est simplement fournie à un serveur. Ceci réduit l'impact de la mise à jour des signatures sur un grand nombre de postes de travail.
  - Protège contre les attaques Web et mixtes.

- Arrête les virus/programmes malveillants, les chevaux de Troie, les vers, ainsi que les nouvelles variantes de ces risques de sécurité.
- Détecte et supprime les spywares/graywares (y compris les rootkits cachés).

- Technologie de réputation de sites Web
  - Protège contre les attaques Web et mixtes.
  - Les clients soucieux de la confidentialité de leurs données n'ont pas à craindre de voir leurs informations confidentielles révélées lors des requêtes de réputation de sites Web adressées à Smart Protection Network.
  - Le temps de réponse aux requêtes de Smart Protection Server est réduit comparativement aux requêtes adressées à Smart Protection Network.
  - L'installation d'un serveur Smart Protection Server dans votre réseau réduit la charge de la passerelle en termes de bande passante.

Trend Micro Smart Protection Network

Trend Micro™ Smart Protection Network™ est une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques liés à la sécurité et les menaces Web. Il repose sur des solutions à la fois locales et hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage, à l'aide d'agents légers permettant d'accéder à une combinaison unique de technologies en ligne de messagerie, File Reputation et de réputation de sites Web alliées à des bases de données de menaces. À mesure que de nouveaux produits, services et utilisateurs accèdent au réseau, la sécurité des clients est automatiquement mise à jour et renforcée, créant ainsi un service de protection de voisinage en temps réel pour les utilisateurs.

Services de File Reputation

Les services de File Reputation vérifient la réputation de chaque fichier par rapport à une base de données en ligne étendue. Les informations sur les programmes malveillants étant stockées en ligne, elles sont instantanément accessibles à tous les utilisateurs. Des réseaux de transmission de contenu et des serveurs de cache très performants

garantissent un temps de latence minimum pendant le processus de vérification. L'architecture de client en ligne procure une protection immédiate et élimine la contrainte liée au déploiement de fichiers de signature tout en réduisant sensiblement l'encombrement de l'agent.

Services de réputation de sites Web

Dotée de l'une des plus grandes bases de données de réputation de domaine du monde, la technologie de réputation de sites Web de Trend Micro assure le suivi de la crédibilité des domaines Web en attribuant un score de réputation dépendant de facteurs tels que l'ancienneté du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. Elle continue ensuite à analyser les sites et à bloquer les utilisateurs tentant d'accéder à ceux qui sont infectés. Les fonctionnalités de réputation de sites Web permettent de garantir que les pages consultées par les utilisateurs sont sûres et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing visant à duper les utilisateurs afin de leur faire divulguer des informations personnelles. Pour une plus grande précision et une réduction des faux positifs, la technologie de réputation de sites Web de Trend Micro affecte des scores de réputation à des pages et liens spécifiques de chaque site, plutôt que de classer comme suspects des sites entiers ou de les bloquer. En effet, il arrive souvent que seule une portion d'un site légitime ait été piratée et les réputations peuvent changer de manière dynamique au fil du temps

Les fonctionnalités de réputation de sites Web permettent de garantir que les pages Web consultées par les utilisateurs sont sûres et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing visant à duper les utilisateurs afin de leur faire divulguer des informations personnelles. La réputation de sites Web bloque les pages Web en fonction de l'évaluation de leur réputation. Lorsqu'elle est activée, la réputation de sites Web contribue à dissuader les utilisateurs d'accéder à des URL malveillantes.

Smart Feedback

Trend Micro™ Smart Feedback assure une liaison permanente entre les produits Trend Micro et avec les centres et technologies de recherche des menaces de la société 24 heures sur 24 et 7 jours sur 7. Chaque nouvelle menace identifiée par un contrôle de

réputation de routine d'un seul client met automatiquement à jour toutes les bases de données de menaces de Trend Micro, et empêche que cette menace ne survienne à nouveau chez un autre client. Grâce à l'analyse constante des données de menaces collectées par son vaste réseau mondial de clients et de partenaires, Trend Micro assure une protection automatique et en temps réel contre les dernières menaces, offrant ainsi une sécurité « unifiée », très semblable à une surveillance de voisinage automatisée qui implique la communauté dans la protection de chacun. La confidentialité des informations personnelles ou professionnelles d'un client est toujours protégée car les données sur les menaces qui sont collectées reposent sur la réputation de la source de communication et non sur le contenu de la communication en question.

Chapitre 2

Utilisation de Smart Protection Server

Ce chapitre fournit des informations sur la configuration de Trend Micro™ Smart Protection Server™.

Les rubriques sont les suivantes:

Configuration initiale

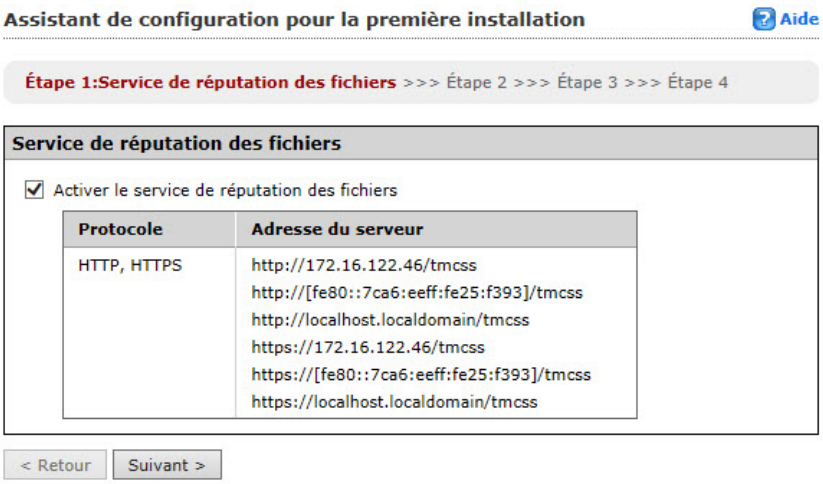
Après l'installation, effectuez les actions suivantes.

Procédure

1. Connectez-vous à la console Web.

   L'assistant de première installation apparaît.

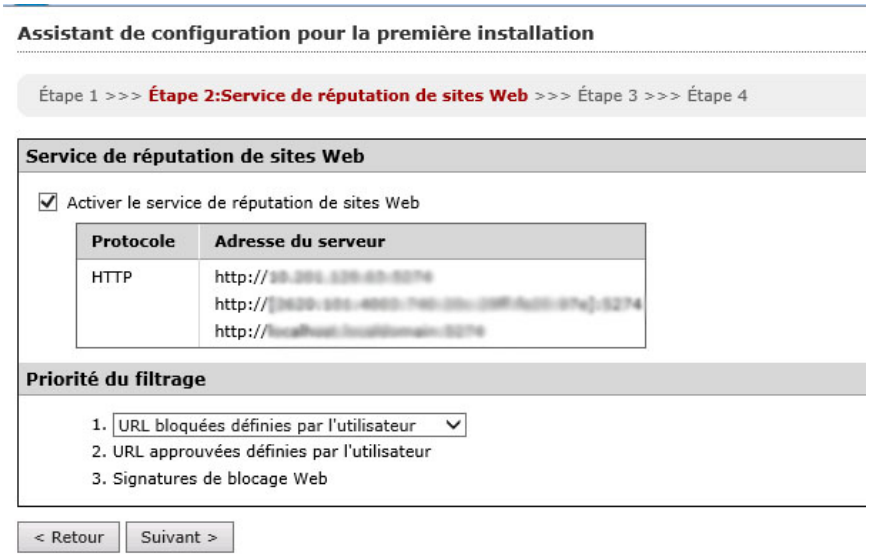
2. Cochez la case **Activer le service File Reputation** pour utiliser la réputation de fichiers.



3. Cliquez sur **Suivant**.

   L'écran Service de réputation de sites Web s'affiche.

4. Cochez la case **Activer le service de réputation de sites Web** pour activer la réputation de sites Web.



5. (Facultatif) Les paramètres Priorité du filtrage vous permettent de spécifier l'ordre des requêtes d'URL.

6. Cliquez sur **Suivant**.

   L'écran Smart Feedback s'affiche.

7. Choisissez d'utiliser Smart Feedback pour aider Trend Micro à fournir des solutions plus rapides aux nouvelles menaces.

8. Cliquez sur **Suivant**.

   L'écran Paramètres proxy s'affiche.

9. Spécifiez les paramètres de proxy si votre réseau utilise un serveur proxy.

10. Cliquez sur **Terminer** pour terminer la configuration initiale de Smart Protection Server.

    L'écran Résumé de la console Web s'affiche.

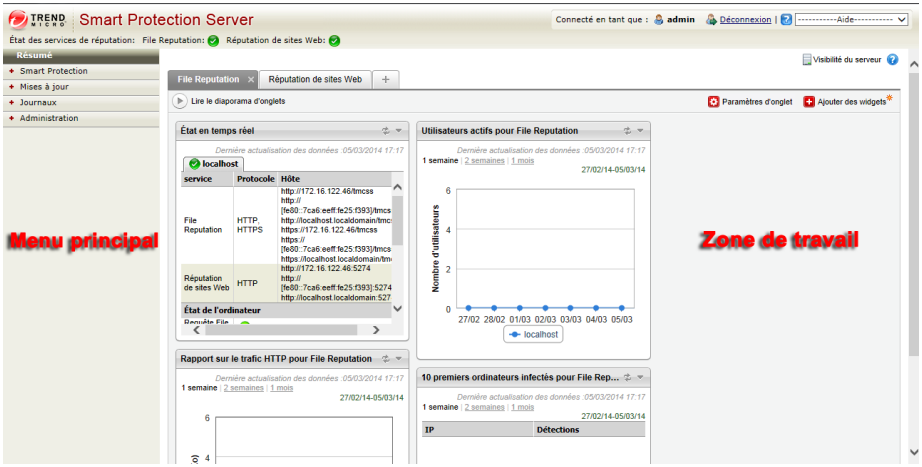
> **Remarque**
>
> Smart Protection Server mettra automatiquement à jour les fichiers de signatures après la configuration initiale.

Utilisation de la console du produit

La console du produit comprend les éléments suivants :

- **Menu principal** : Fournit des liens vers les écrans **Récapitulatif**, **Smart Protection**, **Mises à jour**, **Journaux** et **Administration**.

- **Zone de travail** : affichez des informations résumées et l'état des composants, configurez les paramètres, mettez à jour les composants et effectuez des tâches administratives.



Menu	Description
Résumé	Affiche des informations personnalisées sur les serveurs Smart Protection Server, le trafic et les détections lorsque vous ajoutez des widgets.
Smart Protection	Fournit des options pour la configuration des services de réputation, de la liste des URL définies par l'utilisateur, des objets suspects et de Smart Feedback.
Mises à jour	Fournit des options pour la configuration des mises à jour programmées, des mises à jour manuelles du programme, des téléchargements des packs du programme et de la source de mise à jour.
Journaux	Fournit des options pour interroger les journaux et pour la maintenance des journaux.

MENU	DESCRIPTION
Administration	Fournit des options pour configurer le service SNMP, les notifications, les paramètres proxy et collecter des informations de diagnostic pour le dépannage.

Accès à la console produit

Une fois que vous êtes connecté à la console Web, l'écran initial affiche le résumé de l'état des serveurs Smart Protection Server.

Procédure

1. Ouvrez un navigateur Web et saisissez l'URL indiquée sur la bannière CLI initiale après l'installation.
2. Saisissez `admin` comme nom d'utilisateur et mot de passe dans les champs correspondants.
3. Cliquez sur **Connexion**.

Utilisation de Smart Protection

Cette version de Smart Protection Server inclut les services de File Reputation et de réputation de sites Web.

Utilisation des services de réputation

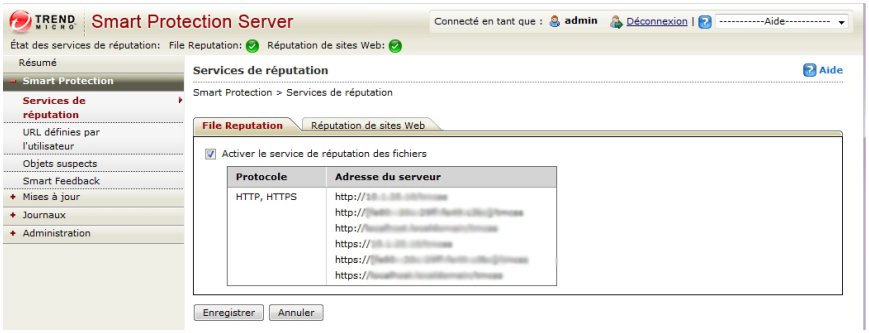
Activez les services de réputation à partir de la console du produit pour permettre aux autres produits Trend Micro d'utiliser Smart Scan.

Activation des services de File Reputation

Activez les services de File Reputation pour prendre en charge les requêtes des endpoints.

Procédure

1. Accédez à **Smart Protection** > **Services de réputation**, puis à l'onglet **File Reputation**.



2. Cochez la case **Activer le service File Reputation**.

3. Cliquez sur **Enregistrer**.

   L'adresse du serveur peut maintenant être utilisée pour les requêtes File Reputation par d'autres produits Trend Micro qui prennent en charge les serveurs Smart Protection Server.

Activation des services de réputation de sites Web

Activez les services de réputation de sites Web pour prendre en charge les requêtes d'URL des endpoints. Voici les options disponibles sur cet écran.

- **Activer le service de réputation de sites Web** : sélectionnez cette option pour prendre en charge les requêtes de réputation de sites Web des endpoints.
- **Adresse du serveur** : utilisé par d'autres produits Trend Micro pour les requêtes de réputation de sites Web.
- **Priorité du filtrage** : sélectionnez cette option pour spécifier la priorité lors du filtrage des URL.

Procédure

1. Accédez à **Smart Protection** > **Services de réputation**, puis cliquez sur l'onglet **Réputation de sites Web**.

2. Cochez la case **Activer le service de réputation de sites Web**.

3. (Facultatif) Spécifiez la priorité des URL approuvées et bloquées définies par l'utilisateur lors du filtrage des URL. Par exemple, si la première priorité est **URL bloquées définies par l'utilisateur**, la seconde priorité est alors **URL approuvées définies par l'utilisateur**.

4. Cliquez sur **Enregistrer**.

   L'adresse du serveur peut désormais être utilisée pour les requêtes File Reputation par d'autres produits Trend Micro qui prennent en charge Smart Protection Server.

Configuration des URL définies par l'utilisateur

Les URL définies par l'utilisateur vous permettent de spécifier vos propres URL approuvé ou bloquées. Cette liste est utilisée pour la réputation de sites Web. Voici les options disponibles sur cet écran.

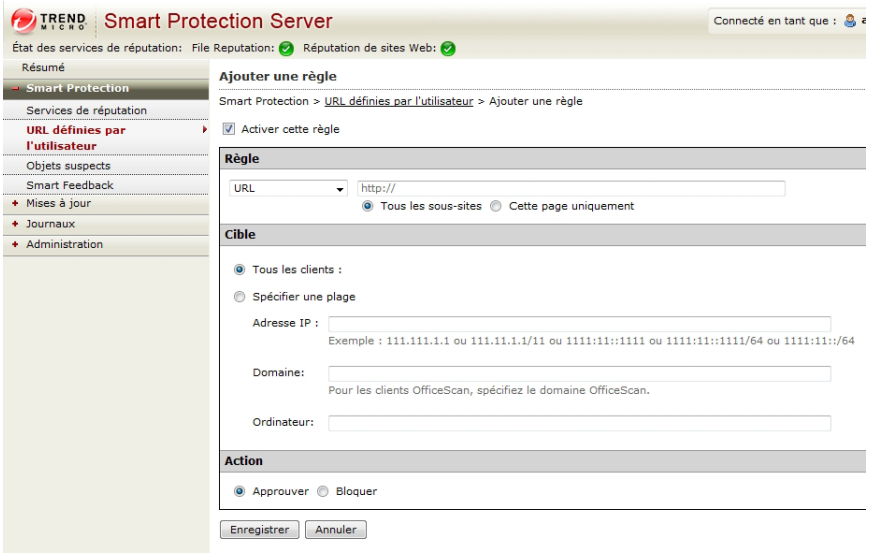
- **Règle de recherche** : sélectionnez cette option pour rechercher une chaîne dans la liste des règles.

- **Tester l'URL** : sélectionnez cette option pour rechercher les règles que l'URL déclenchera. L'URL doit commencer par `http://` ou `https://`.

Procédure

1. Accédez à **Smart Protection** > **URL définies par l'utilisateur**.
2. Sous **Critères de recherche**, cliquez sur **Ajouter**.

   L'écran **Ajouter une règle** apparaît.



3. Cochez la case **Activer cette règle**.
4. Sélectionnez l'une des options suivantes :

   - **URL** : pour spécifier une URL et l'appliquer à tous ses sous-sites ou seulement à une page.
   - **URL avec mot-clé** : pour spécifier une chaîne et utiliser des expressions rationnelles.

Cliquez sur **Tester** pour afficher les résultats de l'application de cette règle aux URL suivantes parmi les 20 URL les plus courantes et aux 100 premières URL du jour précédent dans le journal d'accès Web.

5. Sélectionnez l'une des options suivantes :

   - **Tous les clients** : pour appliquer l'opération à tous les clients.
   - **Spécifier une plage** : application à une plage d'adresses IP, de noms de domaines et de noms d'ordinateurs.

   Remarque

   Cela prend en charge les adresses IPv4 et IPv6.

6. Sélectionnez **Approuver** ou **Bloquer**.
7. Cliquez sur **Enregistrer**.

Importer les URL définies par l'utilisateur

Utilisez cet écran pour importer des URL définies par l'utilisateur à partir d'un autre Smart Protection Server. Voici les options disponibles sur cet écran.

- **Parcourir** : cliquez sur cette option pour sélectionner un fichier `.csv` sur votre ordinateur.
- **Télécharger** : cliquez sur cette option pour télécharger le fichier `.csv` sélectionné.
- **Annuler** : cliquez sur cette option pour revenir à l'écran précédent.

Configuration des objets suspects

Un objet suspect est une adresse IP malveillante ou potentiellement malveillante, un domaine, une URL ou une valeur SHA-1 connus et trouvés dans les échantillons soumis.

Smart Protection Server peut s'abonner aux listes suivantes pour synchroniser les objets suspects :

TABLEAU 2-1. Source d'objets suspects de Smart Protection Server

SOURCE	TYPE D'OBJETS SUSPECTS	DESCRIPTION
Deep Discovery Analyzer • **Virtual Analyzer**	URL	Virtual Analyzer est un environnement virtuel en ligne conçu pour analyser les fichiers suspects. Les images Sandbox permettent d'observer le comportement du fichier dans un environnement qui simule des endpoints sur votre réseau sans risquer de compromettre le réseau. Dans les produits gérés, Virtual Analyzer assure le suivi et analyse les échantillons soumis. Virtual Analyzer marque les objets suspects en fonction de leur potentiel à exposer les systèmes à un danger ou à des pertes.
Control Manager Objets suspects consolidés • **Objets suspects définis par l'utilisateur dans Control Manager** • **Objets suspects de Virtual Analyzer**	URL	Deep Discovery Analyzer envoie une liste d'objets suspects à Control Manager. Les administrateurs Control Manager peuvent ajouter des objets qu'ils considèrent comme suspects, mais qui ne sont pas actuellement dans la liste d'objets suspects de Virtual Analyzer. Les objets suspects définis par l'utilisateur ont une priorité supérieure aux objets suspects de Virtual Analyzer. Control Manager consolide les objets suspects et les actions de scan par rapport aux objets, puis les distribue à Smart Protection Server.

En cas d'abonnement, Smart Protection Server relaie les éléments suivants :

- Informations d'URL suspectes aux produits Trend Micro (tels que les agents OfficeScan, ScanMail et Deep Security) qui envoient des requêtes de réputation de sites Web

- Actions par rapport aux URL suspectes aux agents OfficeScan qui envoient des requêtes de réputation de sites Web.

Remarque

Pour plus d'informations sur la façon dont Control Manager gère les objets suspects, consultez le document : http://docs.trendmicro.com/fr-fr/enterprise/control-manager-60-service-pack-3/whats_new_6sp3/suspicious_object_supported_products.aspx

Procédure

1. Accédez à **Smart Protection** > **Objets suspects**.
2. Saisissez le nom de domaine complet ou l'adresse IP de la **source** d'objets suspects.
3. Saisissez la **clé API** obtenue par la source d'objets suspects.
4. Facultatif : Cliquez sur **Tester la connexion** pour vérifier que le nom de serveur, l'adresse IP et la clé API sont corrects et que la source est disponible.
5. Cliquez sur **S'abonner**.
6. Pour synchroniser immédiatement les objets suspects, sélectionnez **Synchroniser et activer les objets suspects**, puis cliquez sur **Synchroniser maintenant**.

   Remarque

   Cette option est disponible seulement si Smart Protection Server se connecte correctement à la source.

7. Cliquez sur **Enregistrer**.

Activation de Smart Feedback

Trend Micro Smart Feedback partage les informations sur les menaces anonymes avec Trend Micro™ Smart Protection Network™, ce qui permet à Trend Micro d'identifier rapidement les nouvelles menaces et d'y répondre. Vous pouvez désactiver Smart Feedback à tout moment via cette console.

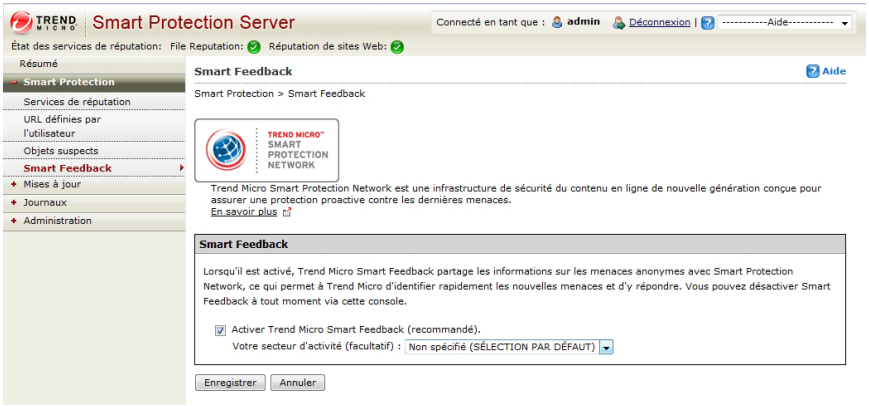
Procédure

1. Accédez à **Smart Protection** > **Smart Feedback**.

Remarque

Vérifiez que le serveur Smart Protection Server dispose d'une connexion Internet avant d'activer Smart Feedback.

2. Sélectionnez **Activer Trend Micro Smart Feedback**.



3. Sélectionnez votre secteur d'activité.

4. Cliquez sur **Enregistrer**.

Mises à jour

Pour être efficace, Smart Protection Server doit utiliser les derniers fichiers de signatures et composants. Trend Micro publie de nouvelles versions des fichiers Smart Scan Pattern toutes les heures.

Conseil

Trend Micro vous recommande de mettre à jour les composants immédiatement après l'installation.

Configuration des mises à jour manuelles

Pour mettre à jour manuellement les fichiers de signatures :

Procédure

1. Accédez à **Mises à jour**.
2. Cliquez sur **Signatures** ou sur **Programme** dans le menu déroulant.
3. Cliquez sur **Mettre à jour** ou sur **Enregistrer et mettre à jour maintenant** pour appliquer les mises à jour immédiatement.

Configuration des mises à jour programmées

Pour effectuer les mises à jour programmées :

Procédure

1. Accédez à **Mises à jour**.
2. Cliquez sur **Signatures** ou sur **Programme** dans le menu déroulant.
3. Programmez les mises à jour.
4. Cliquez sur **Enregistrer**.

Mises à jour des fichiers de signatures

Mettez à jour les fichiers de signatures pour vous assurer que les informations les plus récentes sont appliquées aux requêtes. Voici les options disponibles sur cet écran :

- **Activer les mises à jour programmées** : Sélectionnez cette option pour configurer les mises à jour automatiques toutes les heures ou toutes les 15 minutes.
- **Mettre à jour** : Cliquez sur cette option pour mettre à jour immédiatement tous les fichiers de signatures.

Mises à jour des fichiers programmes

Téléchargez la version la plus récente du produit afin de bénéficier de ses améliorations. Voici les options disponibles sur cet écran.

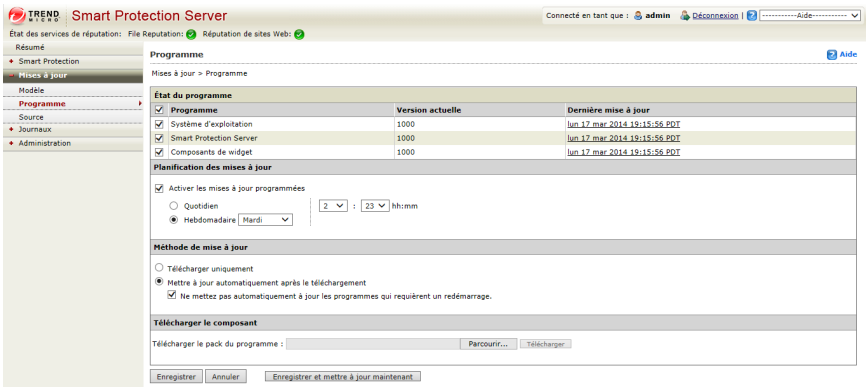
- **Système d'exploitation** : Sélectionnez cette option pour mettre à jour les composants du système d'exploitation.
- **Smart Protection Server** : Sélectionnez cette option pour mettre à jour le fichier du programme du serveur produit.
- **Composant Widgets** : Sélectionnez cette option pour mettre à jour les widgets.
- **Activer les mises à jour programmées** : Sélectionnez cette option pour mettre à jour les fichiers du programme chaque jour à l'heure spécifiée ou chaque semaine.
- **Télécharger uniquement** : Sélectionnez cette option pour télécharger les mises à jour et recevoir une invitation à mettre à jour les fichiers du programme.
- **Mettre à jour automatiquement après le téléchargement** : Sélectionnez cette option pour appliquer toutes les mises à jour au produit après le téléchargement, qu'un redémarrage ou un réamorçage soit requis ou non.
- **Ne mettez pas automatiquement à jour les programmes qui requièrent un redémarrage** : Sélectionnez cette option pour télécharger toutes les mises à jour et n'installer que les programmes qui ne nécessitent pas un redémarrage ou un réamorçage.
- **Télécharger** : Cliquez pour télécharger et mettre à jour un fichier programme pour le serveur Smart Protection Server.
- **Parcourir** : Cliquez pour rechercher un pack de programme.
- **Enregistrer et mettre à jour maintenant** : Cliquez pour appliquer les paramètres et effectuer une mise à jour immédiatement.

Il y a trois façons de mettre à jour le fichier programme : par des mises à jour programmées, des mises à jour manuelles, et en téléchargeant le composant.

Activation des mises à jour programmées

Procédure

1. Accédez à **Mises à jour** > **Programme**.
2. Sélectionnez **Activer les mises à jour programmées** et sélectionnez le programme de mise à jour.



3. Sélectionnez l'une des méthodes de mise à jour suivantes :
   - **Télécharger uniquement** : cochez cette case pour télécharger les fichiers programme sans les installer. Un message apparaît dans la console Web du produit lorsque des mises à jour du fichier programme sont disponibles et peuvent être installées.
   - **Mettre à jour automatiquement après le téléchargement** : cochez cette case pour installer automatiquement les mises à jour du fichier programme lorsqu'elles ont été téléchargées.
     - **Ne mettez pas automatiquement à jour les programmes qui requièrent un redémarrage** : cochez cette case pour qu'un message

s'affiche sur la console Web du produit si la mise à jour nécessite un redémarrage. Les mises à jour du programme qui ne nécessitent pas un redémarrage seront installées automatiquement.

4. Cliquez sur **Enregistrer**.

Exécution des mises à jour manuelles

Procédure

1. Accédez à **Mises à jour** > **Programme**.
2. Sélectionnez l'une des méthodes de mise à jour suivantes :
   - **Télécharger uniquement** : cochez cette case pour télécharger les fichiers programme sans les installer. Un message apparaît dans la console Web du produit lorsque des mises à jour du fichier programme sont disponibles et peuvent être installées.
   - **Mettre à jour automatiquement après le téléchargement** : cochez cette case pour installer automatiquement les mises à jour du fichier programme lorsqu'elles ont été téléchargées.
     - **Ne mettez pas automatiquement à jour les programmes qui requièrent un redémarrage** : cochez cette case pour qu'un message s'affiche sur la console Web du produit si la mise à jour nécessite un redémarrage. Les mises à jour du programme qui ne nécessitent pas un redémarrage seront installées automatiquement.
3. Cliquez sur **Enregistrer et mettre à jour maintenant**.

Téléchargement de fichiers pour effectuer des mises à jour manuelles

Procédure

1. Accédez à **Mises à jour** > **Programme**.

Important

Assurez-vous que le serveur Smart Protection Server n'est pas en train d'effectuer une mise à jour avant de continuer. Si vous devez mettre à jour le programme ou un composant, désactivez d'abord les mises à jour de composants programmées avant de continuer.

2. Sous **Télécharger le composant**, cliquez sur **Parcourir...** pour rechercher le fichier programme pour lequel vous souhaitez faire une mise à jour manuelle.

Remarque

Recherchez le fichier programme que vous avez téléchargé sur le site Web de Trend Micro ou que vous vous êtes procuré auprès de Trend Micro.

3. Localisez le fichier et cliquez sur **Ouvrir**.
4. Cliquez sur **Télécharger**.

Remarque

Si vous avez désactivé le scan programmé afin de mettre à jour le programme ou un composant, réactivez-le après le téléchargement et la mise à jour.

Fichiers programmes disponibles

Utilisez cet écran pour mettre à jour les fichiers programmes disponibles. Voici les options disponibles sur cet écran.

- <Cases à cocher> : cochez la case du programme disponible à mettre à jour.
- **Mettre à jour** : cliquez sur cette option pour mettre à jour les programmes sélectionnés.

Configuration d'une source de mise à jour

Utilisez cet écran pour spécifier la source de mise à jour pour File Reputation et la réputation de sites Web. La source de mise à jour par défaut est le Trend Micro ActiveUpdate Server. Voici les options disponibles sur cet écran.

- **Trend Micro ActiveUpdate Server** : sélectionnez cette option pour télécharger des mises à jour depuis le Trend Micro ActiveUpdate Server.
- **Autre source de mise à jour** : sélectionnez cette option pour spécifier une source de mise à jour telle que Trend Micro Control Manager.

Procédure

1. Accédez à **Mises à jour** > **Source** et sélectionnez l'onglet **File Reputation** ou **Réputation de sites Web**.
2. Sélectionnez **Trend Micro ActiveUpdate Server** ou **Autre source de mise à jour** et saisissez une URL.
3. Cliquez sur **Enregistrer**.

Tâches adminstratives

Les tâches administratives vous permettent de configurer les paramètres du service SNMP, les notifications, les paramètres du serveur proxy ou de télécharger des informations de diagnostic.

Service SNMP

Smart Protection Server prend en charge SNMP pour offrir plus de souplesse dans la surveillance du produit. Configurez les paramètres et téléchargez le fichier MIB à partir de l'écran **Service SNMP**. Voici les options disponibles sur cet écran.

- **Activer le service SNMP** : sélectionnez cette option pour utiliser SNMP.
- **Nom de communauté** : spécifiez un nom de communauté SNMP.
- **Activer la restriction IP** : sélectionnez cette option pour activer la restriction d'adresse IP.

Remarque

Le CIDR (Classless Inter-Domain Routing) n'est pas pris en charge pour la restriction IP. Empêchez tout accès non autorisé au service SNMP en activant la restriction d'adresse IP.

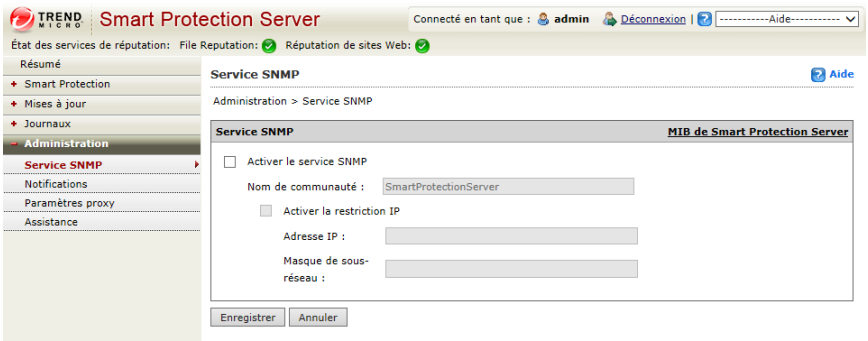
- **Adresse IP** : spécifiez une adresse IP pour utiliser le service SNMP afin de surveiller le bon fonctionnement du système.
- **Masque de sous-réseau** : spécifiez un masque de sous-réseau pour définir la plage d'adresses IP et utiliser le service SNMP afin de surveiller l'état de l'ordinateur.
- **MIB Smart Protection Server** : cliquez sur cette option pour télécharger le fichier MIB du serveur Smart Protection Server.
- **Enregistrer** : cliquez sur cette option pour conserver les paramètres.
- **Annuler** : cliquez sur cette option pour annuler les changements.

Configuration du service SNMP

Configurez les paramètres du service SNMP pour permettre aux systèmes de gestion SNMP de surveiller l'état du serveur Smart Protection Server.

Procédure

1. Accédez à **Administration** > **Service SNMP**.



2. Cochez la case **Activer le service SNMP**.
3. Spécifiez un **nom de communauté**.
4. Cochez la case **Activer la restriction IP** pour prévenir tout accès non autorisé au service SNMP.

   Remarque

   Le CIDR (Classless Inter-Domain Routing) n'est pas pris en charge pour la restriction IP.

5. Spécifiez une adresse IP.
6. Spécifiez un masque de sous-réseau.
7. Cliquez sur **Enregistrer**.

Téléchargement du fichier MIB

Téléchargez le fichier MIB à partir de la console Web pour utiliser le service SNMP.

Procédure

1. Accédez à **Administration** > **Service SNMP**.
2. Cliquez sur **MIB de Smart Protection Server** pour télécharger le fichier MIB. Un message de confirmation apparaît.
3. Cliquez sur **Enregistrer**.

   L'écran **Enregistrer sous** apparaît.
4. Spécifiez l'emplacement de l'enregistrement.
5. Cliquez sur **Enregistrer**.

MIB de Smart Protection Server

Le tableau suivant fournit la description du MIB de Smart Protection Server.

Nom de l'objet	Identificateur de l'objet (OID)	Description
Trend-MIB:: TBLVersion	1.3.6.1.4.1.6101.1.2.1.1	Renvoie la version actuelle du Smart Scan Pattern.
Trend-MIB:: TBLLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.2	Renvoie la date et l'heure de la dernière mise à jour réussie du Smart Scan Pattern.
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101.1.2.1.3	Renvoie l'état de la dernière mise à jour du Smart Scan Pattern. • 0: La dernière mise à jour du fichier de signatures a réussi. • <code d'erreur> : La dernière mise à jour du fichier de signatures a échoué.
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.4	Renvoie un message d'erreur si la dernière mise à jour du fichier Smart Scan Pattern a échoué.
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	Renvoie la version actuelle des signatures de blocage Web.
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	Renvoie la date et l'heure de la dernière mise à jour réussie des signatures de blocage Web.

Nom de l'objet	Identificateur de l'objet (OID)	Description
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Renvoie l'état de la dernière mise à jour des signatures de blocage Web. • 0: La dernière mise à jour du fichier de signatures a réussi. • <code d'erreur> : La dernière mise à jour du fichier de signatures a échoué.
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	Renvoie un message d'erreur si la dernière mise à jour des signatures de blocage Web a échoué.
Trend-MIB:: LastVerifyError	1.3.6.1.4.1.6101.1.2.2.2	Renvoie l'état de la requête de réputation de fichiers. • 0: La requête de File Reputation se comporte comme prévu. • <code d'erreur> : La requête de File Reputation ne se comporte pas comme prévu.

NOM DE L'OBJET	IDENTIFICATEUR DE L'OBJET (OID)	DESCRIPTION
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101.1.2.2.3	Renvoie l'état de la requête de réputation de sites Web. • 0: La requête de réputation de sites Web se comporte comme prévu. • <code d'erreur> : La requête de réputation de sites Web ne se comporte pas comme prévu.
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.4	Renvoie un message d'erreur si le dernier état de fonctionnement d'une requête de File Reputation a échoué.
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.5	Renvoie un message d'erreur si le dernier état de fonctionnement d'une requête de réputation de sites Web a échoué.

MIB pris en charge

Le tableau suivant fournit la description des autres MIB pris en charge.

NOM DE L'OBJET	IDENTIFICATEUR DE L'OBJET (OID)	DESCRIPTION
Système SNMP MIB-2	1.3.6.1.2.1.1	Le groupe système comprend des informations relatives au système sur lequel réside l'entité. Les objets de ce groupe sont utilisés pour la gestion des erreurs et la gestion de la configuration. Voir IETF RFC 1213.
Interfaces SNMP MIB-2	1.3.6.1.2.1.2	Le groupe d'objets des interfaces contient des informations sur chaque interface d'un périphérique réseau. Ce groupe fournit des informations utiles sur la gestion des erreurs, la gestion de la configuration, la gestion des performances et la gestion de la comptabilité. Voir IETF RFC 2863.

Paramètres proxy

Si vous utilisez un serveur proxy dans le réseau, configurez les paramètres proxy. Voici les options disponibles sur cet écran.

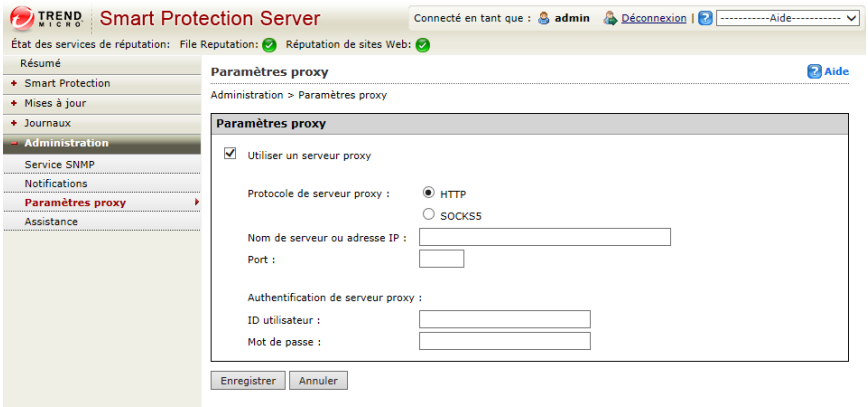
- **Utiliser un serveur proxy** : sélectionnez cette option si votre réseau utilise un serveur proxy.
- **HTTP** : sélectionnez cette option si votre serveur proxy utilise le protocole HTTP.
- **SOCKS5** : sélectionnez cette option si votre serveur proxy utilise le protocole SOCKS5.
- **Nom de serveur ou adresse IP** : saisissez le nom du serveur proxy ou l'adresse IP.
- **Port** : Saisissez le numéro du port.

- **ID utilisateur** : saisissez l'ID utilisateur du serveur proxy si ce dernier requiert une authentification.
- **Mot de passe** : saisissez le mot de passe du serveur proxy si ce dernier requiert une authentification.

Configuration des paramètres proxy

Procédure

1. Accédez à **Administration** > **Paramètres proxy**.



2. Cochez la case **Utiliser un serveur proxy** pour les mises à jour.
3. Sélectionnez **HTTP** ou **SOCKS5** comme protocole du proxy.

> **Remarque**
>
> Smart Protection Server ne prend plus en charge les configurations de proxy SOCKS4.

4. Saisissez le nom du serveur ou l'adresse IP.
5. Saisissez le numéro du port.

6. Si votre serveur proxy nécessite des informations d'authentification, saisissez l'**ID utilisateur** et le **mot de passe**.
7. Cliquez sur **Enregistrer**.

Assistance

Utilisez la console Web pour télécharger des informations de diagnostic applicables au dépannage et au support.

Cliquez sur **Démarrer** pour commencer la collecte des informations de diagnostic.

Téléchargement des informations système pour l'assistance

Procédure

1. Accédez à **Administration** > **Assistance**.
2. Cliquez sur **Démarrer**.

   L'écran de progression du téléchargement apparaît.
3. Cliquez sur **Enregistrer** lorsque l'invite concernant le fichier téléchargé apparaît.
4. Spécifiez l'emplacement et le nom du fichier.
5. Cliquez sur **Enregistrer**.

Modification du mot de passe de la console produit

Le mot de passe de la console produit est le principal moyen pour protéger le serveur Smart Protection Server des modifications non autorisées. Pour bénéficier d'un environnement plus sûr, changez régulièrement le mot de passe de la console et utilisez un mot de passe difficile à deviner. Vous pouvez changer le mot de passe du compte

administrateur par l'intermédiaire de l'interface de ligne de commande (CLI) : Utilisez la commande « configure password » dans l'interface de ligne de commande pour apporter des modifications.

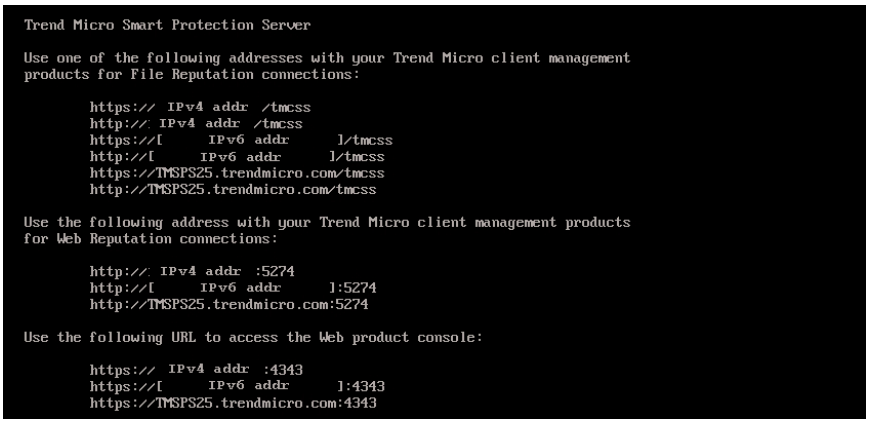
Conseil

Pour créer un mot de passe sécurisé, tenez compte de ce qui suit :

- Incluez à la fois des lettres et des chiffres.
- Évitez les mots du dictionnaire (quelle que soit la langue).
- Orthographiez intentionnellement les mots de façon incorrecte.
- Utilisez des expressions ou combinez des mots.
- Utilisez une combinaison de majuscules et de minuscules.
- Utilisez des symboles.

Procédure

1. Connectez-vous à la console CLI à l'aide du compte administrateur.



2. Saisissez ce qui suit pour activer les commandes d'administration:

```
enable
```

3. Saisissez la commande suivante :

   ```
   configure password admin
   ```

4. Saisissez le nouveau mot de passe.

5. Saisissez une seconde fois le nouveau mot de passe pour le confirmer.

Importation de certificats

Cette version de Smart Protection Server permet aux administrateurs de régénérer ou d'importer le certificat de serveur pour plus de sécurité.

Procédure

1. Accédez à **Administration** > **Certificat**.

   Les « informations du certificat de serveur » actuel s'affichent.

2. Cliquez sur **Remplacer le certificat actuel**.

3. Cliquez sur **Parcourir...** afin de sélectionner un certificat valide à télécharger. Le certificat doit être un fichier .pem.

4. Cliquez sur **Suivant**.

5. Vérifiez les détails du nouveau certificat, puis cliquez sur **Terminer**. Patientez quelques secondes pendant l'importation du certificat.

Intégration aux produits et services Trend Micro

Smart Protection Server s'intègre aux produits et services Trend Micro listés dans les tableaux suivantes.Référez-vous aux sections correspondantes de l'aide en ligne des produits intégrés pour plus de détails sur l'intégration.

TABLEAU 2-2. Services de File Reputation

COMPOSANTS UTILISÉS	SOURCE DES COMPOSANTS	INTÉGRATION DES PRODUITS ET VERSIONS MINIMUM PRISES EN CHARGES	PREMIÈRE VERSION DE SMART PROTECTION SERVER
Fichier de signatures Smart Scan **Remarque** Smart Scan Pattern fonctionne en combinaison avec le Smart Scan Agent Pattern installé sur le produit intégré.	• Serveur ActiveUpdate de Trend Micro (par défaut) • HTTP ou HTTPS pris en charge comme autre source de mise à jour	• OfficeScan 10 • Core Protection Module 10.5 • Deep Security 7.5 • InterScan Messaging Security Virtual Appliance 9.1 • InterScan Web Security Virtual Appliance 6.5 SP1 • ScanMail for Microsoft Exchange 10 SP1 • PortalProtect 2.1 pour SharePoint 2.1 • Threat Mitigator 2.5 • Worry-Free Business Security 6.0	1.0
Proxy du service Smart Protection (utilisé pour la fonction File Reputation de la communauté)	S/O (prédéfini)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1 • OfficeScan XG	3.0 Patch 2

TABLEAU 2-3. Services de réputation de sites Web

COMPOSANTS UTILISÉS	SOURCE DES COMPOSANTS	INTÉGRATION DES PRODUITS ET VERSIONS MINIMUM PRISES EN CHARGES	PREMIÈRE VERSION DE SMART PROTECTION SERVER
Signatures de blocage Web	• Trend Micro Active Update Server (par défaut) • Autre source de mise à jour prise en charge	• OfficeScan 10.5 • Core Protection Module 10.5 • Deep Discovery Inspector 2.6 • Deep Security 7.5 • ScanMail for Microsoft Exchange 10.0 SP1 • ScanMail for Lotus Domino 5.6 • PortalProtect 2.1 • Trend Micro Security (pour Mac) 2.0	2.0
URL approuvées/ bloquées	S/O (liste configurée directement depuis la console Smart Protection Server™)		2.0
URL suspectes	• Control Manager 6.0 SP2 • Deep Discovery Analyzer 5.0		2.6 Patch 1
URL suspectes améliorées	• Control Manager 6.0 SP3	• OfficeScan 11 SP1	3.0 Patch 1
Proxy du service Smart Protection (utilisé pour le service d'inspection Web)	S/O (prédéfini)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

Tableau 2-4. Services de réputation de l'application mobile

Composants utilisés	Source des composants	Intégration des produits et versions minimum prises en charges	Première version de Smart Protection Server
Proxy du service Smart Protection	S/O (prédéfini)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

Tableau 2-5. Certified Safe Software Service

Composants utilisés	Source des composants	Intégration des produits et versions minimum prises en charges	Première version de Smart Protection Server
Proxy du service Smart Protection	S/O (prédéfini)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

Tableau 2-6. Apprentissage automatique prédictif

Composants utilisés	Source des composants	Intégration des produits et versions minimum prises en charges	Première version de Smart Protection Server
Proxy du service Smart Protection	S/O (prédéfini)	• OfficeScan XG	3.1

Remarque

Le proxy du service Smart Protection redirige les demandes de requêtes depuis les produits intégrés vers Smart Protection Network à des fins d'analyse complémentaire.

Chapitre 3

Surveillance de Smart Protection Server™

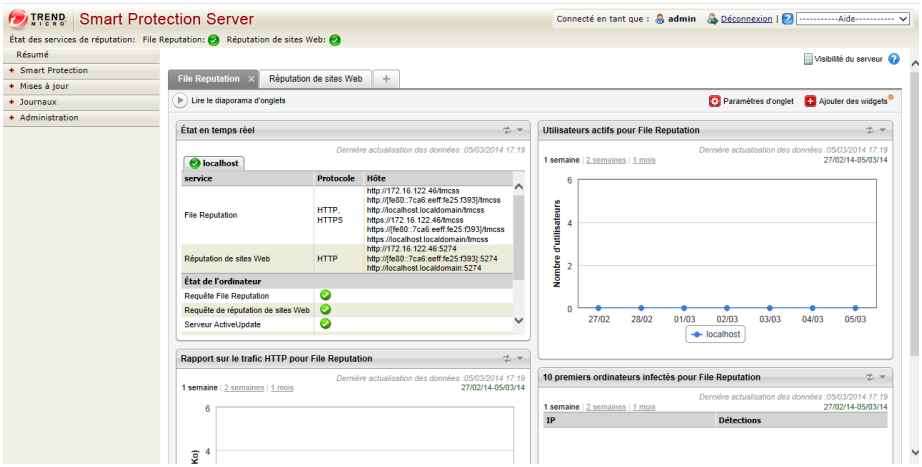
Surveillez Trend Micro™ Smart Protection Server™ à l'aide des journaux et des widgets de l'écran Résumé.

Les rubriques sont les suivantes:

Utilisation de l'écran Résumé

L'écran **Résumé** peut afficher des informations personnalisées concernant les serveurs Smart Protection Server, le trafic et les détections.

Smart Protection Server prend en charge les protocoles HTTP et HTTPS pour les connexions au service de File Reputation et le protocole HTTP pour les connexions au service de réputation de sites Web. HTTPS assure une connexion plus sûre alors que HTTP utilise moins de bande passante. Les adresses Smart Protection Server sont affichées dans la bannière de la console de l'interface de ligne de commande (CLI).



L'écran **Résumé** comprend les éléments d'interface utilisateur suivants :

- **Visibilité du serveur**: cliquez sur cette option pour ajouter des serveurs à la liste Visibilité du serveur ou configurer les paramètres du serveur proxy pour la connexion aux serveurs dans la liste Visibilité du serveur. La modification des informations du serveur est identique pour tous les widgets.

Remarque

Les adresses Smart Protection Server sont utilisées avec les produits Trend Micro qui gèrent des endpoints. Les adresses de serveur sont utilisées pour configurer les connexions des endpoints aux serveurs Smart Protection Server.

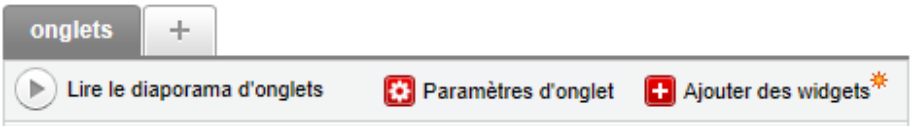
- Les onglets fournissent un endroit pour accueillir les widgets. Pour obtenir des informations détaillées, voir *Onglets à la page 3-3*.
- Les widgets constituent les composants centraux du tableau de bord. Pour obtenir des informations détaillées, voir *Widgets à la page 3-5*.

Onglets

Les onglets fournissent un endroit pour accueillir les widgets. Chaque onglet de l'écran **Résumé** peut contenir jusqu'à 20 widgets. L'écran **Résumé** peut accueillir jusqu'à 30 onglets.

Tâches via les onglets

Le tableau suivant répertorie toutes les tâches liées aux onglets :



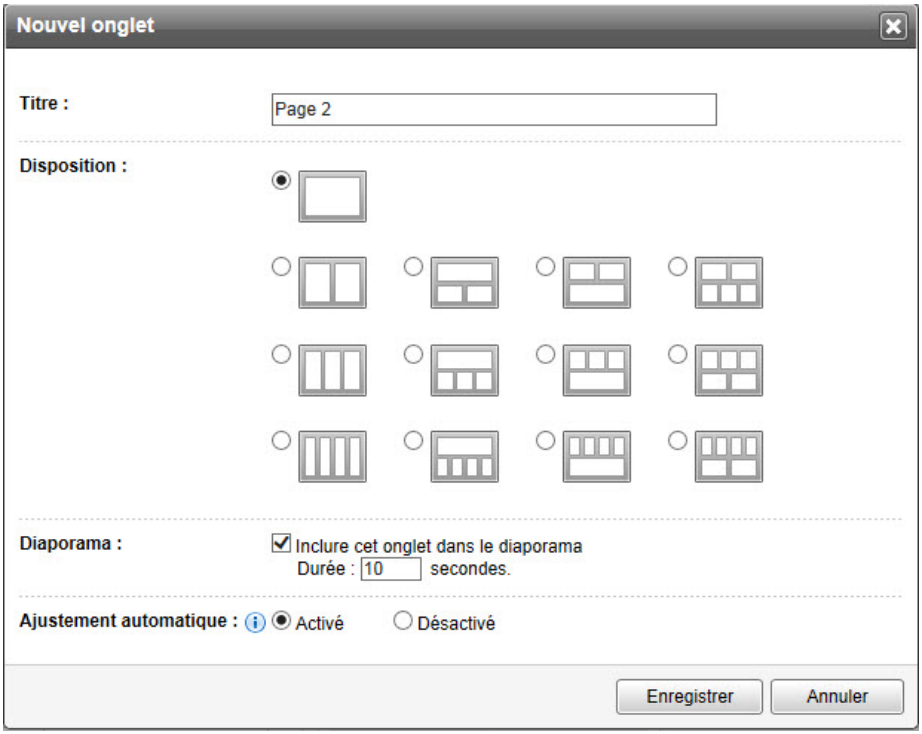
Tâche	Étapes
Ajouter un onglet	Cliquez sur l'icône plus (+) en haut de l'écran **Résumé**. La fenêtre **Nouvel onglet** s'affiche. Pour plus d'informations sur cette fenêtre, voir *Fenêtre nouvel Onglet à la page 3-4*.
Modifier les paramètres des onglets	Cliquez sur **Paramètres des onglets**. Une fenêtre semblable à la fenêtre **Nouvel onglet** s'affiche pour vous permettre de modifier les paramètres.
Lire le diaporama d'onglets	Cliquez sur **Lire le diaporama d'onglets**. Les informations contenues dans les onglets sélectionnés changeront comme dans un diaporama.
Déplacer un onglet	Utilisez le glisser-déplacer pour déplacer un onglet.

TÂCHE	ÉTAPES
Supprimer un onglet	Cliquez sur l'icône Supprimer ( ) en regard du titre de l'onglet. La suppression d'un onglet supprime également tous les widgets de l'onglet.

Fenêtre nouvel Onglet

La fenêtre **Nouvel onglet** s'ouvre lorsque vous ajoutez un nouvel onglet dans l'écran **Résumé**.

Cette fenêtre comprend les options suivantes :



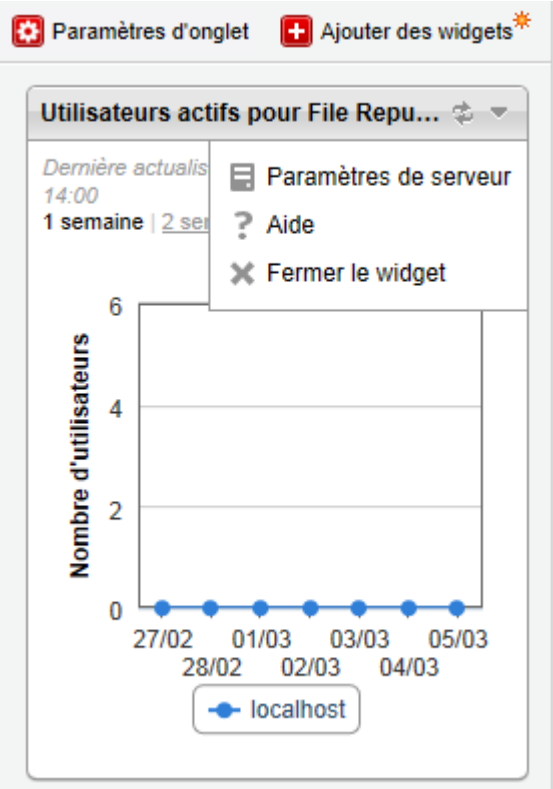
OPTION	ÉTAPES
Titre	Saisissez le nom de l'onglet.
Disposition	Choisissez parmi les dispositions disponibles.
Diaporama	Les informations contenues dans les onglets sélectionnés changeront comme dans un diaporama. Si vous activez cette option, vous pouvez sélectionner les onglets devant s'afficher dans votre diaporama et vous pouvez également contrôler la vitesse de lecture du diaporama.
Ajustement automatique	L'ajustement automatique ajuste un widget afin qu'il rentre dans la zone.

Widgets

Les widgets vous permettent de personnaliser les informations affichées dans l'écran **Résumé**. Il est possible d'ajouter de nouveaux widgets à la console Web. Il est possible de faire glisser des widgets pour personnaliser l'ordre dans lequel ils s'affichent. Les packs de widgets disponibles peuvent être téléchargés et mis à jour en utilisant l'écran Mise à jour du programme. Après avoir mis à jour le pack de widgets, il est possible d'ajouter le nouveau widget à partir de l'écran **Résumé**.

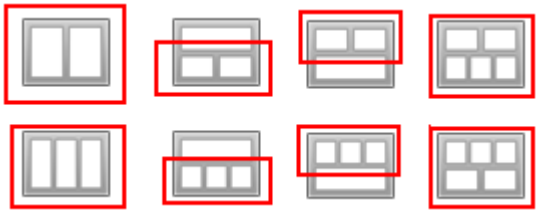
Tâches des widgets

Le tableau suivant répertorie les tâches liées aux widgets :



TÂCHE	ÉTAPES
Ajouter un widget	Ouvrez un onglet et cliquez sur **Ajouter des widgets** dans l'angle supérieur droit de l'onglet. L'écran **Ajouter des widgets** apparaît.
Rafraîchir les données du widget	Cliquez sur l'icône Actualiser ( ).

TÂCHE	ÉTAPES
Configurer les paramètres du serveur	Cliquez sur l'icône en triangle ( ), puis sur **Paramètres du serveur** ( ) pour permettre/interdire au widget d'obtenir des informations du serveur. Vous pouvez aussi cliquer sur **Vérifier la visibilité du serveur** pour ajouter des serveurs de la liste Visibilité du serveur ou configurer des paramètres de serveur proxy afin d'établir la connexion avec les serveurs de la liste Visibilité du serveur.
Afficher l'aide	Cliquez sur l'icône en triangle ( ), puis sur **Aide** ( ).
Supprimer un widget	Cliquez sur l'icône en triangle ( ), puis sur **Fermer le widget** ( ). Cette action supprime le widget de l'onglet le contenant, mais pas des autres onglets ni de la liste des widgets dans l'écran **Ajouter des widgets**.
Déplacer un widget	Utilisez le glisser-déplacer pour déplacer un widget dans une zone différente à l'intérieur de l'onglet.

TÂCHE	ÉTAPES
Redimensionner un widget	Pour redimensionner un widget, pointez le curseur sur son côté droit. Lorsqu'une ligne verticale épaisse et une flèche apparaissent (comme indiqué dans l'image suivante), déplacez le curseur vers la gauche ou vers la droite.  Il est possible de redimensionner les widgets se trouvant dans les onglets à plusieurs colonnes uniquement. Ces onglets ont l'une des dispositions suivantes ; les sections en surbrillance indiquent l'emplacement des widgets redimensionnables. 

Widgets disponibles

Les widgets suivants sont disponibles dans cette version.

État en temps réel

Ce widget permet de surveiller en temps réel l'état du serveur Smart Protection Server.

Remarque

Lorsque ce widget s'affiche sur l'écran Résumé, la session de la console du produit n'expire pas. L'état de l'ordinateur est mis à jour toutes les minutes ; de ce fait, la session n'expire pas en raison des requêtes envoyées au serveur. Cependant, la session arrivera à expiration si l'onglet actuellement affiché ne contient pas ce widget.

TABLEAU 3-1. Données du widget

DONNÉES	DESCRIPTION
Service	Services proposés par Smart Protection Server.
Protocole	Cette option permet d'afficher les protocoles pris en charge par les services. File Reputation prend en charge les protocoles HTTP et HTTPS. La réputation de sites Web prend en charge le protocole HTTP. HTTPS assure une connexion plus sûre alors que HTTP utilise moins de bande passante.
Hôte	Adresses des services de réputation de sites Web et File Reputation Ces adresses sont utilisées avec les produits Trend Micro qui prennent en charge les serveurs Smart Protection Server. Elles permettent de configurer les connexions aux serveurs Smart Protection Server.

DONNÉES	DESCRIPTION
État de l'ordinateur	Les éléments suivants s'affichent sous État de fonctionnement : • **Requête File Reputation** : indique si File Reputation fonctionne comme prévu. • **Requête de réputation de sites Web** : indique si la réputation de sites Web fonctionne comme prévu. • **ActiveUpdate** : indique si ActiveUpdate fonctionne comme prévu. • **Charge moyenne de l'UC** : indique la charge moyenne de l'ordinateur générée par le noyau pour les 1, 5 et 15 minutes passées. • **Mémoire disponible** : indique la quantité de mémoire physique disponible sur l'ordinateur. • **Utilisation du changement de disque** : indique l'utilisation du changement de disque. • **Espace disponible** : indique l'espace disque disponible sur l'ordinateur.

Utilisateurs actifs pour File Reputation

Le widget Utilisateurs actifs affiche le nombre d'utilisateurs ayant envoyé des requêtes de réputation de fichiers au serveur Smart Protection Server. Chaque ordinateur client unique est considéré comme un utilisateur actif.

Remarque

Ce widget affiche les informations dans un graphique 2D et il est mis à jour toutes les heures. Vous pouvez aussi cliquer sur l'icône Actualiser ( ) à tout moment pour mettre à jour les données.

TABLEAU 3-2. Données du widget

DONNÉES	DESCRIPTION
Utilisateurs	Nombre d'utilisateurs envoyant des requêtes aux serveurs Smart Protection Server.
Date	Date de la requête.

Rapport sur le trafic HTTP pour File Reputation

Le widget Rapport sur le trafic HTTP affiche le trafic réseau total en kilo-octets (Ko) envoyé vers le serveur Smart Protection Server à partir des requêtes de réputation de fichiers générées par les clients. Les informations de ce widget sont mises à jour toutes les heures et les données sont affichées sous forme de graphique en 3D. Vous pouvez aussi cliquer sur l'icône Actualiser () à tout moment pour mettre à jour les données.

Remarque

Vous pouvez cliquer avec le bouton droit de la souris sur le graphique afin d'afficher les options permettant de réinitialiser le graphique, de l'afficher en 2D, 3D, 100% et de l'ajuster. Il vous est également possible de cliquer sur le nom du serveur pour afficher les valeurs correspondant à chaque jour sur le graphique.

TABLEAU 3-3. Données du widget

DONNÉES	DESCRIPTION
Trafic (Ko)	Trafic réseau généré par les requêtes.
Date	Date des requêtes.

10 premiers ordinateurs bloqués pour File Reputation

Ce widget dresse la liste des adresses IP des 10 ordinateurs répertoriés comme étant les plus infectés après que Smart Protection Server ait reçu un virus connu à partir d'une requête de réputation de fichiers. Les informations de ce widget s'affichent dans un tableau, qui inclut l'adresse IP de l'ordinateur et le nombre total de détections de chacun d'eux. Les informations de ce widget sont mises à jour toutes les heures. Vous pouvez aussi cliquer sur l'icône Actualiser () à tout moment pour mettre à jour les données.

Ce widget permet de suivre les ordinateurs les plus infectés de votre réseau.

Remarque

Si vous activez plusieurs serveurs Smart Protection Server dans ce widget, ce dernier calculera le nombre total de détections sur le serveur sélectionné et affichera la liste des 10 ordinateurs les plus infectés selon les serveurs Smart Protection Server sélectionnés dans la liste.

TABLEAU 3-4. Données du widget

DONNÉES	DESCRIPTION
IP	Adresse IP de l'ordinateur.
Détections	Nombre de menaces de sécurité détectées par cet ordinateur.

Utilisateurs actifs pour la réputation de sites Web

Le widget Utilisateurs actifs indique le nombre d'utilisateurs ayant envoyé des requêtes de réputation de sites Web au serveur Smart Protection Server. Chaque ordinateur client unique est considéré comme un utilisateur actif.

Remarque

Ce widget affiche les informations dans un graphique 2D et il est mis à jour toutes les 5 minutes. Vous pouvez aussi cliquer sur l'icône Actualiser ( ) à tout moment pour mettre à jour les données.

TABLEAU 3-5. Données du widget

DONNÉES	DESCRIPTION
Utilisateurs	Nombre d'utilisateurs envoyant des requêtes aux serveurs Smart Protection Server.
Date	Date de la requête.

Rapport sur le trafic HTTP pour la réputation de sites Web

Le widget Rapport sur le trafic HTTP affiche le trafic réseau total en kilo-octets (Ko) envoyé vers le serveur Smart Protection Server à partir des requêtes de réputation de sites Web générées par les clients. Les informations de ce widget sont mises à jour toutes les heures et les données sont affichées sous forme de graphique en 3D. Vous pouvez aussi cliquer sur l'icône Actualiser ( ) à tout moment pour mettre à jour les données.

Remarque

Vous pouvez cliquer avec le bouton droit de la souris sur le graphique afin d'afficher les options permettant de réinitialiser le graphique, de l'afficher en 2D, 3D, 100% et de l'ajuster. Il vous est également possible de cliquer sur le nom du serveur pour afficher les valeurs correspondant à chaque jour sur le graphique.

TABLEAU 3-6. Données du widget

DONNÉES	DESCRIPTION
Trafic (Ko)	Trafic réseau généré par les requêtes.
Date	Date des requêtes.

10 premiers ordinateurs bloqués pour la réputation de sites Web

Ce widget dresse la liste des adresses IP des 10 ordinateurs répertoriés comme étant les plus bloqués après que Smart Protection Server a reçu une URL pour une requête de réputation de sites Web. Les informations de ce widget s'affichent dans un tableau, qui inclut l'adresse IP de l'ordinateur et le nombre total d'URL bloquées sur chacun d'eux. Les informations de ce widget sont mises à jour tous les jours. Vous pouvez aussi cliquer sur l'icône Actualiser ( ) à tout moment pour mettre à jour les données.

Ce widget permet de suivre les ordinateurs qui accèdent aux sites les plus bloqués de votre réseau.

Remarque

Si vous activez plusieurs serveurs Smart Protection Server dans ce widget, ce dernier calculera le nombre total de détections sur le serveur Smart Protection Server sélectionné et affichera la liste des 10 ordinateurs les plus bloqués selon les serveurs Smart Protection Server sélectionnés dans la liste.

TABLEAU 3-7. Données du widget

DONNÉES	DESCRIPTION
IP	Adresse IP de l'ordinateur.
Détections	Nombre d'URL bloquées sur cet ordinateur

Journaux

Utilisez les journaux pour surveiller l'état du serveur Smart Protection Server. Pour afficher les informations des journaux, effectuez une requête.

URL bloquées

L'écran **URL bloquées** affiche des informations relatives aux requêtes de réputation de sites Web ayant rapporté des résultats malveillants.

Les options disponibles sur cet écran sont indiquées ci-dessous.

- **Mot-clé** : spécifiez les mots-clés à utiliser lors de la recherche d'URL.
- **Période** : Sélectionnez une plage de dates.
- **Source** : Sélectionnez une ou plusieurs sources pour afficher les journaux correspondants.
  - **URL bloquées définies par l'utilisateur** : Affiche les URL bloquées qui correspondent aux URL bloquées définies par l'utilisateur dans Smart Protection Server.
  - **Signatures de blocage Web** : Affiche les URL bloquées correspondant aux entrées indiquées dans les signatures de blocage Web.

- **URL C&C associées à :** Affiche les URL bloquées correspondant aux entrées indiquées dans les sources suivantes :
  - **Objets suspects définis par l'utilisateur dans Control Manager** : Sous-ensemble des objets suspects définis par l'utilisateur dans Control Manager
  - **Virtual Analyzer** : Sous-ensemble des objets suspects des produits activés pour Virtual Analyzer, tels que Deep Discovery Advisor, Deep Discovery Analyzer et Control Manager
  - **Global Intelligence dans les signatures de blocage Web** : Trend Micro Smart Protection Network compile la liste Global Intelligence à partir de sources dans le monde entier, puis teste et évalue le niveau de risque de chaque adresse de rappel C&C. Les services de réputation de sites Web utilisent la liste Global Intelligence avec les scores de réputation pour les sites Web malveillants afin d'offrir une meilleure sécurité contre les menaces avancées. Le niveau de sécurité de la réputation de sites Web détermine les mesures prises par rapport aux sites Web malveillants ou aux serveurs C&C en fonction des niveaux de risque affectés.

Les détails affichés sur cet écran sont présentés ci-dessous :

- **Date et heure** : date et heure de l'événement de blocage de l'URL.
- **URL** : URL bloquée.
- **Afficher le journal** : Affiche les informations de la source concernant l'URL bloquée.
- **GUID du client** : GUID de l'ordinateur ayant tenté d'accéder à l'URL bloquée.
- **GUID du serveur** : GUID du produit Trend Micro qui prend en charge les serveurs Smart Protection Server.
- **IP du client** : adresse IP de l'ordinateur ayant tenté d'accéder à l'URL bloquée.
- **Ordinateur** : nom de l'ordinateur ayant tenté d'accéder à l'URL bloquée.
- **Entité de produit** : Produit Trend Micro ayant détecté l'URL.

Journal de mise à jour

L'écran Journal de mise à jour affiche des informations sur les mises à jour des fichiers programme ou de signatures. Voici les options disponibles sur cet écran.

- **Période** : Sélectionnez la période à laquelle la mise à jour a eu lieu.
- **Type** : Sélectionnez le type de mise à jour à afficher.

Détails du journal :

- **Date et heure** : Date et heure de mise à jour du serveur.
- **Nom du composant** : Composant qui a été mis à jour.
- **Résultat** : Il peut s'agit d'une réussite ou d'un échec.
- **Description** (Description) : Décrit l'événement de mise à jour.
- **Méthode de mise à jour** : Il s'agit du scan traditionnel ou de Smart Scan.

Journal de service de réputation

L'écran Journal de service de réputation affiche des informations relatives aux requêtes de réputation de sites Web et de File Reputation. Voici les options disponibles sur cet écran.

- **Service** : Indiquez le service.
- **Résultat** : Indiquez le type de résultat.
- **Période** : Sélectionnez une plage de dates.

Détails du journal :

- **Date et heure** : Date et heure auxquelles l'état du service de réputation de sites Web ou de File Reputation a été vérifié.
- **Service** : Il peut s'agir du service de réputation de sites Web ou de File Reputation.
- **Résultat** : Il peut s'agit d'une réussite ou d'un échec.

- **Description** (Description) : Décrit l'état du service de réputation de sites Web ou de File Reputation.

Maintenance des journaux

Effectuez la maintenance des journaux pour supprimer ceux qui sont devenus inutiles. Voici les options disponibles sur cet écran.

- **Journal de mise à jour des signatures** : sélectionnez cette option pour purger les entrées du journal de mise à jour du fichier de signatures.
- **Journal de mise à jour du programme** : sélectionnez cette option pour purger les entrées du journal de mise à jour.
- **URL bloquées** : sélectionnez cette option pour purger les entrées requêtes d'URL.
- **Journal de service de réputation** : sélectionnez cette option pour purger les entrées d'événements de service de réputation.
- **Supprimer tous les journaux** : sélectionnez cette option pour supprimer tous les journaux.
- **Purger les journaux antérieurs au nombre de jours suivant** : sélectionnez cette option pour purger les anciens journaux.
- **Activer la purge programmée** : sélectionnez cette option pour programmer la purge automatique.

Procédure

1. Accédez à **Journaux** > **Maintenance des journaux**.
2. Sélectionnez les types de journaux à purger.
3. Choisissez de supprimer tous les journaux ou les journaux qui sont plus vieux que le nombre de jours spécifié.
4. Sélectionnez un programme de purge ou cliquez sur **Purger maintenant**.
5. Cliquez sur **Enregistrer**.

Notifications

Vous pouvez configurer Smart Protection Server pour envoyer des messages électroniques ou des notifications par déroutement SNMP (Simple Network Management Protocol) à certaines personnes en cas de changement d'état des services ou des mises à jour.

Notifications par e-mail

Configurez les paramètres de notification par e-mail pour envoyer un e-mail aux administrateurs en cas de changement d'état dans les services ou les mises à jour. Voici les options disponibles sur cet écran.

- **Serveur SMTP** : saisissez l'adresse IP du serveur SMTP.
- **Numéro de port** : saisissez le numéro de port du serveur SMTP.
- **De** : saisissez une adresse électronique dans le champ de l'expéditeur des notifications par e-mail.
- **Services** : choisissez d'envoyer des notifications pour le changement d'état de la réputation de fichiers, de sites Web, et la mise à jour des signatures.
- **À** : saisissez une ou plusieurs adresses électroniques pour envoyer des notifications pour cet événement.
- **Objet** : saisissez un nouvel objet ou utilisez le texte de l'objet par défaut pour cet événement.
- **Message** : saisissez un nouveau message ou utilisez le texte du message par défaut pour cet événement.
- **Changement d'état de File Reputation** : choisissez d'envoyer une notification pour les changements d'état et spécifiez le destinataire de cette notification.
- **Changement d'état de la réputation de sites Web** : choisissez d'envoyer une notification pour les changements d'état et spécifiez le destinataire de cette notification.

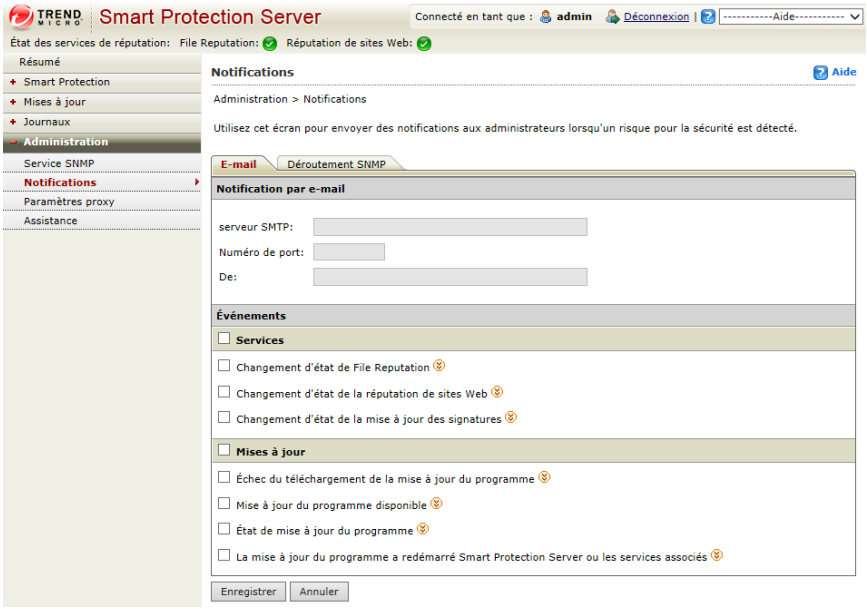
- **Changement d'état de la mise à jour des signatures** : choisissez d'envoyer une notification pour les changements d'état et spécifiez le destinataire de cette notification.
- **Mises à jour** : choisissez d'envoyer des notifications pour toutes les notifications associées au programme.
- **Échec du téléchargement de la mise à jour du programme** : sélectionnez cette option pour envoyer une notification si la mise à jour du programme n'a pas été téléchargée correctement et spécifiez le destinataire de cette notification.
- **Mise à jour du programme disponible** : sélectionnez cette option pour envoyer une notification si une mise à jour d'un programme nécessite une confirmation et spécifiez le destinataire de cette notification.
- **État de mise à jour du programme** : sélectionnez cette option pour envoyer une notification concernant la mise à jour d'un programme et spécifiez le destinataire de cette notification.
- **La mise à jour du programme a redémarré Smart Protection Server ou les services associés** : sélectionnez cette option pour envoyer une notification lorsque le processus de mise à jour du programme redémarre le serveur Smart Protection Server ou les services associés et spécifiez le destinataire de cette notification.
- **Message par défaut** : cliquez sur cette option pour rétablir le texte par défaut Trend Micro des champs Objet et Message.

Configuration des notifications par e-mail

Procédure

1. Accédez à **Administration** > **Notifications**, puis à l'onglet **Courrier électronique**.

L'onglet des notifications par e-mail apparaît.



2. Cochez la case **Services** pour recevoir une notification par courrier électronique concernant les changements d'état de tous les services ou sélectionnez des services spécifiques dans les options affichées :

   - **Changement d'état de File Reputation** : sélectionnez cette option pour envoyer une notification pour les changements d'état et spécifiez le destinataire, l'objet et le message.
   - **Changement d'état de la réputation de sites Web** : sélectionnez cette option pour envoyer une notification pour les changements d'état et spécifiez le destinataire, l'objet et le message.
   - **Changement d'état de la mise à jour des signatures** : sélectionnez cette option pour envoyer une notification pour les changements d'état et spécifiez le destinataire, l'objet et le message.

3. Cochez la case **Mises à jour** ou sélectionnez l'une des options suivantes :

- **Échec du téléchargement de la mise à jour du programme** : sélectionnez cette option pour envoyer une notification pour cet événement et spécifiez le destinataire, l'objet et le message.
- **Mise à jour du programme disponible** : sélectionnez cette option pour envoyer une notification pour cet événement et spécifiez le destinataire, l'objet et le message.
- **État de mise à jour du programme** : sélectionnez cette option pour envoyer une notification pour cet événement et spécifiez le destinataire, l'objet et le message.
- **La mise à jour du programme a redémarré Smart Protection Server ou les services associés** : sélectionnez cette option pour envoyer une notification pour cet événement et spécifiez le destinataire, l'objet et le message.

4. Saisissez l'adresse IP du serveur SMTP dans le champ **Serveur SMTP**.
5. Saisissez le numéro du port SMTP.
6. Saisissez une adresse électronique dans le champ **De**. Toutes les notifications par e-mail affichent cette adresse dans le champ De des messages électroniques.
7. Cliquez sur **Enregistrer**.

Notifications de déroutement SNMP

Configurez les paramètres de notification SNMP (Simple Network Management Protocol) pour informer les administrateurs, via le déroutement SNMP, en cas de changement d'état dans les services. Voici les options disponibles sur cet écran.

- **Adresse IP du serveur** : Spécifiez l'adresse IP du destinataire du déroutement SNMP.
- **Nom de communauté** : spécifiez le nom de communauté SNMP.
- **Services** : sélectionnez cette option pour envoyer une notification SNMP pour le changement d'état de File Reputation, de la réputation de sites Web et les mises à jour des signatures.

- **Message** : saisissez un nouveau message ou utilisez le texte du message par défaut pour cet événement.
- **Changement d'état de File Reputation** : choisissez d'envoyer une notification pour les changements d'état.
- **Changement d'état de la réputation de sites Web** : choisissez d'envoyer une notification pour les changements d'état.
- **Changement d'état de la mise à jour des signatures** : choisissez d'envoyer une notification pour les changements d'état.
- **Message par défaut** : Cliquez sur cette option pour rétablir le texte par défaut Trend Micro des champs Message.

Configuration des notifications de déroutement SNMP

Configurez les paramètres de notification SNMP (Simple Network Management Protocol) pour informer les administrateurs, via le déroutement SNMP, en cas de changement d'état dans les services.

Procédure

1. Accédez à **Administration** > **Notifications**, puis à l'onglet **SNMP**.

L'onglet des notifications de déroutement SNMP apparaît.

2. Cochez la case **Services** ou sélectionnez l'une des cases suivantes :

   - **Changement d'état de File Reputation** : sélectionnez cette option pour envoyer une notification pour les changements d'état et spécifiez le destinataire, l'objet et le message.
   - **Changement d'état de la réputation de sites Web** : sélectionnez cette option pour envoyer une notification pour les changements d'état et spécifiez le destinataire, l'objet et le message.
   - **Changement d'état de la mise à jour des signatures** : sélectionnez cette option pour envoyer une notification pour les changements d'état et spécifiez le destinataire, l'objet et le message.

3. Saisissez l'adresse IP du serveur de déroutement SNMP.

4. Saisissez le nom de communauté SNMP.

5. Cliquez sur **Enregistrer**.

Chapitre 4

Intégration à Trend Micro Control Manager

Smart Protection Server s'intègre à Control Manager.

Les rubriques sont les suivantes :

Trend Micro Control Manager

Trend Micro Control Manager™ est une console d'administration centrale qui gère les produits et services Trend Micro aux niveaux de la passerelle, du serveur de messagerie et du parc informatique de l'entreprise. La console d'administration à interface Web Control Manager fournit un point de surveillance unique pour les produits et services gérés au sein du réseau.

Control Manager permet aux administrateurs système de surveiller et de reporter des activités telles que des infections, des violations de sécurité ou des points d'entrée de virus. Les administrateurs système peuvent télécharger et déployer des composants au sein du réseau, afin de s'assurer que cette protection est cohérente et à jour. Control Manager autorise à la fois les mises à jour manuelles et pré-programmées, ainsi que la configuration et l'administration de produits par groupes ou de manière individuelle pour plus de flexibilité.

Versions prises en charge de Control Manager

Cette version de Smart Protection Server prend en charge les versions suivantes de Control Manager.

Fonctionnalités	Version de Control Manager	
	6.0 SP3	6.0 SP2 ou versions antérieures
Synchronisation d'actions et d'objets suspects	Oui	Non
Utilisation de Control Manager comme source de mise à jour alternative	Oui	Oui

Remarque

Smart Protection Server se connecte uniquement à des réseaux Control Manager IPv4 pure ou double pile.

Intégration de Control Manager avec cette version de Smart Protection Server

Cette version de Smart Protection Server inclut les fonctionnalités suivantes :

TABLEAU 4-1. Intégration à Control Manager

FONCTION	DESCRIPTION
Synchronisation d'actions et d'objets suspects	1. Control Manager consolide les objets suspects et les actions de scan, puis relaie cette information à Smart Protection Server. 2. Smart Protection Server relaie les URL suspectes et les actions aux agents Office Scan. Pour les produits envoyant des requêtes de réputation de sites Web (tels que Portal Protect et Deep Security), Smart Protection Server relaie uniquement les URL suspectes. **Remarque** Pour plus d'informations sur la façon dont Control Manager gère les objets suspects, consultez http://docs.trendmicro.com/all/ent/tmcm/v6.0-sp3/fr-fr/tmcm_6.0_sp3_ctd_primer/ctd_primer.pdf
Control Manager comme source de mise à jour alternative	Control Manager peut se comporter comme une source de mise à jour si Smart Protection Server n'a pas de connexion à Internet.

Chapitre 5

Obtenir de l'aide

Ce chapitre fournit des détails sur la façon d'obtenir une aide supplémentaire durant l'utilisation de Trend Micro™ Smart Protection Server™ .

Les rubriques sont les suivantes:

Utilisation du portail d'assistance

Le portail d'assistance Trend Micro est une ressource accessible 24 heures sur 24 et 7 jours sur 7 qui contient les informations les plus récentes à la fois sur les problèmes courants et inhabituels.

Procédure

1. Accédez à http://esupport.trendmicro.com.
2. Sélectionnez un produit ou un service dans la liste déroulante appropriée et indiquez les autres informations associées.

   La page de produits **Assistance technique** s'affiche.
3. Utilisez la zone **Rechercher dans l'assistance** pour rechercher les options disponibles.
4. Si vous ne trouvez aucune solution, cliquez sur **Envoyer une requête d'assistance** dans le volet de navigation de gauche et ajoutez les détails appropriés, ou bien soumettez une requête d'assistance ici :

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   Un ingénieur de l'assistance Trend Micro étudie la requête et répond sous 24 heures au maximum.

Problèmes connus

Les problèmes connus documentent les comportements inattendus du produit qui peuvent requérir temporairement une solution palliative. Trend Micro recommande de toujours consulter les documents Lisez-moi pour obtenir des informations sur la configuration requise et les problèmes connus qui pourraient affecter l'installation ou les performances. Les documents Lisez-moi contiennent également une description des nouveautés d'une version particulière, ainsi que d'autres informations utiles.

Les problèmes connus les plus récents et les solutions possibles peuvent également être consultés dans la base de connaissances Trend Micro :

http://esupport.trendmicro.com

Correctifs de type hotfix, patchs et Service Packs

Après la publication officielle d'un produit, Trend Micro développe souvent des correctifs de type hotfix, des patchs et des service packs afin de corriger les problèmes, d'améliorer les performances des produits et d'ajouter de nouvelles fonctionnalités.

Le paragraphe suivant résume les éléments que Trend Micro peut publier :

- **Correctif de type hotfix** : alternative ou solution apportée à des problèmes signalés par les utilisateurs. Trend Micro ne développe et publie des correctifs de type hotfix que pour des clients spécifiques.
- **Patch de sécurité** : correctif de type hotfix unique ou groupe de correctifs de type hotfix pouvant être déployés au niveau de tous les clients
- **Patch** : groupe de patchs de sécurité pouvant être déployés au niveau de tous les clients
- **Service Packs** : amélioration significative des fonctions permettant une mise à niveau du produit

Votre revendeur ou votre service d'assistance technique peut vous contacter lorsque ces éléments sont disponibles. Consultez le site Web de Trend Micro pour obtenir des informations sur les nouveaux correctifs de type hotfix, patchs et service packs :

http://downloadcenter.trendmicro.com/?regs=FR

Toutes les versions incluent un fichier Lisez-moi contenant des informations relatives à l'installation, au déploiement et à la configuration. Veuillez lire attentivement le fichier Lisez-moi avant d'exécuter l'installation.

Encyclopédie des menaces

La plupart des programmes malveillants actuels sont des « menaces mixtes » (deux technologies ou plus combinées pour contourner les protocoles de sécurité des ordinateurs). Trend Micro lutte contre ces programmes malveillants complexes avec des

produits qui créent une stratégie de défense personnalisée. L'Encyclopédie des menaces fournit une liste exhaustive de noms et de symptômes pour différentes menaces mixtes, y compris des programmes malveillants connus, des spams, des URL malveillantes et des vulnérabilités connues.

Accédez au site http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp pour en savoir plus sur les éléments suivannts :

- Programmes et code mobile malveillants actuellement actifs ou « en circulation »
- Pages d'informations de menaces liées afin de créer pour un historique complet des attaques Web
- Informations sur les menaces Internet concernant des attaques et des menaces de sécurité ciblées
- Informations sur les attaques Web et les tendances en ligne
- Rapports hebdomadaires sur les programmes malveillants

Comment contacter Trend Micro

Les techniciens de Trend Micro peuvent être contactés par téléphone, télécopie ou courrier électronique :

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

- Sites d'assistance à travers le monde :

  http://www.trendmicro.fr/apropos/contact/index.html

- Documentation des produits Trend Micro :

http://docs.trendmicro.com/fr-fr/home.aspx

Optimisation de la demande d'assistance

Pour améliorer la résolution des problèmes, préparez les informations suivantes :

- Étapes permettant de reproduire le problème
- Informations sur l'appareil ou le réseau
- Marque et modèle de l'ordinateur, ainsi que tout matériel complémentaire connecté au point final
- Quantité de mémoire et espace libre sur le disque dur
- Version du système d'exploitation et du Service Pack
- Version du client du point final
- Numéro de série et code d'activation
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché
- Plate-forme de virtualisation (VMware™ ou Hyper-V™) et version

TrendLabs

TrendLabs℠ est un réseau mondial de centres de recherche, de développement et d'action conçu pour la surveillance des menaces, la prévention des attaques et la fourniture en toute transparence et en temps voulu de solutions 24 heures sur 24 et 7 jours sur 7. Épine dorsale de l'infrastructure de services de Trend Micro, TrendLabs regroupe plusieurs centaines d'ingénieurs et de membres certifiés du personnel d'assistance qui proposent un large éventail de services d'assistance technique et d'assistance produit.

TrendLabs surveille les menaces dans le monde entier pour fournir des mesures de sécurité efficaces conçues pour détecter, éviter et éliminer les attaques. La portée de ces

efforts se mesure au jour le jour, alors que les mises à jour des fichiers de signatures de virus et les ajustements du moteur de scan sont fréquemment partagés avec les clients.

Pour en savoir plus sur TrendLabs, consultez le site suivant :

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Annexe A

Commandes de l'interface de ligne de commande (CLI)

Cette section décrit les commandes de l'interface de ligne de commande (CLI) que vous pouvez utiliser dans le produit pour effectuer les tâches de surveillance, de débogage, de dépannage et de configuration. Connectez-vous à l'interface CLI par l'intermédiaire de la machine virtuelle avec votre compte administrateur. Les commandes CLI permettent aux administrateurs d'effectuer des tâches de configuration et d'utiliser des fonctions de débogage et de dépannage. L'interface CLI offre d'autres commandes qui permettent de surveiller les ressources et les fonctions stratégiques. Pour accéder à l'interface CLI, vous devez disposer du compte et du mot de passe d'administrateur.

COMMANDE	SYNTAXE	DESCRIPTION
certificate regen self-sign	**certificate regen self-sign** <Issued_to> <Issued_by> <Validity>	Régénération d'un certificat auto-signé. <Issued_to> : Nom commun ou NC du destinataire du certificat <Issued_by> : Nom commun ou NC de l'émetteur du certificat <Validity> : Le nombre de jours durant lequel le certificat est valide
certificate update CA	**certificate update CA**	Téléchargement du lot CA le plus récent
configure date	**configure date** <date> <heure>	Configuration de la date et enregistrement en CMOS date DATE_FIELD [DATE_FIELD] time TIME_FIELD [TIME_FIELD]
configure dns ipv4	**configure dns ipv4** <dns1> [dns2]	Configuration des paramètres DNS IPv4 dns1 IPv4_ADDR Serveur DNS principal dns2 IPv4_ADDR Serveur DNS secondaire []
configure dns ipv6	**configure dns ipv6** <dns1> [dns2]	Configuration des paramètres DNS IPv6 dns1 IPv6_ADDR Serveur DNS principal dns2 IPv6_ADDR Serveur DNS secondaire []

COMMANDE	SYNTAXE	DESCRIPTION
configure hostname	**configure hostname** <nom d'hôte>	Configuration du nom d'hôte hostname HOSTNAME Nom d'hôte ou FQDN
configure ipv4 dhcp	**configure ipv4 dhcp [vlan]**	Configuration de l'interface Ethernet par défaut pour l'utilisation de DHCP vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv4 static	**configure ipv4 static** <ip> <masque> <passerelle> [vlan]	Configuration de l'interface Ethernet par défaut pour l'utilisation de la configuration IPv4 statique vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv6 auto	**configure ipv6 auto** [vlan]	Configuration de l'interface Ethernet par défaut pour l'utilisation de la configuration automatique IPV6 du protocole de découverte des voisins. vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv6 dhcp	**configure ipv6 dhcp** [vlan]	Configuration de l'interface Ethernet par défaut pour l'utilisation de la configuration IPv6 dynamique (DHCPv6) vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]

COMMANDE	SYNTAXE	DESCRIPTION
configure ipv6 static	**configure ipv6 static** <ip v6> <masque v6> <passerelle v6> [vlan]	Configuration de l'interface Ethernet par défaut pour l'utilisation de la configuration IPv6 statique vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure locale de_DE	**configure locale de_DE**	Configuration des paramètres régionaux pour l'allemand
configure locale en_US	**configure locale en_US**	Configuration des paramètres régionaux pour l'anglais
configure locale es_ES	**configure locale es_ES**	Configuration des paramètres régionaux pour l'espagnol
configure locale fr_FR	**configure locale fr_FR**	Configuration des paramètres régionaux pour le français
configure locale it_IT	**configure locale it_IT**	Configuration des paramètres régionaux pour le français
configure locale ja_JP	**configure locale ja_JP**	Configuration des paramètres régionaux pour le japonais
configure locale ko_KR	**configure locale ko_KR**	Configuration des paramètres régionaux pour le coréen
configure locale ru_RU	**configure locale ru_RU**	Configuration des paramètres régionaux pour le russe

COMMANDE	SYNTAXE	DESCRIPTION
configure locale zh_CN	**configure locale zh_CN**	Configuration des paramètres régionaux pour le chinois (simplifié)
configure locale zh_TW	**configure locale zh_TW**	Configuration des paramètres régionaux pour le chinois (traditionnel)
configure ntp	**configure ntp <ip ou FQDN>**	Configurer le serveur NTP
configure port	**configure port <port_http_frs> <port_https_frs> <port_http_wrs>**	Modifier les ports des services de File Reputation et de réputation de sites Web.
configure password	**configure password** <utilisateur>	Configure account password user USER Nom d'utilisateur pour lequel vous voulez changer le mot de passe. L'utilisateur peut être « admin », « root » ou tout utilisateur du groupe d'administrateurs du serveur Smart Protection Server.

COMMANDE	SYNTAXE	DESCRIPTION
configure proxy-service	**configure proxy-service** <wis_url> <cfr_url> <grid_url> <mars_url>	Modification des URL du service de protection global Trend Micro. <wis_url> : URL du service d'inspection Web <cfr_url> : URL File Reputation de la communauté <grid_url> : URL de la base de données d'informations et de ressources Goodware <mars_url> : URL du service de réputation de l'application mobile
configure service	**configure service inter-face** <nom if>	Configuration des paramètres par défaut du serveur
configure timezone Africa Cairo	**configure timezone Africa Cairo**	Configuration du fuseau horaire sur Afrique/Le Caire.
configure timezone Africa Harare	**configure timezone Africa Harare**	Configuration du fuseau horaire sur Afrique/Harare.
configure timezone Africa Nairobi	**configure timezone Africa Nairobi**	Configuration du fuseau horaire sur Afrique/Nairobi
configure timezone America Anchorage	**configure timezone America Anchorage**	Configuration du fuseau horaire sur Amérique/ Anchorage
configure timezone America Bogota	**configure timezone America Bogota**	Configuration du fuseau horaire sur Amérique/ Bogota
configure timezone America Buenos_Aires	**configure timezone America Buenos_Aires**	Configuration du fuseau horaire sur Amérique/ Buenos Aires

COMMANDE	SYNTAXE	DESCRIPTION
`configure timezone America Caracas`	`configure timezone America Caracas`	Configuration du fuseau horaire sur Amérique/ Caracas
`configure timezone America Chicago`	`configure timezone America Chicago`	Configuration du fuseau horaire sur Amérique/ Chicago
`configure timezone America Chihuahua`	`configure timezone America Chihuahua`	Configuration du fuseau horaire sur Amérique/ Chihuahua
`configure timezone America Denver`	`configure timezone America Denver`	Configuration du fuseau horaire sur Amérique/ Denver
`configure timezone America Godthab`	`configure timezone America Godthab`	Configuration du fuseau horaire sur Amérique/Nuuk
`configure timezone America Lima`	`configure timezone America Lima`	Configuration du fuseau horaire sur Amérique/Lima
`configure timezone America Los_Angeles`	`configure timezone America Los_Angeles`	Configuration du fuseau horaire sur Amérique/Los Angeles
`configure timezone America Mexico_City`	`configure timezone America Mexico_City`	Configuration du fuseau horaire sur Amérique/ Mexico
`configure timezone America New_York`	`configure timezone America New_York`	Configuration du fuseau horaire sur Amérique/New York
`configure timezone America Noronha`	`configure timezone America Noronha`	Configuration du fuseau horaire sur Amérique/ Noronha
`configure timezone America Phoenix`	`configure timezone America Phoenix`	Configuration du fuseau horaire sur Amérique/ Phoenix

COMMANDE	SYNTAXE	DESCRIPTION
`configure timezone America Santiago`	`configure timezone America Santiago`	Configuration du fuseau horaire sur Amérique/ Santiago
`configure timezone America St_Johns`	`configure timezone America St_Johns`	Configuration du fuseau horaire sur Amérique/St Johns
`configure timezone America Tegucigalpa`	`configure timezone America Tegucigalpa`	Configuration du fuseau horaire sur Amérique/ Tegucigalpa
`configure timezone Asia Almaty`	`configure timezone Asia Almaty`	Configuration du fuseau horaire sur Asie/Almaty
`configure timezone Asia Baghdad`	`configure timezone Asia Baghdad`	Configuration du fuseau horaire sur Asie/Bagdad
`configure timezone Asia Baku`	`configure timezone Asia Baku`	Configuration du fuseau horaire sur Asie/Bakou
`configure timezone Asia Bangkok`	`configure timezone Asia Bangkok`	Configuration du fuseau horaire sur Asie/Bangkok
`configure timezone Asia Calcutta`	`configure timezone Asia Calcutta`	Configuration du fuseau horaire sur Asie/Calcutta
`configure timezone Asia Colombo`	`configure timezone Asia Colombo`	Configuration du fuseau horaire sur Asie/Colombo
`configure timezone Asia Dhaka`	`configure timezone Asia Dhaka`	Configuration du fuseau horaire sur Asie/Dhaka
`configure timezone Asia Hong_Kong`	`configure timezone Asia Hong_Kong`	Configuration du fuseau horaire sur Asie/Hong Kong
`configure timezone Asia Irkutsk`	`configure timezone Asia Irkutsk`	Configuration du fuseau horaire sur Asie/Irkoutsk
`configure timezone Asia Jerusalem`	`configure timezone Asia Jerusalem`	Configuration du fuseau horaire sur Asie/Jérusalem

COMMANDE	SYNTAXE	DESCRIPTION
`configure timezone Asia Kabul`	`configure timezone Asia Kabul`	Configuration du fuseau horaire sur Asie/Kaboul
`configure timezone Asia Karachi`	`configure timezone Asia Karachi`	Configuration du fuseau horaire sur Asie/Karachi
`configure timezone Asia Katmandu`	`configure timezone Asia Katmandu`	Configuration du fuseau horaire sur Asie/Katmandou
`configure timezone Asia Krasnoyarsk`	`configure timezone Asia Krasnoyarsk`	Configuration du fuseau horaire sur Asie/ Krasnoïarsk
`configure timezone Asia Kuala_Lumpur`	`configure timezone Asia Kuala_Lumpur`	Configuration du fuseau horaire sur Asie/Kuala Lumpur
`configure timezone Asia Kuwait`	`configure timezone Asia Kuwait`	Configuration du fuseau horaire sur Asie/Koweït
`configure timezone Asia Magadan`	`configure timezone Asia Magadan`	Configuration du fuseau horaire sur Asie/Magadan
`configure timezone Asia Manila`	`configure timezone Asia Manila`	Configuration du fuseau horaire sur Asie/Manille
`configure timezone Asia Muscat`	`configure timezone Asia Muscat`	Configuration du fuseau horaire sur Asie/Muscat
`configure timezone Asia Rangoon`	`configure timezone Asia Rangoon`	Configuration du fuseau horaire sur Asie/Rangoon
`configure timezone Asia Seoul`	`configure timezone Asia Seoul`	Configuration du fuseau horaire sur Asie/Séoul
`configure timezone Asia Shanghai`	`configure timezone Asia Shanghai`	Configuration du fuseau horaire sur Asie/Shanghai
`configure timezone Asia Singapore`	`configure timezone Asia Singapore`	Configuration du fuseau horaire sur Asie/Singapour

COMMANDE	SYNTAXE	DESCRIPTION
`configure timezone Asia Taipei`	`configure timezone Asia Taipei`	Configuration du fuseau horaire sur Asie/Taipei
`configure timezone Asia Tehran`	`configure timezone Asia Tehran`	Configuration du fuseau horaire sur Asie/Téhéran
`configure timezone Asia Tokyo`	`configure timezone Asia Tokyo`	Configuration du fuseau horaire sur Asie/Tokyo
`configure timezone Asia Yakutsk`	`configure timezone Asia Yakutsk`	Configuration du fuseau horaire sur Asie/Iakoutsk
`configure timezone Atlantic Azores`	`configure timezone Atlantic Azores`	Configuration du fuseau horaire sur Atlantique/ Açores
`configure timezone Australia Adelaide`	`configure timezone Australia Adelaide`	Configuration du fuseau horaire sur Australie/ Adélaïde
`configure timezone Australia Brisbane`	`configure timezone Australia Brisbane`	Configuration du fuseau horaire sur Australie/ Brisbane
`configure timezone Australia Darwin`	`configure timezone Australia Darwin`	Configuration du fuseau horaire sur Australie/Darwin
`configure timezone Australia Hobart`	`configure timezone Australia Hobart`	Configuration du fuseau horaire sur Australie/Hobart
`configure timezone Australia Melbourne`	`configure timezone Australia Melbourne`	Configuration du fuseau horaire sur Australie/ Melbourne
`configure timezone Australia Perth`	`configure timezone Australia Perth`	Configuration du fuseau horaire sur Australie/Perth
`configure timezone Europe Amsterdam`	`configure timezone Europe Amsterdam`	Configuration du fuseau horaire sur Europe/ Amsterdam
`configure timezone Europe Athens`	`configure timezone Europe Athens`	Configuration du fuseau horaire sur Europe/Athènes

Commande	Syntaxe	Description
`configure timezone Europe Belgrade`	`configure timezone Europe Belgrade`	Configuration du fuseau horaire sur Europe/Belgrade
`configure timezone Europe Berlin`	`configure timezone Europe Berlin`	Configuration du fuseau horaire sur Europe/Berlin
`configure timezone Europe Brussels`	`configure timezone Europe Brussels`	Configuration du fuseau horaire sur Europe/Bruxelles
`configure timezone Europe Bucharest`	`configure timezone Europe Bucharest`	Configuration du fuseau horaire sur Europe/Bucarest
`configure timezone Europe Dublin`	`configure timezone Europe Dublin`	Configuration du fuseau horaire sur Europe/Dublin
`configure timezone Europe Moscow`	`configure timezone Europe Moscow`	Configuration du fuseau horaire sur Europe/Moscou
`configure timezone Europe Paris`	`configure timezone Europe Paris`	Configuration du fuseau horaire sur Europe/Paris
`configure timezone Pacific Auckland`	`configure timezone Pacific Auckland`	Configuration du fuseau horaire sur Pacifique/Auckland
`configure timezone Pacific Fiji`	`configure timezone Pacific Fiji`	Configuration du fuseau horaire sur Pacifique/Fidji
`configure timezone Pacific Guam`	`configure timezone Pacific Guam`	Configuration du fuseau horaire sur Pacifique/Guam
`configure timezone Pacific Honolulu`	`configure timezone Pacific Honolulu`	Configuration du fuseau horaire sur Pacifique/Honolulu
`configure timezone Pacific Kwajalein`	`configure timezone Pacific Kwajalein`	Configuration du fuseau horaire sur Pacifique/Kwajalein

COMMANDE	SYNTAXE	DESCRIPTION
`configure timezone Pacific Midway`	`configure timezone Pacific Midway`	Configuration du fuseau horaire sur Pacifique/ Midway
`configure timezone US Alaska`	`configure timezone US Alaska`	Configuration du fuseau horaire sur États-Unis/ Alaska
`configure timezone US Arizona`	`configure timezone US Arizona`	Configuration du fuseau horaire sur États-Unis/ Arizona
`configure timezone US Central`	`configure timezone US Central`	Configuration du fuseau horaire sur États-Unis/ Central
`configure timezone US East-Indiana`	`configure timezone US East-Indiana`	Configuration du fuseau horaire sur États-Unis/Est de l'Indiana
`configure timezone US Eastern`	`configure timezone US Eastern`	Configuration du fuseau horaire sur États-Unis/Est
`configure timezone US Hawaii`	`configure timezone US Hawaii`	Configuration du fuseau horaire sur États-Unis/ Hawaii
`configure timezone US Mountain`	`configure timezone US Mountain`	Configuration du fuseau horaire sur États-Unis/ Montagnes Rocheuses
`configure timezone US Pacific`	`configure timezone US Pacific`	Configuration du fuseau horaire sur États-Unis/ Pacifique
`disable adhoc-query`	`disable adhoc-query`	Désactivation du journal d'accès Web
`disable ssh`	`disable ssh`	Désactivation du démon sshd
`enable`	`enable`	Activation des commandes d'administration

COMMANDE	SYNTAXE	DESCRIPTION
enable adhoc-query	**enable adhoc-query**	Activation du journal d'accès Web
enable hyperv-ic	**enable hyperv-ic**	Activation des composants d'intégration Hyper-V Linux sur le serveur Smart Protection Server
enable ssh	**enable ssh**	Activation du démon sshd
exit	**exit**	Quitter la session
aide	**aide**	Affichage d'une présentation de la syntaxe CLI.
history	**history** [limit]	Affichage de l'historique de ligne de commande de la session en cours `limit`spécifie le nombre de commandes CLI à afficher. Exemple : Une `limite` de « 5 » entraîne l'affichage de 5 commandes CLI.
reboot	**reboot** [time]	Redémarrage de cet ordinateur après un délai spécifié ou immédiatement `time` UNIT Temps en minutes pour le redémarrage de cet ordinateur [0]
show date	**show date**	Affichage de la date et de l'heure actuelle
show hostname	**show hostname**	Affichage du nom d'hôte du réseau
show interfaces	**show interfaces**	Affichage des informations de l'interface réseau

COMMANDE	SYNTAXE	DESCRIPTION
`show ipv4 address`	`show ipv4 address`	Affichage de l'adresse réseau IPv4
`show ipv4 dns`	`show ipv4 dns`	Affichage des serveurs DNS du réseau IPv4
`show ipv4 gateway`	`show ipv4 gateway`	Affichage de la passerelle réseau IPv4
`show ipv4 route`	`show ipv4 route`	Affichage de la table de routage réseau IPv4
`show ipv4 type`	`show ipv4 type`	Affichage du type de configuration réseau IPv4 (dhcp / statique)
`show ipv6 address`	`show ipv6 address`	Affichage de l'adresse réseau IPv6
`show ipv6 dns`	`show ipv6 dns`	Affichage des serveurs DNS du réseau IPv6
`show ipv6 gateway`	`show ipv6 gateway`	Affichage de la passerelle réseau IPv6
`show ipv6 route`	`show ipv6 route`	Affichage de la table de routage réseau IPv6
`show ipv6 type`	`show ipv6 type`	Affichage du type de configuration réseau IPv6 (auto / dhcp / statique)
`show timezone`	`show timezone`	Affichage du fuseau horaire du réseau
`show uptime`	`show uptime`	Affichage du temps utilisable système actuel
`show url management`	`show url management`	Affichage de l'URL de la console Web

COMMANDE	SYNTAXE	DESCRIPTION
show url FileReputationService	**show url FileReputationService**	Afficher les adresses de connexion des endpoints pour les services de File Reputation
show url WebReputationService	**show url WebReputationService**	Afficher les adresses de connexion des endpoints pour les services de réputation de sites Web
shutdown	**shutdown** [time]	Arrêt de cet ordinateur après un délai spécifié ou immédiatement time UNIT Temps en minutes pour l'arrêt de cet ordinateur [0]

Index

TREND MICRO INCORPORATED

Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France

Tél. : +33 (0) 1 76 68 65 00 info@trendmmicro.com

www.trendmicro.com

Item Code: APFM37522/160819