GUIDE D'ADMINISTRATION

Cisco Small Business

Cisco ProtectLink™ Endpoint 1.0

OL-24289-01

Table des matières

1

Présentation de Cisco ProtectLink Endpoint

Ce chapitre contient les rubriques suivantes :

Présentation générale de Cisco ProtectLink

Vous pouvez utiliser deux services Cisco ProtectLink pour offrir une solution de sécurité intégrée et multicouche de protection de l'entreprise et des utilisateurs :

- **ProtectLink Endpoint**
- **ProtectLink Web**
- **ProtectLink Gateway**

ProtectLink Endpoint

Cisco ProtectLink Endpoint est un service de sécurité hébergé optimisé par Trend Micro Worry-Free™ Business Security Hosted.

Ce service travaille avec le périphérique de sécurité Cisco, protège les ordinateurs et les serveurs Microsoft™ Windows™ contre les logiciels espions, les virus et autres logiciels malveillants. ProtectLink Endpoint autorise la mise en œuvre de stratégies d'accès au réseau en fonction du périphérique de sécurité.

En tant que service hébergé, Cisco ProtectLink Endpoint offre des avantages significatifs par rapport à une solution sur site :

- Autorise l'accès à la console où que vous soyez.
- Diminue la maintenance matérielle et logicielle sur site.

- Optimise la protection grâce à des mises à jour et à un ajustement réalisé par Cisco.
- Réduit les coûts d'infrastructure en facilitant le déploiement et l'administration.

ProtectLink Web

Cisco ProtectLink Web offre à tous les utilisateurs une protection contre les menaces Web afin d'éviter l'accès à des sites Web dangereux, ainsi qu'un filtrage des adresses URL destinées au contrôle de l'accès des employés à des sites Web considérés comme non liés à des sujets professionnels.

Cisco ProtectLink Web est un sous-ensemble de Cisco ProtectLink Gateway, mais offre une protection contre les menaces Web pour un nombre illimité d'utilisateurs, à la différence de Cisco ProtectLink Gateway, disponible sous la forme de licences pour 25 ou 100 postes.

ProtectLink Gateway

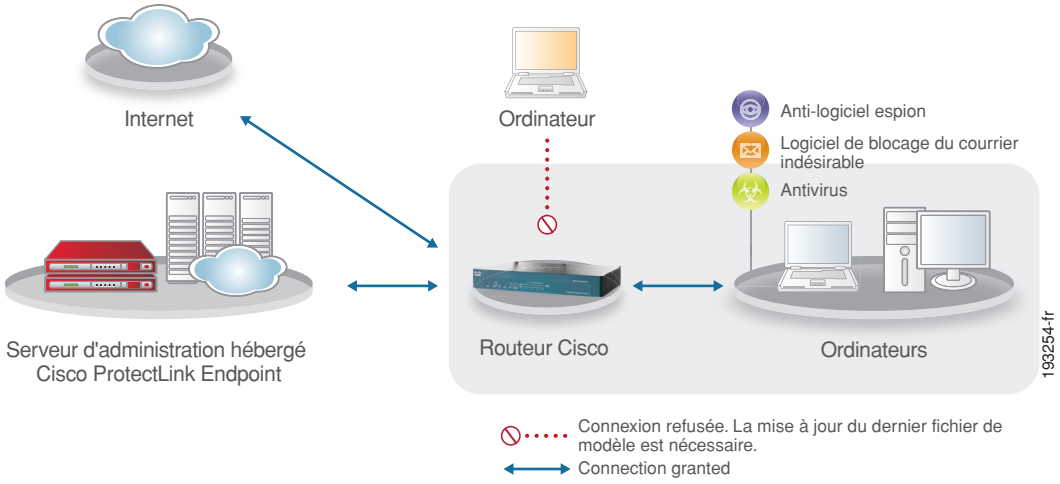
Cisco ProtectLink Gateway offre au routeur ou au périphérique de sécurité Cisco Small Business les fonctionnalités de sécurité Web de Cisco ProtectLink Web et les combine au système de sécurité de la messagerie électronique afin d'éviter le courrier indésirable, les virus et les tentatives d'hameçonnage.

Cependant, à la différence de Cisco ProtectLink Web, Cisco ProtectLink Gateway est disponible sous la forme de licences pour 25 ou 100 postes.

Principes de fonctionnement de Cisco ProtectLink Endpoint

La **Figure 1** affiche le flux du trafic sur les sites Web et du trafic de messagerie lors d'un accès à Internet via le service Cisco ProtectLink Endpoint Service et le périphérique de sécurité Cisco Small Business. Cisco ProtectLink Endpoint Service protège les ordinateurs de bureau qui utilisent Trend Micro WFBS-H.

Figure 1 Principes de fonctionnement de ProtectLink Endpoint



Protection des ordinateurs de bureau

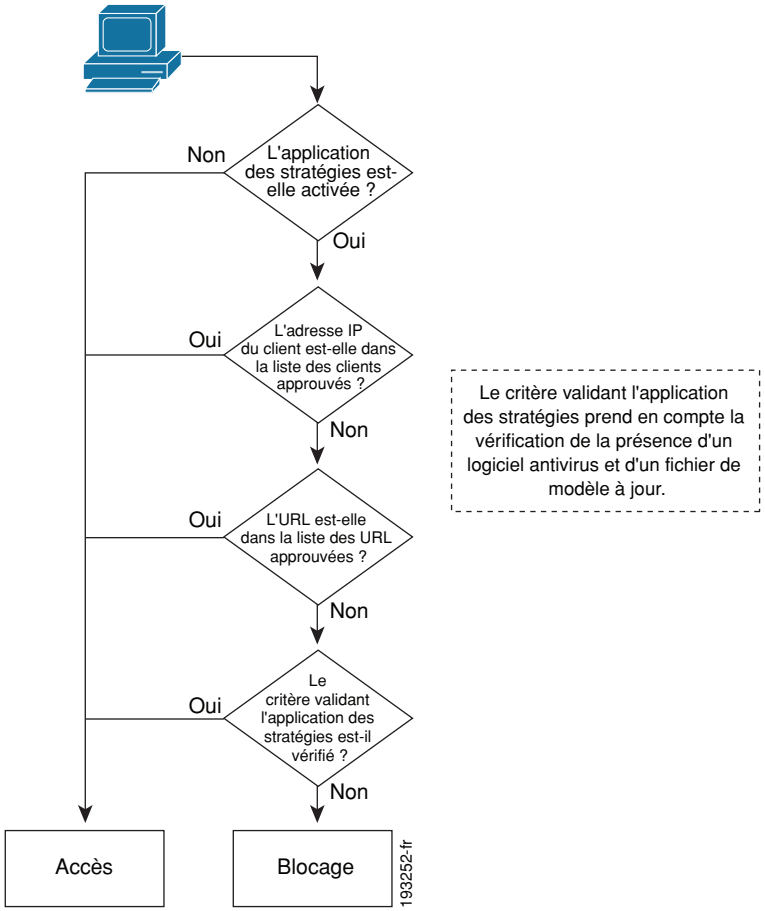
Cisco ProtectLink Endpoint s'intègre à Trend Micro WFBS-H pour offrir une protection des ordinateurs de bureau.

CONSEIL Pour obtenir de plus amples informations ou des documents relatifs à Worry-Free Business Security Hosted, accédez à l'adresse : http://us.trendmicro.com/us/products/sb/worry-free-business-security-hosted

Grâce à WFBS-H, une solution hébergée, les administrateurs peuvent automatiquement éviter les menaces sur les réseaux. Ils peuvent également créer des rapports, consulter l'état (résumé ou complet) des menaces, des risques liés à la sécurité et des mises à jour système.

Après avoir installé WFBS-H Agent sur un ordinateur, procédez à l'installation de Threat Management Agent (TMAgent). TMAgent permet d'avoir la garantie que chaque ordinateur dispose d'une solution antivirus. S'il existe des ordinateurs sur lesquels TMAgent n'est pas installé, le périphérique de sécurité bloque l'accès au Web. Cette fonctionnalité offre une protection en évitant que des attaques perpétrées sur des ordinateurs vulnérables exposent le réseau à des menaces. La **Figure 2** illustre le workflow.

Figure 2 Workflow de Endpoint Protection



Avantages de l'utilisation de ProtectLink Endpoint

Les services hébergés offrent un avantage important par rapport à une solution sur site :

- Le réseau est complètement protégé des menaces provenant des e-mails et du Web.
- Préserve la bande passante de connexion à Internet.
- Diminue la quantité de matériel et de logiciel sur site.
- Optimise la protection grâce à des mises à jour et à un ajustement réalisé par Cisco.
- Réduit les coûts d'infrastructure en facilitant le déploiement et l'administration.

REMARQUE Pour de plus amples informations sur ProtectLink Web et ProtectLink Gateway, veuillez vous reporter à *ProtectLink Web and Gateway 1.0 Administration Guide*.

2

Déployer Cisco ProtectLink Endpoint

Vous pouvez déployer Cisco ProtectLink Endpoint en suivant la procédure simple décrite dans les sections suivantes :

- **Configuration système requise, page 10**
- **Configuration du routeur et mise à niveau du microprogramme, page 12**
- **Enregistrer ProtectLink Endpoint, page 13**
- **Activer ProtectLink Endpoint, page 20**

REMARQUE Avant de suivre ces instructions, vous devez tout d'abord effectuer les tâches de configuration initiales pour votre périphérique de sécurité. Pour plus d'informations, reportez-vous à la documentation de votre périphérique de sécurité.

Configuration système requise

Vous pouvez utiliser ce service sur les ordinateurs dont la configuration du système et du navigateur web respecte les exigences suivantes :

- Système d'exploitation :

  Windows 2000 Édition 32 bits ;

  - Microsoft Windows 2000 Édition Professionnelle avec Service Pack 4 ou ultérieur ;
  - Microsoft Windows 2000 Server Edition avec Service Pack 4 ou ultérieur ;
  - Microsoft Windows 2000 Advanced Edition avec Service Pack 4 ou ultérieur ;

  Windows XP Édition 32 bits ou 64 bits ;

  - Microsoft Windows XP Professional avec Service Pack 2 ;

- Microsoft Windows XP Édition Familiale avec Service Pack 2 ;
- Microsoft Windows XP Édition Tablet PC avec Service Pack 2 ;

Windows Server 2003 Édition 32 bits ou 64 bits ;

- Microsoft Windows Server 2003 Édition Standard (avec Service Pack 1) ;
- Microsoft Windows Server 2003 Édition Entreprise avec Service Pack 1) ;
- Microsoft Windows Server 2003 R2 Édition Standard (avec Service Pack 1) ;
- Microsoft Windows Server 2003 R2 Édition Enterprise (avec Service Pack 1) ;

Windows Small Business Server 2003 R2 Édition 32 bits ou 64 bits ;

- Microsoft Windows Small Business Server 2003 R2 Édition Standard ;
- Microsoft Windows Small Business Server 2003 R2 Édition Premium ;

Windows Vista Édition 32 bits ou 64 bits ;

- Microsoft Windows Vista Édition Familiale Basique ;
- Microsoft Windows Vista Édition Familiale Premium ;
- Microsoft Windows Vista Édition Professionnelle ;
- Microsoft Windows Vista Édition Entreprise ;
- Microsoft Windows Vista Édition Intégrale ;

Windows Server 2008 Édition 32 bits ou 64 bits ;

- Microsoft Windows Server 2008 Édition Standard ;
- Microsoft Windows Server 2008 Édition Datacenter ;
- Microsoft Windows Server 2008 Édition Entreprise ;

Windows Small Business Server 2008 Édition 32 bits ou 64 bits ;

- Microsoft Windows Small Business Server 2008 Édition Standard ;
- Microsoft Windows Small Business Server 2008 Édition Premium ;

Windows Essential Business Server 2008 Édition 32 bits ou 64 bits ;

- Microsoft Windows Essential Business Server 2008 Édition Standard ;
- Microsoft Windows Essential Business Server 2008 Édition Premium ;

Windows Home Server Édition 32 bits ;

- Microsoft Windows Home Server ;

- Processeur : Intel™ Pentium™ ou AMD™ ;
- RAM : 256 Mo ou plus (en fonction du système d'exploitation) ;
- Espace disque : 350 Mo ;
- Navigateur web : Microsoft Internet Explorer version 6.0 ou 7.0 ;
- Moniteur prenant en charge une résolution de 800 x 600 avec 256 couleurs ;
- Connexion Internet ;
- Adobe™ Acrobat™ Reader version 7.0 ou 8.0 pour l'affichage des rapports ;
- Un périphérique de sécurité de la série 500 si vous devez utiliser la fonctionnalité d'application de ProtectLink Endpoint.

Configuration du routeur et mise à niveau du microprogramme

Configurez le routeur ou le périphérique de sécurité et installez le dernier microprogramme en suivant les instructions se trouvant dans la documentation du périphérique. Une fois le dernier microprogramme installé, l'utilitaire de configuration intègre un module ProtectLink qui se trouve dans la barre de menus. Reportez-vous aux exemples suivants :

REMARQUE Si ProtectLink est pris en charge par le routeur ou le périphérique de sécurité et qu'il n'apparaît pas dans la barre de menus, procédez à la mise à niveau du microprogramme. Pour de plus amples informations, reportez-vous au guide d'administration du périphérique.

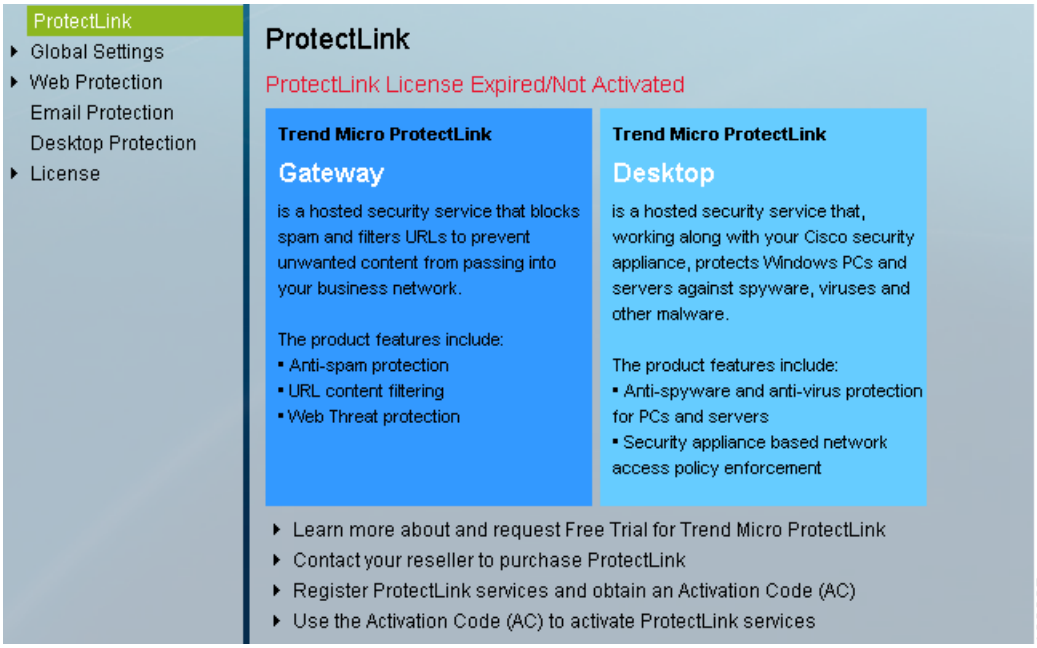
Enregistrer ProtectLink Endpoint

Enregistrez votre service pour l'activer et abonnez-vous pour accéder au portail web de l'administration en ligne. Pour enregistrer un service, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

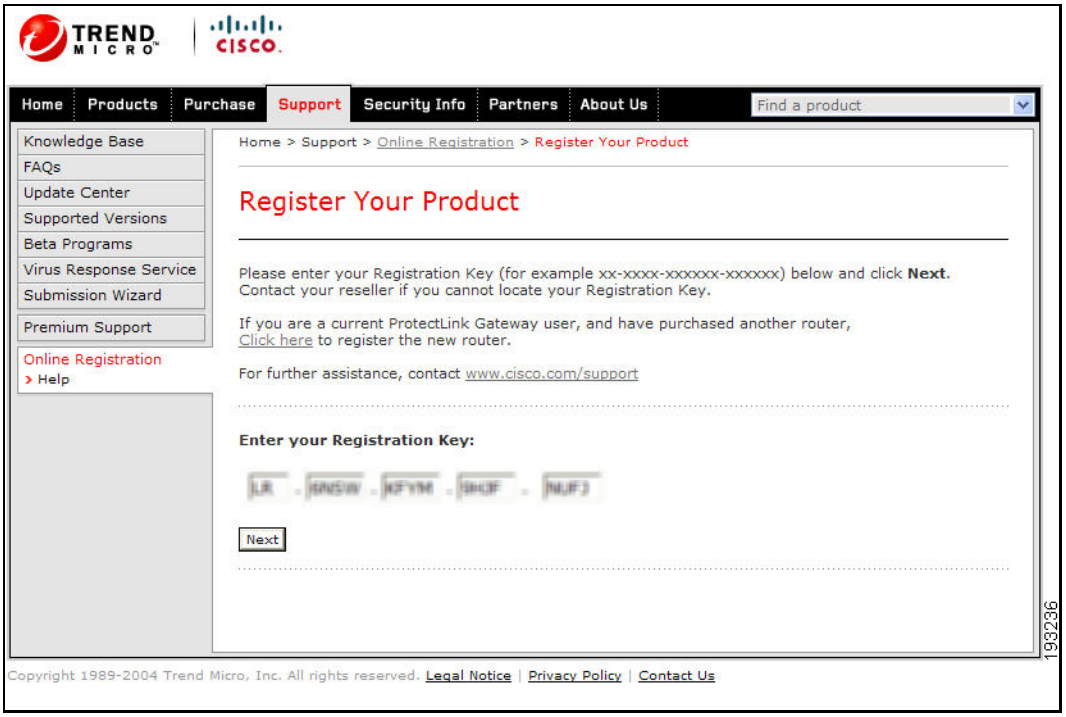
ÉTAPE 2 Dans la barre de menus cliquez sur **ProtectLink**, puis cliquez sur **ProtectLink** dans l'arborescence de navigation.

La page ProtectLink s'affiche.



ÉTAPE 3 Cliquez sur le lien : **Register ProtectLink services and obtain an Activation Code (AC).**

La page Register Your Product s'affiche.

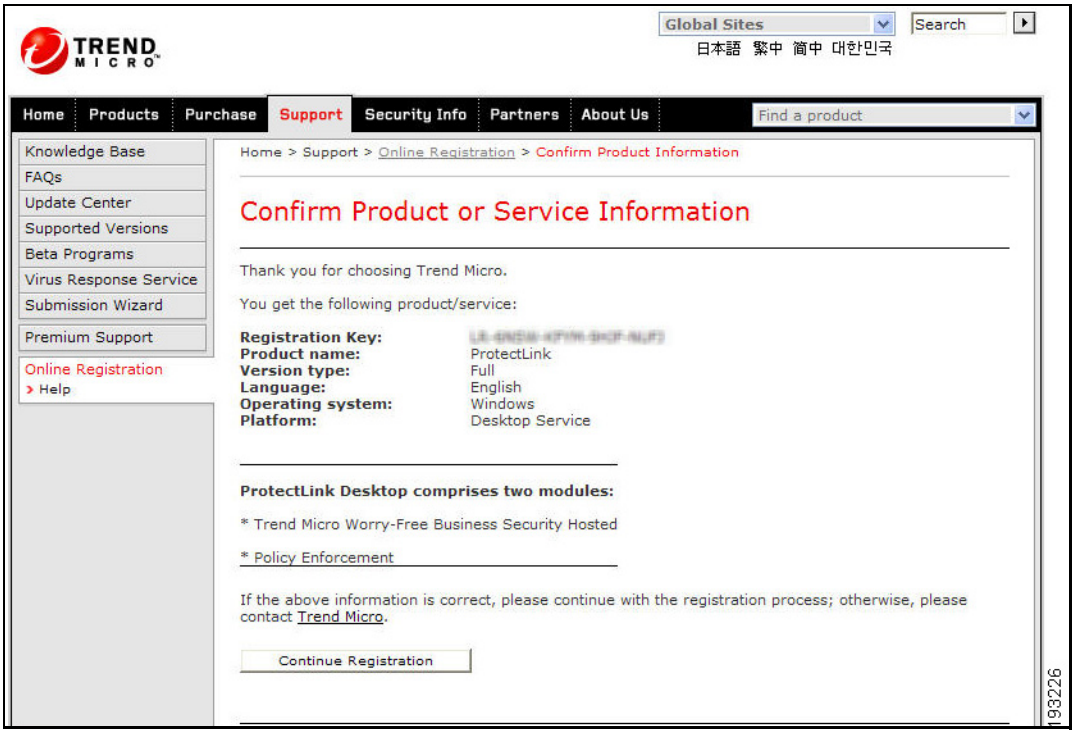


ÉTAPE 4 Saisissez la **clé d'enregistrement**, puis cliquez sur **Next**.

La page Confirm License Terms s'affiche.

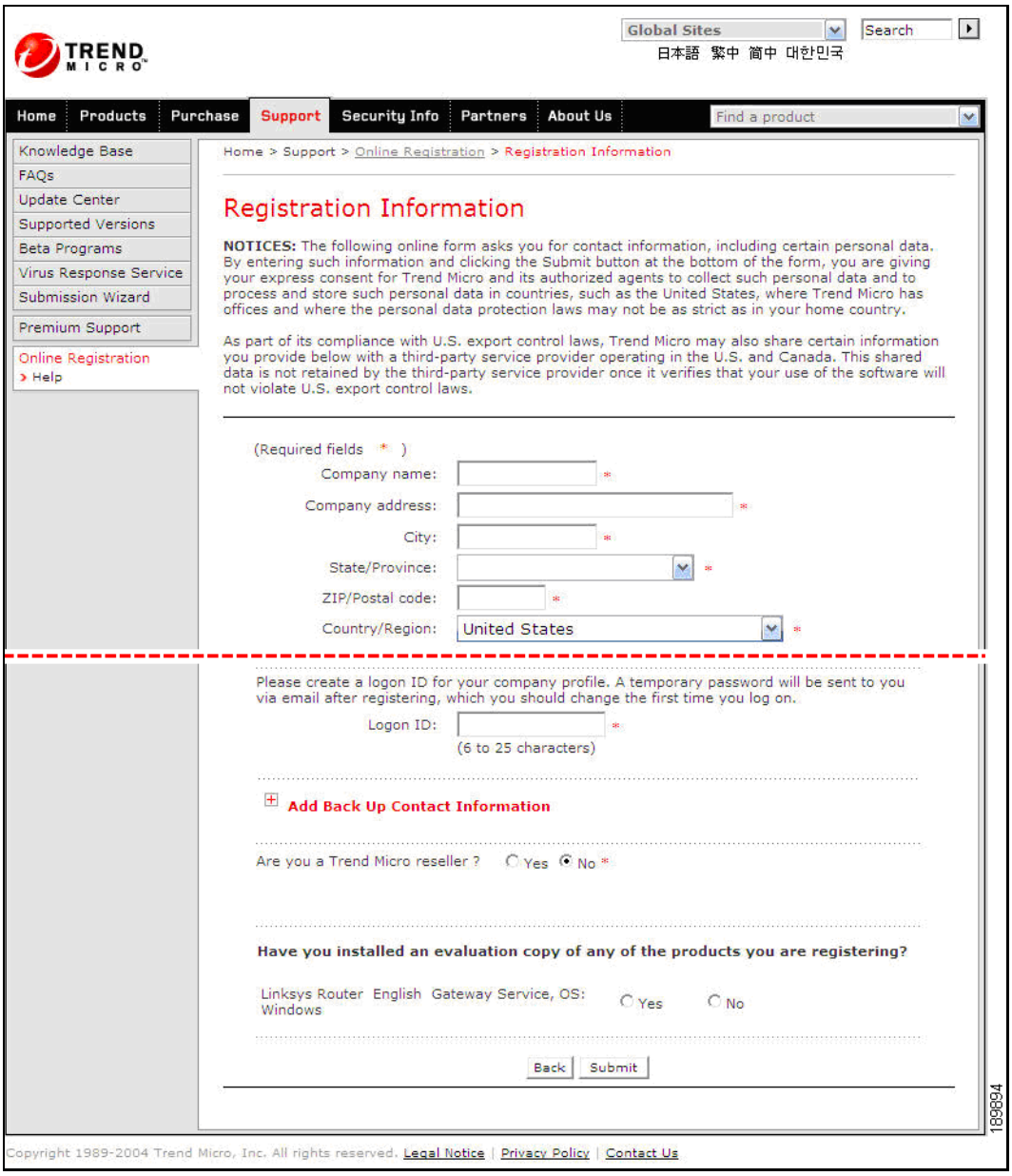
ÉTAPE 5 Lisez soigneusement les conditions de licence. Si vous acceptez les conditions, cliquez sur **I Accept**, puis cliquez sur **Submit**.

La page Confirm Product or Service Information s'affiche.



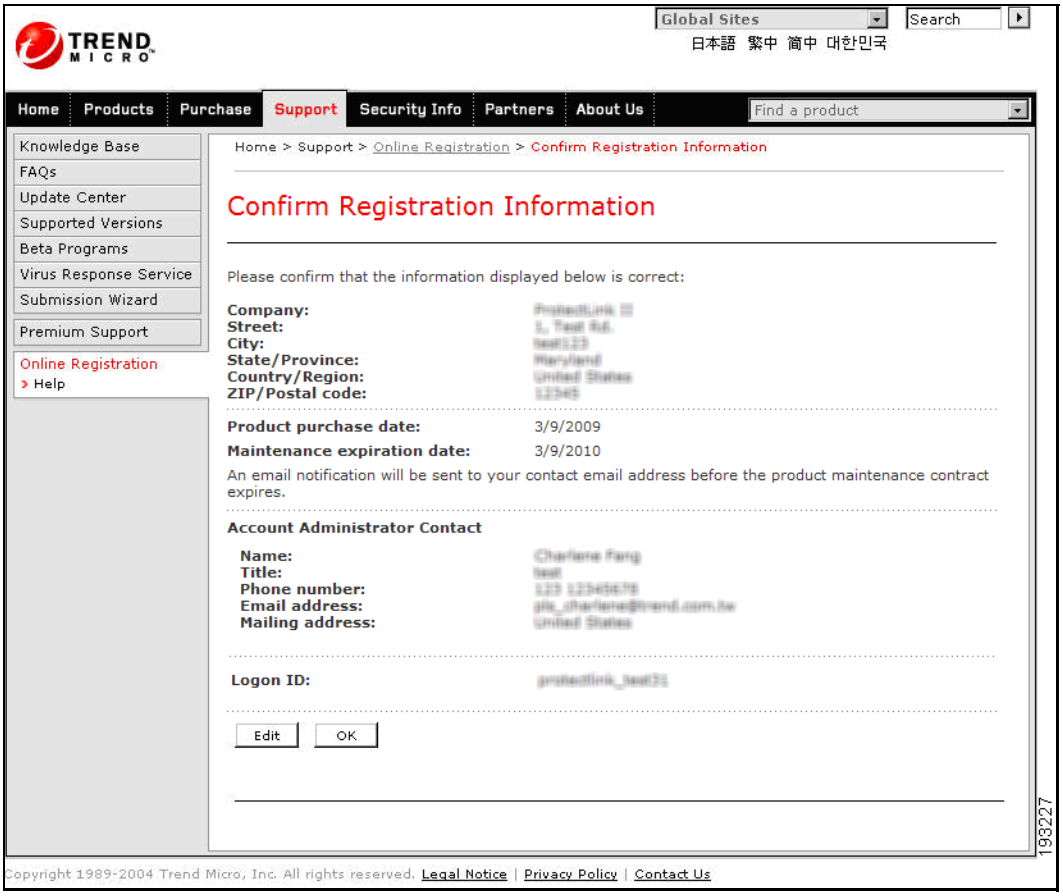
ÉTAPE 6 Cliquez sur **Continue Registration**.

La page Registration Information s'affiche.



ÉTAPE 7 Saisissez l'intégralité de vos coordonnées, y compris votre adresse électronique et un identifiant de connexion pour le profil de votre société, puis cliquez sur **Submit**.

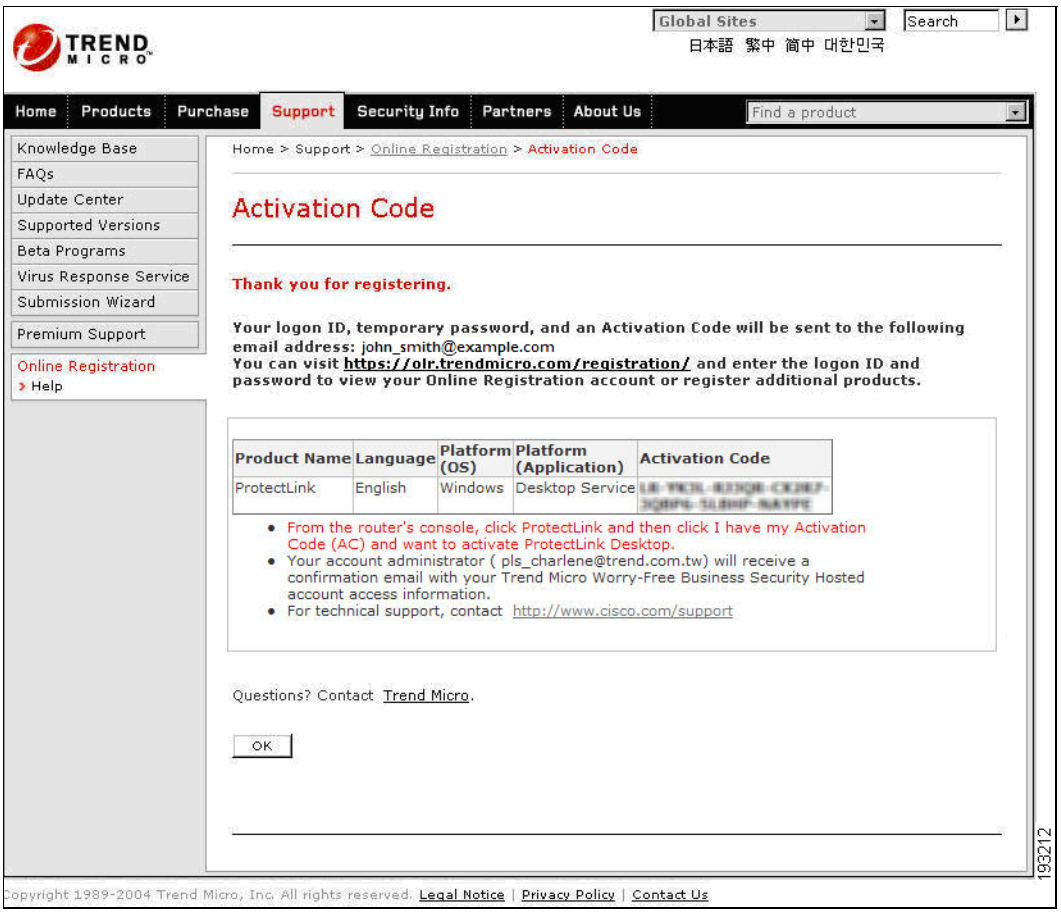
La page Confirm Registration s'affiche, avec vos coordonnées et vos domaines.



ÉTAPE 8 Vérifiez que les informations sont correctes.

- Cliquez sur **Edit** si vous devez procéder à des modifications.
- Si les informations sont correctes, cliquez sur **OK**. ProtectLink Endpoint est activé.

La page Activation Code s'affiche et indique votre code d'activation. Vous pouvez imprimer cette page et la conserver pour vous y référer ultérieurement.



REMARQUE **Par la suite**, vous pouvez accéder à https://olr.trendmicro.com/registration/ pour consulter votre compte en ligne ou pour enregistrer de nouveaux produits Cisco ProtectLink.

ÉTAPE 9 Cliquez sur **OK** pour terminer le processus d'enregistrement.

Activer ProtectLink Endpoint

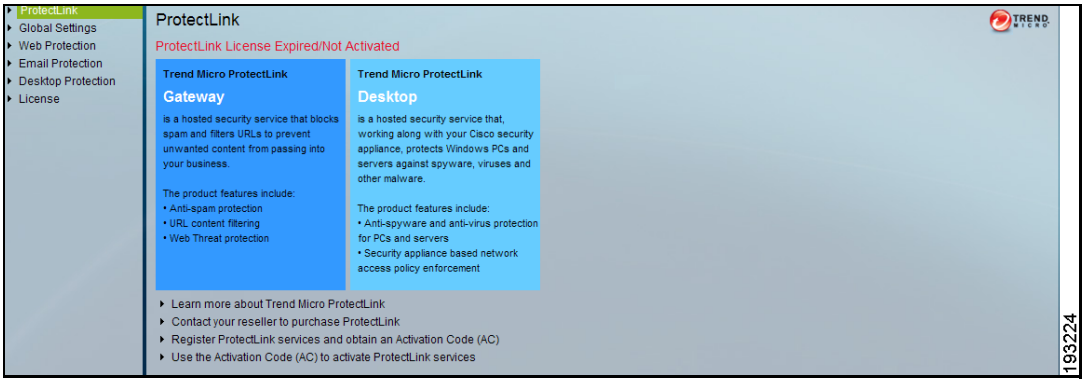
Vous devriez recevoir dans les 24 heures un message électronique vous indiquant que vous avez enregistré votre compte ProtectLink Endpoint avec succès (Reportez-vous à **Chapitre 6, « Courrier électronique post-enregistrement et post-activation »**). Le message électronique contient l'URL permettant d'accéder à la console, votre identifiant de connexion et un mot de passe temporaire, que vous devrez changer lors de votre prochaine connexion.

Pour commencer à utiliser ProtectLink Endpoint, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink.**

La page ProtectLink s'affiche.



ÉTAPE 3 En bas de la page, cliquez sur le lien : **Use the Activation Code (AC) to activate ProtectLink services.**

La page Activate Your Product: > Step 1: Enter Activation Code s'affiche.

ÉTAPE 4 Saisissez votre **code d'activation**, puis cliquez sur **Next**.

La page Activate Your Product: > Step 2: Verify Product Information s'affiche.

ÉTAPE 5 Vérifiez que les informations indiquées sont correctes.

- Un message s'affiche si des informations doivent être corrigées. Vous pouvez cliquer sur **Back** et modifier ces informations.
- Si les informations sont correctes, cliquez sur **Next**.

La page Activate Your Product: > Step 3: Finish Activation s'affiche. Vous avez activé le produit avec succès.

3

Configuration de Cisco ProtectLink Endpoint

Une fois que vous avez activé votre compte, configurez votre périphérique de sécurité pour la protection des ordinateurs de bureau, en procédant de la manière indiquée dans les sections suivantes :

- **Garantir la protection des ordinateurs de bureau connectés au réseau, page 23**
- **Activer l'application de la politique, page 31**
- **Configuration des paramètres globaux, page 32**
- **État et renouvellement de la licence, page 35**
- **Activer le journal système > Journal des événements de blocage d'appels sortants, page 53**

Garantir la protection des ordinateurs de bureau connectés au réseau

La protection des ordinateurs de bureau est assurée par Trend Micro WFBS-H. Avant d'activer le système, vous devez installer les composants requis sur tous les ordinateurs qui utilisent un périphérique de sécurité pour accéder à Internet. Une fois l'application de la politique activée, seuls les ordinateurs disposant d'un agent hébergé Worry-Free Business Security (ou de toute autre application antivirus) avec des fichiers de signature à jour et un agent de gestion des menaces seront autorisés à accéder à Internet.

La liste suivante résume les tâches à effectuer. Les procédures sont expliquées en détail après ce résumé.

1. Créez les paquets WFBS-H.

2. Installez les paquets sur les ordinateurs.

3. Téléchargez et installez le TMAgent sur tous les ordinateurs.

1. Créez les paquets WFBS-H.

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **Web Protection > Desktop Protection** dans l'arborescence de navigation.

ÉTAPE 3 Sur la page ProtectLink Endpoint, cliquez sur le lien WFBS-H pour accéder au portail web WFBS-H dont voici l'URL :

https://wfbs-h.trendmicro.com/wfbsh/protectlinklogin.aspx

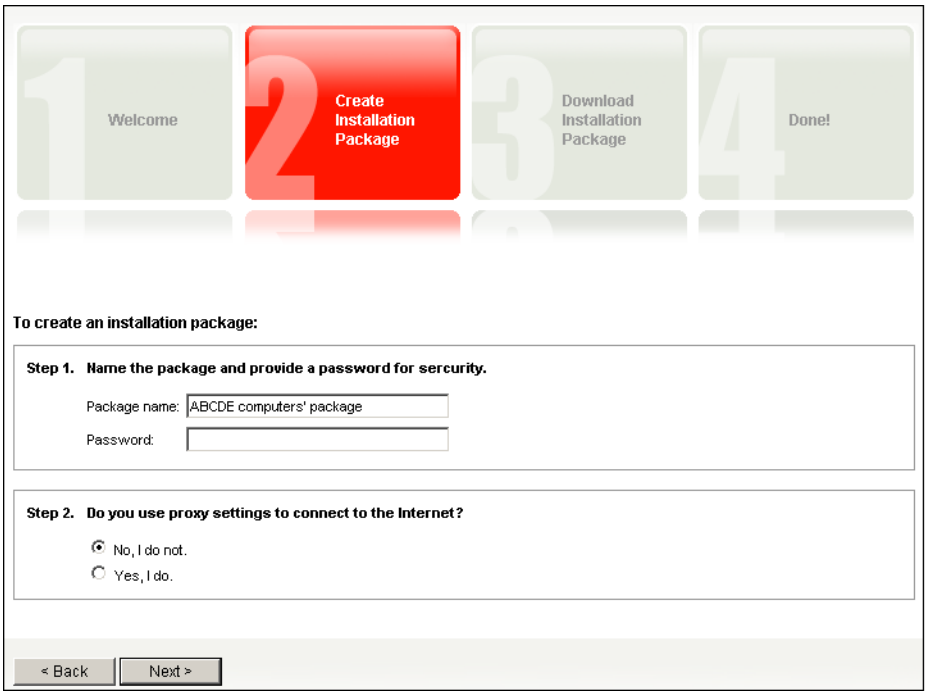
La page de connexion s'affiche.

ÉTAPE 4 Saisissez le **nom d'utilisateur WFBS-H** et le **mot de passe** temporaire que vous avez reçus lorsque vous avez activé Cisco ProtectLink Endpoint. Cliquez sur **Log on**.

La page d'accueil s'affiche. Vous pouvez voir votre code d'activation sur la page d'accueil.

ÉTAPE 5 Cliquez sur **Next** pour créer les paquets.

La page Create Installation Package s'affiche.

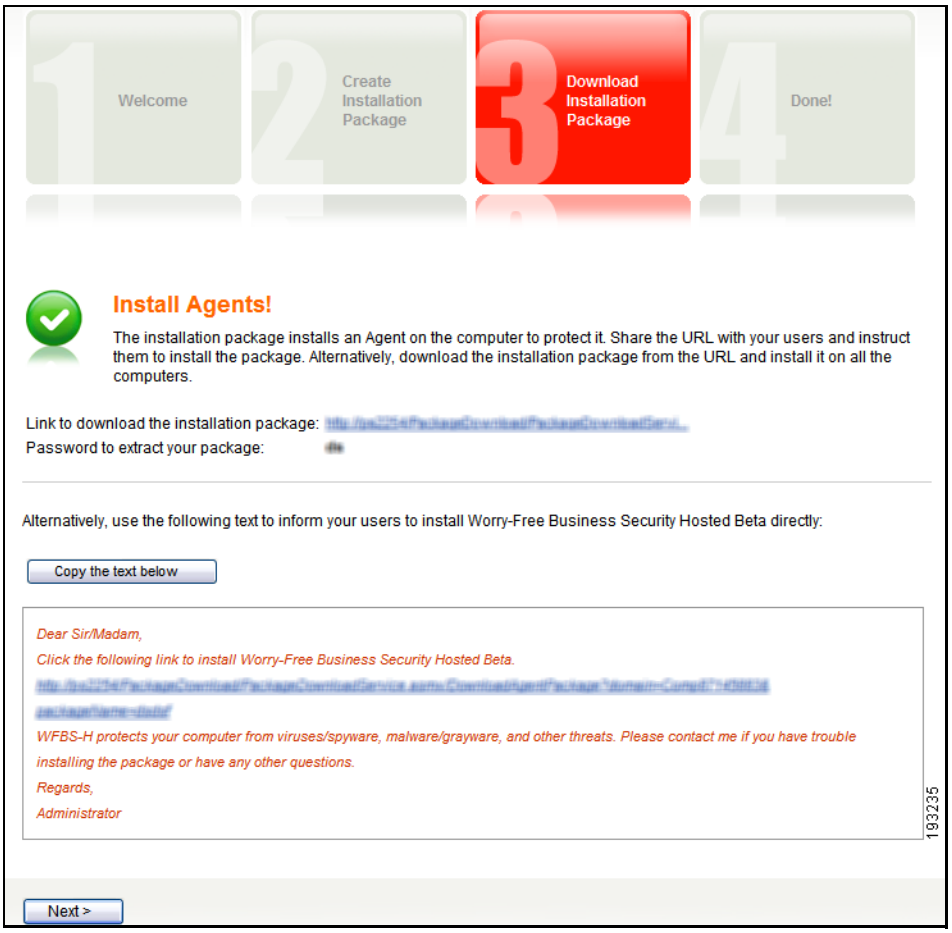


ÉTAPE 6 Pour créer les paquets qui permettent d'installer les agents sur les ordinateurs clients, saisissez les informations suivantes :

- **Package Name** : saisissez un nom de paquet.
- **Password** : saisissez un mot de passe, qui devra être utilisé pour extraire le paquet.
- **Do you use proxy settings to connect to the Internet?** :
  - Si vous n'utilisez pas de paramètres proxy, cliquez sur **No, I do not**.
  - Si vous utilisez des paramètres proxy, cliquez sur **Yes, I do**. Les options de configuration s'affichent.
- Si vous utilisez des paramètres proxy, sélectionnez les paramètres proxy requis pour que les agents puissent communiquer avec le serveur WFBS-H :
  - **Automatically detect settings** : le programme d'installation de l'agent détecte automatiquement les paramètres requis pour installer le paquet.
  - **Automatic configuration script** : WFBS-H met à jour l'emplacement du script de configuration dans le champ Address. Il utilise le script de configuration de cette URL pour installer le paquet.
  - **Manual configuration** : WFBS-H met à jour la configuration proxy suivante dans le champ Manual configuration.
- Si vous avez choisi la configuration manuelle, saisissez les informations suivantes :
  - **Server IP Address** : saisissez l'adresse IP du serveur proxy. Vous pouvez trouver l'adresse IP du serveur proxy dans les paramètres d'Internet Explorer.
  - **Port** : saisissez le numéro de port utilisé par le serveur proxy pour les connexions clients.
  - **User ID** : saisissez le nom de compte utilisé par l'ordinateur client pour se connecter au serveur proxy.
  - **Password** : saisissez le mot de passe correspondant à cet identifiant utilisateur.

ÉTAPE 7 Cliquez sur **Next**.

La page Download Installation Package s'affiche.



ÉTAPE 8 Pour télécharger le paquet d'installation, cliquez sur le **lien désigné par : Link to download the installation package**.

Vous pouvez également cliquer sur **Copy the text below** pour copier le texte dans la zone. Vous pouvez utiliser ce texte pour informer les utilisateurs qu'ils doivent installer l'agent.

ÉTAPE 9 Cliquez sur **Next**.

La page Done s'affiche.

ÉTAPE 10 Cliquez sur **OK**.

La page Summary s'affiche.

REMARQUE Ensuite, poursuivez vers **2. Installez les paquets sur les ordinateurs.**

2. Installez les paquets sur les ordinateurs.

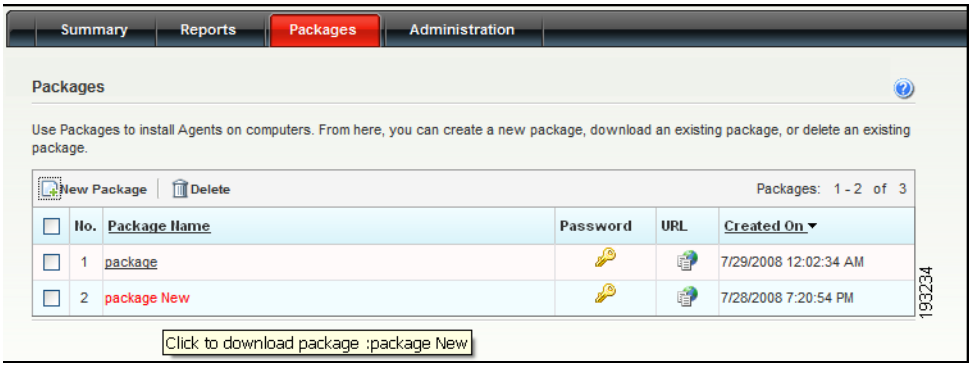
Une fois que vous avez créé un paquet, suivez ces étapes pour télécharger et installer ces paquets sur les ordinateurs connectés au périphérique de sécurité.

REMARQUE Une fois que vous avez installé un paquet, il faut environ une heure avant que les agents commencent à envoyer des rapports à WFBS-H.

ÉTAPE 1 Pour reprendre la procédure précédente, cliquez sur l'onglet **Packages** du portail web WFBS-H.

> **REMARQUE** Pour accéder au portail web WFBS-H, lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous. Dans la barre de menu, cliquez sur **ProtectLink,** puis sur **Web Protection > Desktop Protection** dans l'arborescence de navigation. Sur la page ProtectLink Endpoint, cliquez sur le lien WFBS-H. Connectez-vous ensuite au portail web WFBS-H.

La page Packages s'affiche.



ÉTAPE 2 Dans la liste, cliquez sur le nom du paquet. La boîte de dialogue **File Download** s'affiche.

ÉTAPE 3 Cliquez sur **Save** pour enregistrer le paquet sur votre ordinateur.

ÉTAPE 4 Installez ces paquets sur les ordinateurs que vous souhaitez protéger.

> **REMARQUE** Pour les ordinateurs sous Windows Vista, installez le paquet avec les droits administrateurs (à l'aide de l'option **Exécuter en tant qu'administrateur**).

REMARQUE Ensuite, poursuivez vers **3. Téléchargez et installez le TMAgent sur tous les ordinateurs.**

3. Téléchargez et installez le TMAgent sur tous les ordinateurs.

Le TMAgent garantit qu'un antivirus est installé chez le client. Si aucun antivirus n'est installé sur un ordinateur, le TMAgent alerte le périphérique de sécurité. Lorsque l'application de la politique est activée sur le périphérique de sécurité, les ordinateurs non protégés ne peuvent plus accéder au web.

ÉTAPE 1 Téléchargez le TMAgent à partir de l'URL suivante :

www.trendmicro.com/download/product.asp?productid=94

ÉTAPE 2 Cliquez sur le lien menant au fichier (.MSI).

ÉTAPE 3 Lorsque la consigne de sécurité s'affiche, cliquez sur **Save**, puis choisissez un emplacement sur votre ordinateur.

ÉTAPE 4 Une fois le fichier téléchargé, double-cliquez dessus pour exécuter le programme d'installation.

ÉTAPE 5 Installez le TMAgent sur tous les ordinateurs connectés au périphérique de sécurité.

Activer l'application de la politique

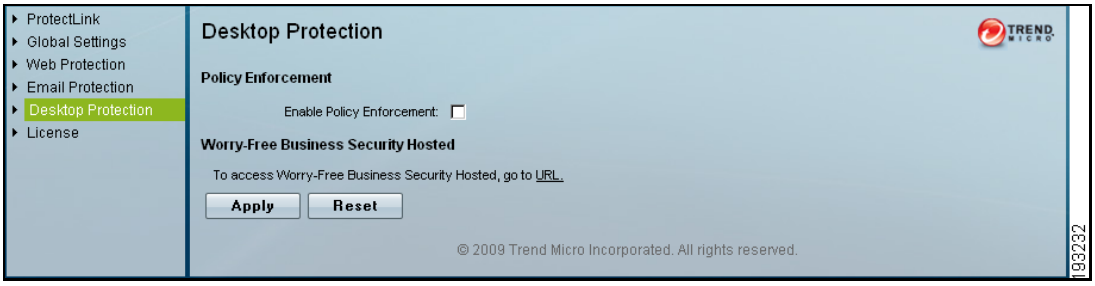
Activez l'application de la politique pour vous assurer que seuls les ordinateurs protégés peuvent accéder à Internet.

Pour activer l'application de la politique, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **Web Protection > Desktop Protection** dans l'arborescence de navigation.

La page Desktop Protection Policy Enforcement s'affiche.



ÉTAPE 3 Cochez la case **Enable Policy Enforcement** . Une fois cette fonctionnalité activée, seuls les ordinateurs disposant d'un Worry-Free Business Security Hosted Agent (ou de toute autre application antivirus) avec des fichiers de signature à jour et un agent de gestion des menaces seront autorisés à accéder à Internet.

> **REMARQUE** Seul le port 80 sera bloqué sur les ordinateurs qui ne respectent pas ces exigences.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration des paramètres globaux

Cette section comporte les tâches suivantes :

Configuration des clients approuvés

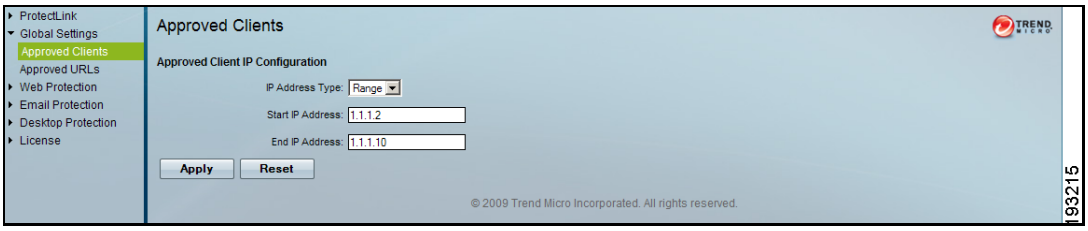
- La liste des clients approuvés répertorie les ordinateurs qui ont un accès au web sans restriction. Pour configurer les clients approuvés, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **Global Settings > Approved Clients**.

ÉTAPE 3 Pour activer cette fonctionnalité, cochez la case **Enable Approved Clients List**, puis cliquez sur **Apply**.

ÉTAPE 4 Pour ajouter un nouvel ordinateur à la liste, cliquez sur **Add**.



ÉTAPE 5 Saisissez les informations suivantes :

- **IP Address Type** : choisissez **Single** pour saisir une seule adresse IP ou **Range** pour indiquer une plage d'adresses IP.
- **Start IP Address** : s'il n'y a qu'une adresse IP (option Single sélectionnée), saisissez-la ici. S'il y a une plage d'adresses IP (Range), saisissez ici la première d'entre elles.
- **End IP Address** : s'il n'y a qu'une adresse IP (Single), ne pas renseigner ce champ. S'il y a une plage d'adresses IP (Range), saisissez ici la dernière d'entre elles. ProtectLink approuvera l'ensemble des requêtes d'URL provenant des adresses IP spécifiées. Par exemple, 1.1.1.2 à 1.1.1.10 permettra l'approbation de toutes les adresses IP qui se trouvent dans cette plage.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres. Les détails s'affichent dans la liste des clients approuvés de la page Approved Clients.

Configuration des URL approuvées

La liste des URL approuvées répertorie la liste des sites web qui peuvent être consultés. Les sites approuvés sont définis par des URL spécifiques ou par des mots clés dans les URL.

Pour configurer les URL approuvées, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **Global Settings > Approved URLs**.

ÉTAPE 3 Pour activer cette fonctionnalité, cochez la case **Enable Approved URLs List**, puis cliquez sur **Apply**.

ÉTAPE 4 Pour ajouter une URL ou un mot clé à la liste, cliquez sur **Add**.

ÉTAPE 5 Saisissez les informations suivantes :

- **URL** : saisissez le nom du site ou un mot clé.
- **Match Type** : choisissez l'une des options suivantes :
  - **Web site** : choisissez cette option si vous ne souhaitez permettre l'accès qu'à l'URL exacte que vous avez entrée dans la zone de texte URL. Par exemple, si vous avez entré *www.yahoo.com* pour l'URL, les utilisateurs pourront accéder à www.yahoo.com, mais ils ne pourront pas aller sur www.yahoo.com.uk ou www.yahoo.co.jp
  - **URL keyword** : choisissez cette option si vous souhaitez autoriser l'accès à toutes les URL qui contiennent le mot clé que vous avez entré dans la zone de texte URL. Par exemple, si vous avez entré *yahoo* pour l'URL, les utilisateurs pourront accéder à www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk et www.yahoo.co.jp

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres. Les détails s'affichent dans la liste des clients approuvés de la page Approved Clients.

État et renouvellement de la licence

Dans l'utilitaire de configuration de votre périphérique de sécurité ou de votre routeur, vous pouvez vérifier l'état de votre licence et ajouter des postes au compte ProtectLink.

Cette section comporte les tâches suivantes :

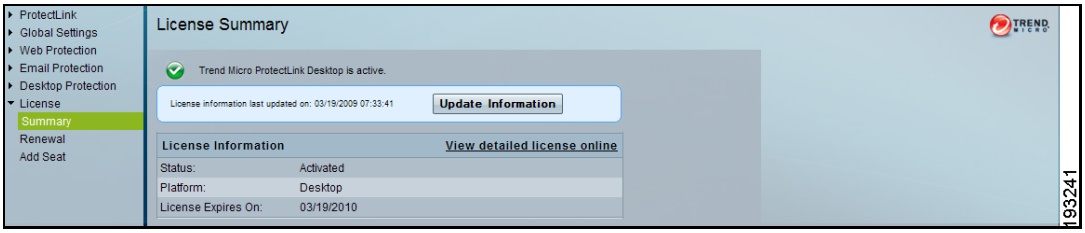
- **Renouveler une licence, page 37**
- **Ajouter des postes, page 44**

Pour vérifier les informations de licence, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink**, puis sur **License > Summary** dans l'arborescence de navigation.

La page License Summary s'affiche et vous indique l'état de la licence.



Vous pouvez effectuer les tâches suivantes :

- Afficher les informations de licence détaillées ;
- Renouveler la licence ;
- Ajouter des postes à une licence existante.

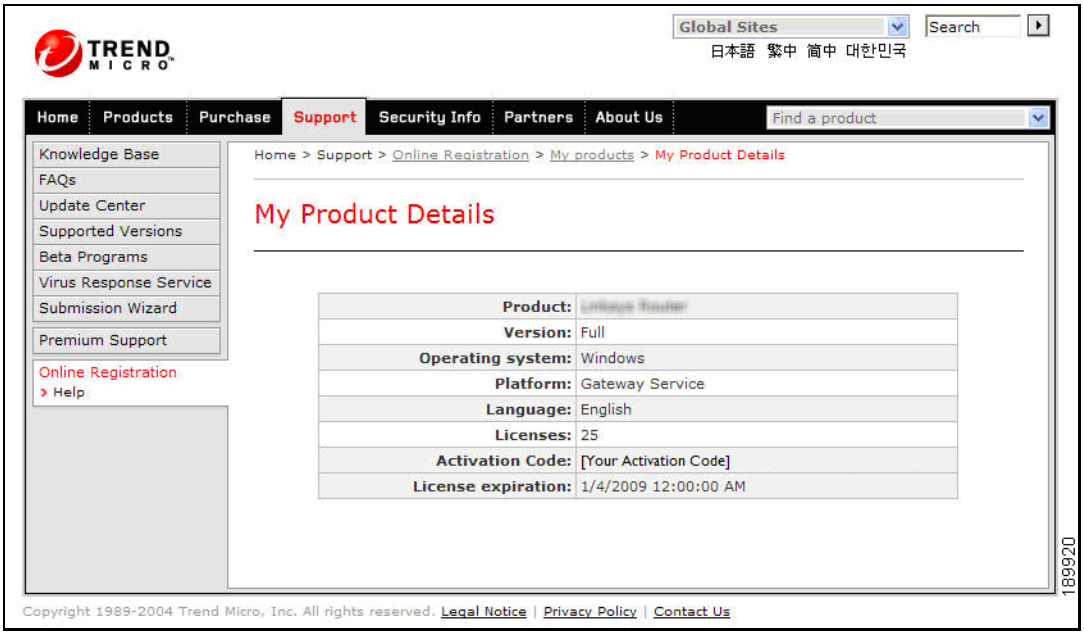
L'icône d'état et le message vous renseignent sur l'état de la licence.

Icône	Message
	Le service Cisco ProtectLink est actif.
	Le service Cisco ProtectLink Service expirera dans 30 jours.
	Le service Cisco ProtectLink a expiré.

ÉTAPE 3 Cliquez sur **Update Information** pour mettre à jour les informations concernant la licence. Les informations de licence sont mises à jour et une date indiquant quand elles ont été mises à jour pour la dernière fois est ajoutée.

ÉTAPE 4 Cliquez sur le lien **View detailed license online** pour afficher plus de détails à propos de la licence du produit.

La page My Product Details s'affiche.



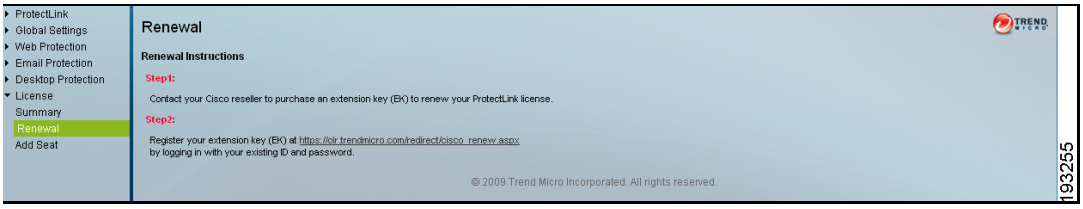
Renouveler une licence

REMARQUE Vous devez acheter une clé d'extension (EK, Extension Key) à votre revendeur Cisco.

Pour renouveler une licence, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **License > Renewal**.

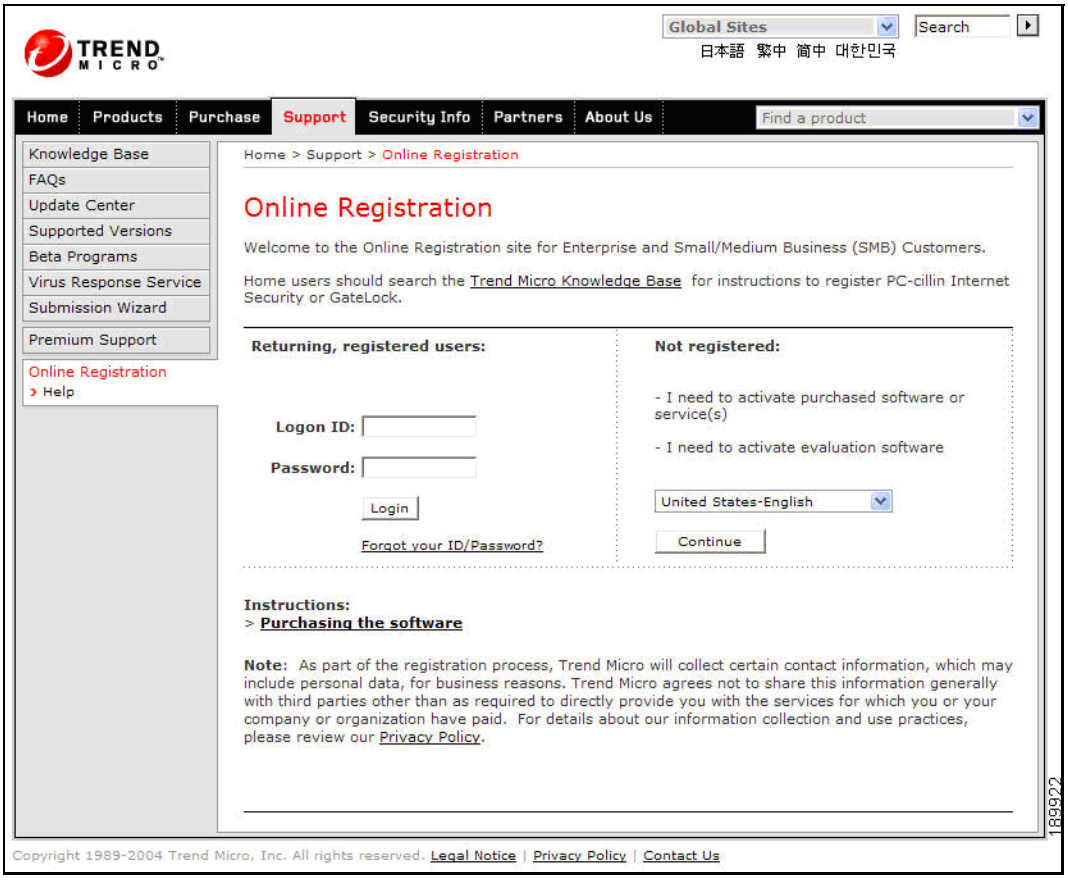


ÉTAPE 3 Suivez les instructions indiquées sur la page :

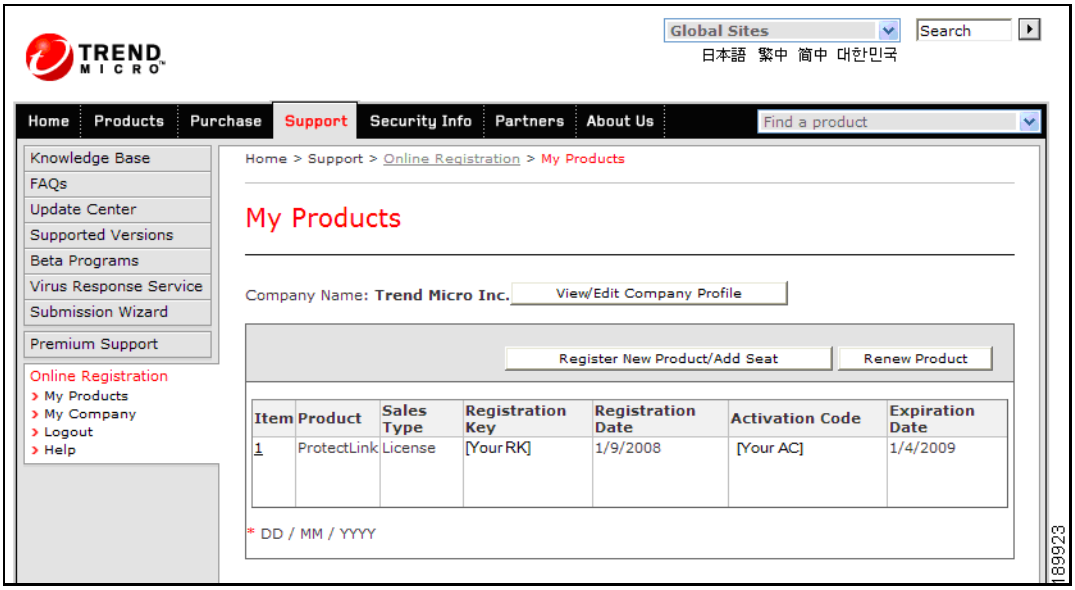
a. Contactez votre revendeur Cisco pour acheter une clé d'extension (EK) afin de renouveler la licence ProtectLink.

b. Cliquez sur le lien Cisco pour lancer le portail web de Cisco et enregistrer votre clé d'extension.

La page Cisco Online Registration s'affiche.

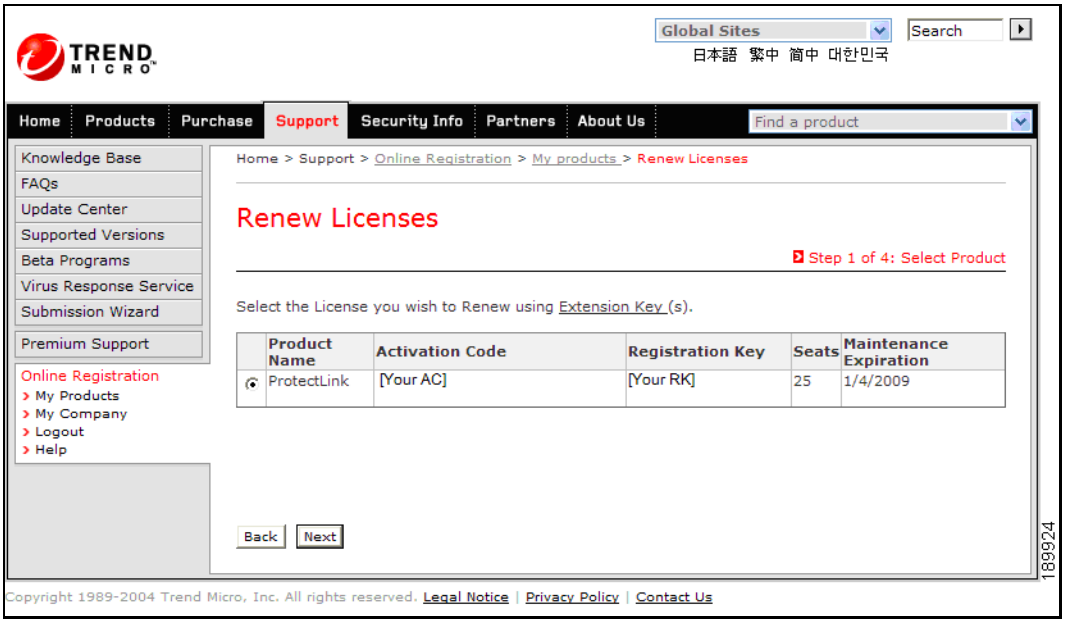


ÉTAPE 4 Saisissez votre identifiant et votre mot de passe de connexion ProtectLink, puis cliquez sur **Login**.



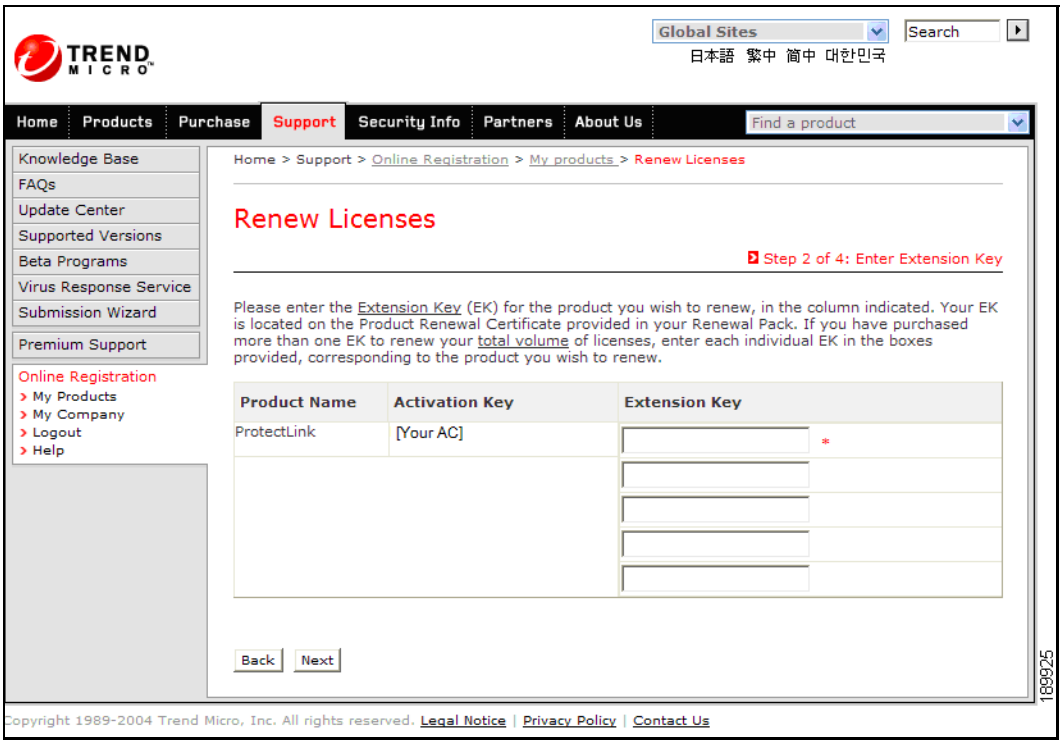
ÉTAPE 5 Cliquez sur **Renew Product**.

La page Renew Licenses > Step 1 of 4: Select Product s'affiche.



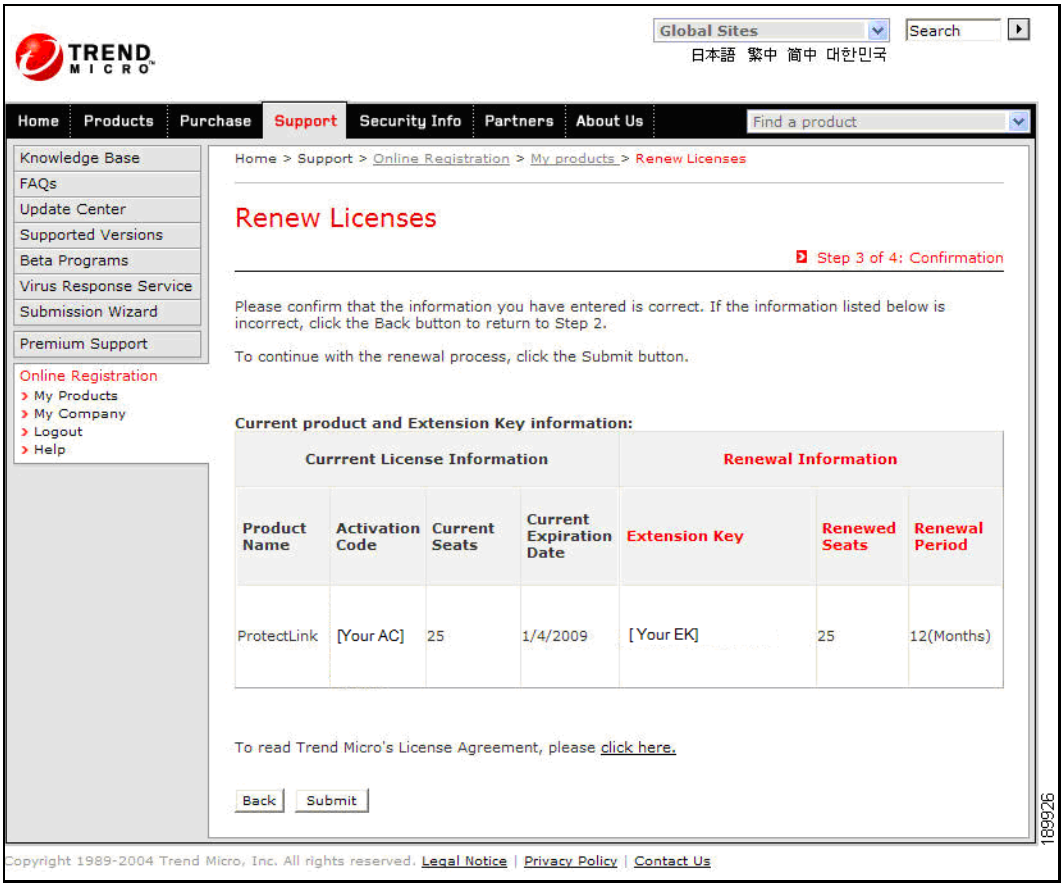
ÉTAPE 6 Sélectionnez la licence à renouveler, puis cliquez sur **Next**.

La page Renew Licenses > Step 2 of 4: Enter Extension Key s'affiche.



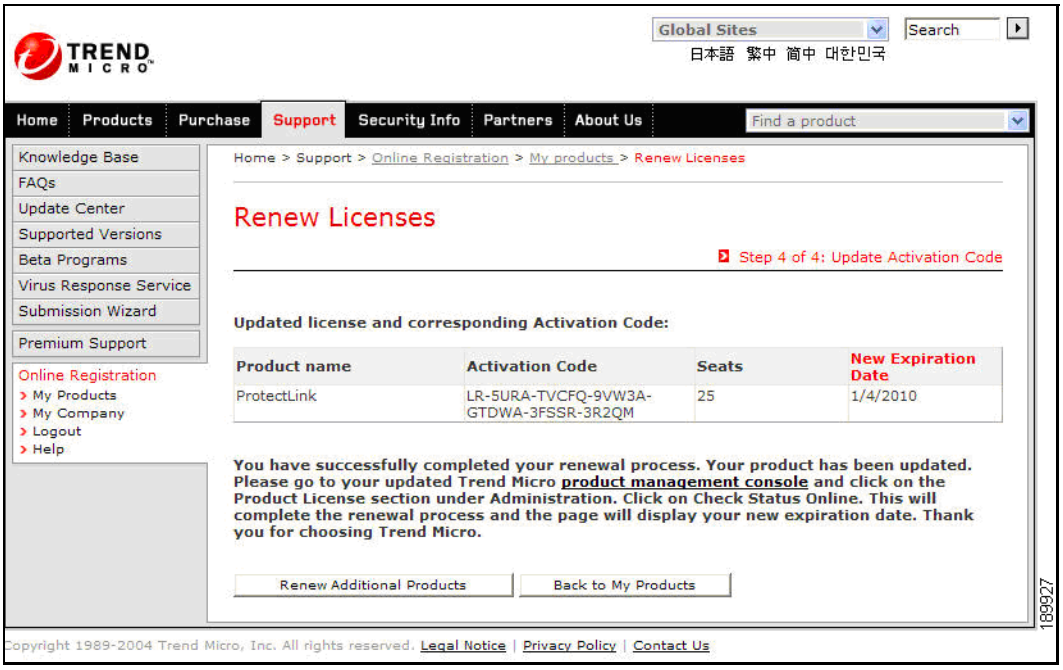
ÉTAPE 7 Saisissez la **clé d'extension** du produit que vous souhaitez renouveler (ProtectLink), puis cliquez sur **Next**.

La page Renew Licenses > Step 3 of 4: Confirmation s'affiche.



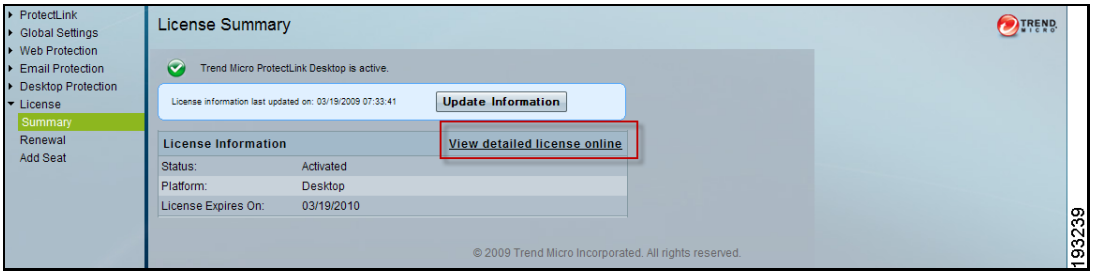
ÉTAPE 8 Vérifiez les informations sur le produit actuel et la clé d'extension, puis cliquez sur **Submit**.

La page Renew Licenses > Step 4 of 4: Update Activation Code s'affiche et vous indique que vous avez renouvelé la licence avec succès.



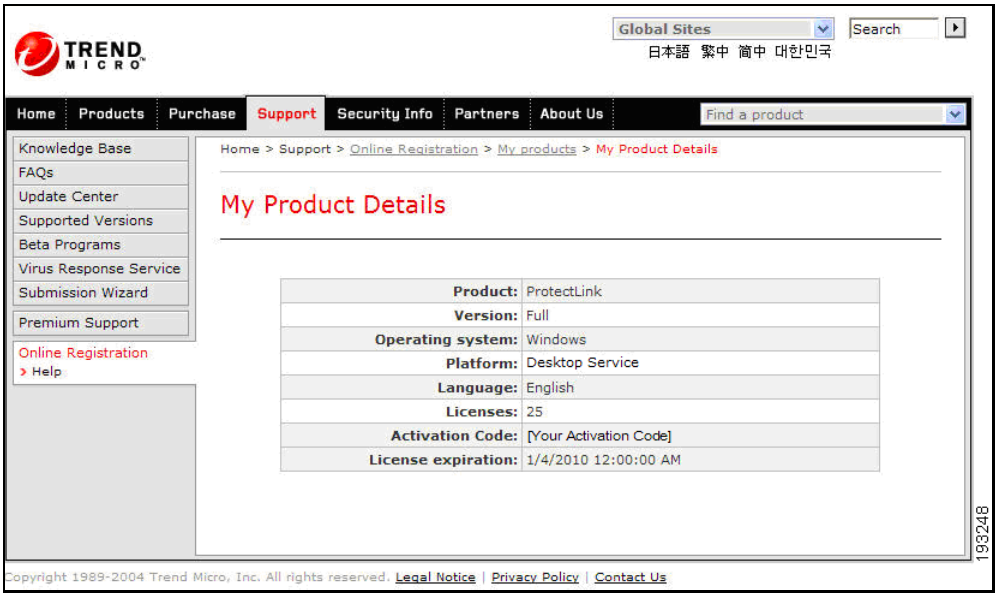
ÉTAPE 9 Pour terminer le processus de renouvellement, retournez à l'utilitaire de configuration du périphérique de sécurité.

ÉTAPE 10 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **License > Summary**.



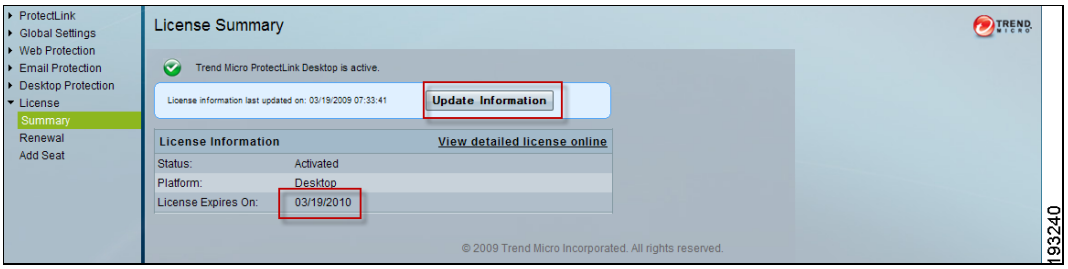
ÉTAPE 11 Cliquez sur **View detailed license online**.

La page My Product Details s'affiche. Vous pouvez y consulter les détails du produit ProtectLink et la date d'expiration de la nouvelle licence.



ÉTAPE 12 Retournez à l'utilitaire de configuration du périphérique de sécurité.

ÉTAPE 13 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **License > Summary**.



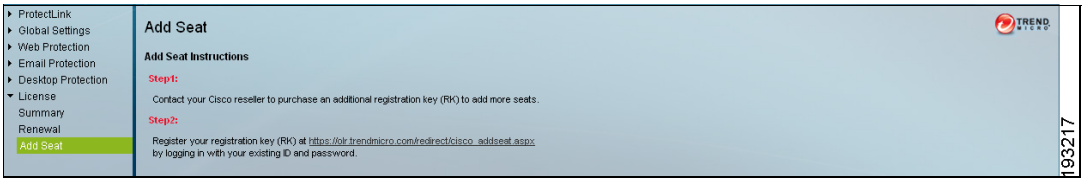
ÉTAPE 14 Cliquez sur **Update Information**. Les informations concernant la licence sont à jour et vous indiquent la nouvelle date d'expiration de ProtectLink.

Ajouter des postes

Lorsque vous achetez des services ProtectLink, vous pouvez choisir entre les options 5 postes et 25 postes. Pour ajouter des postes à la licence, et permettre ainsi la protection de nouveaux ordinateurs, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

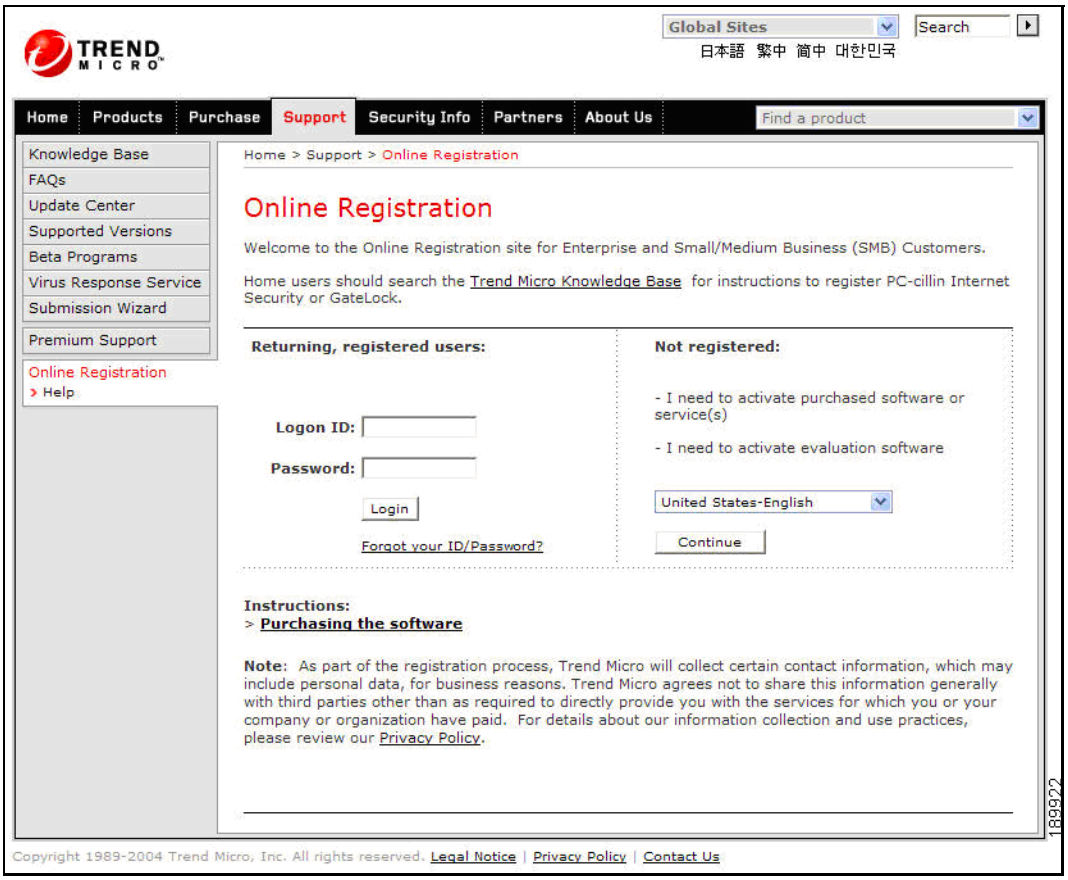
ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink,** puis sur **License > Add Seat**.



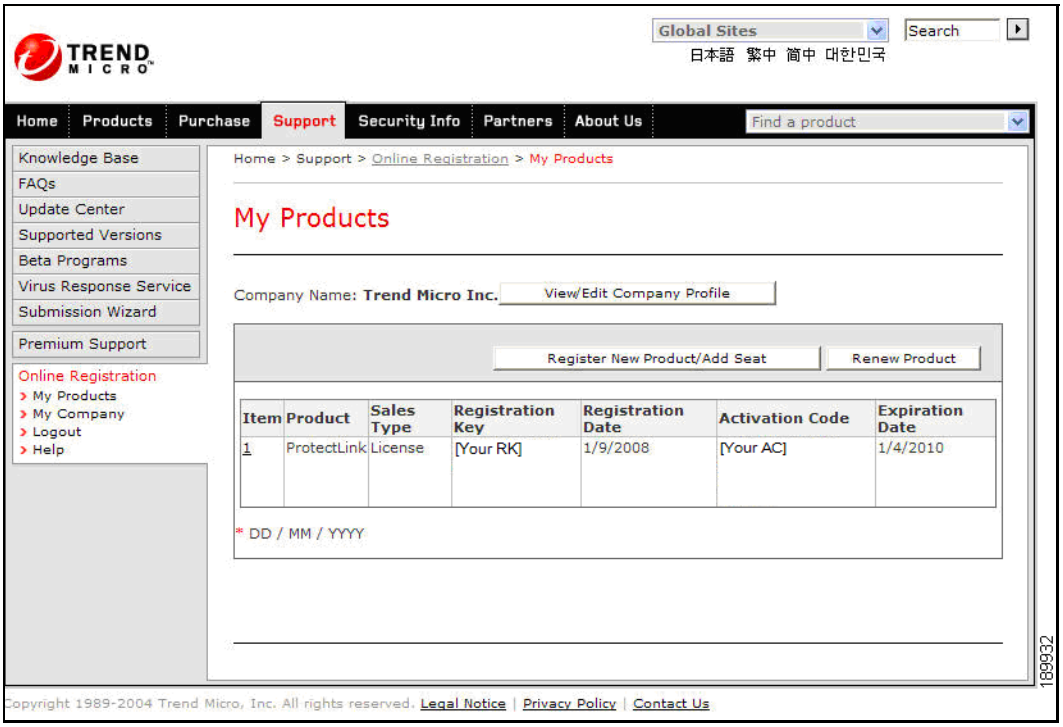
ÉTAPE 3 Pour poursuivre, suivez les instructions indiquées sur la page :

a. Contactez votre revendeur Cisco pour acheter une clé d'enregistrement supplémentaire (RK, registration key) afin d'ajouter des postes.

b. Cliquez sur le lien pour vous connecter au portail web et enregistrer le produit.

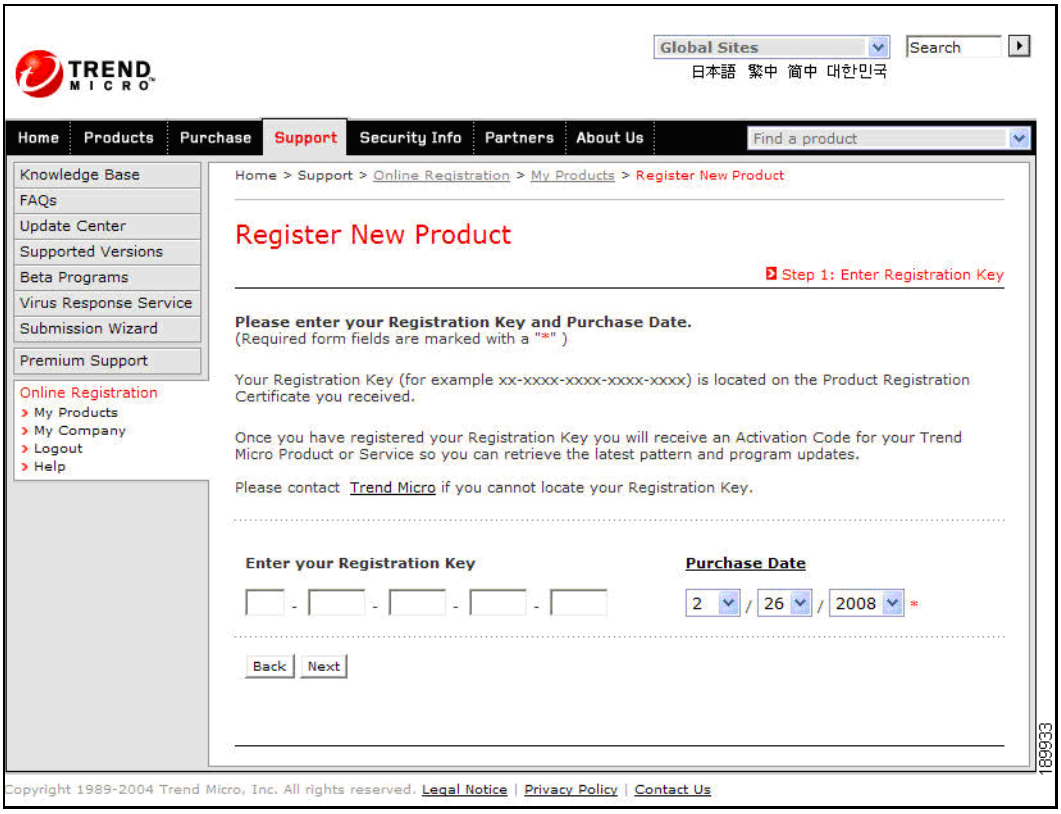


ÉTAPE 4 Saisissez votre identifiant et votre mot de passe de connexion, puis cliquez sur **Login**.



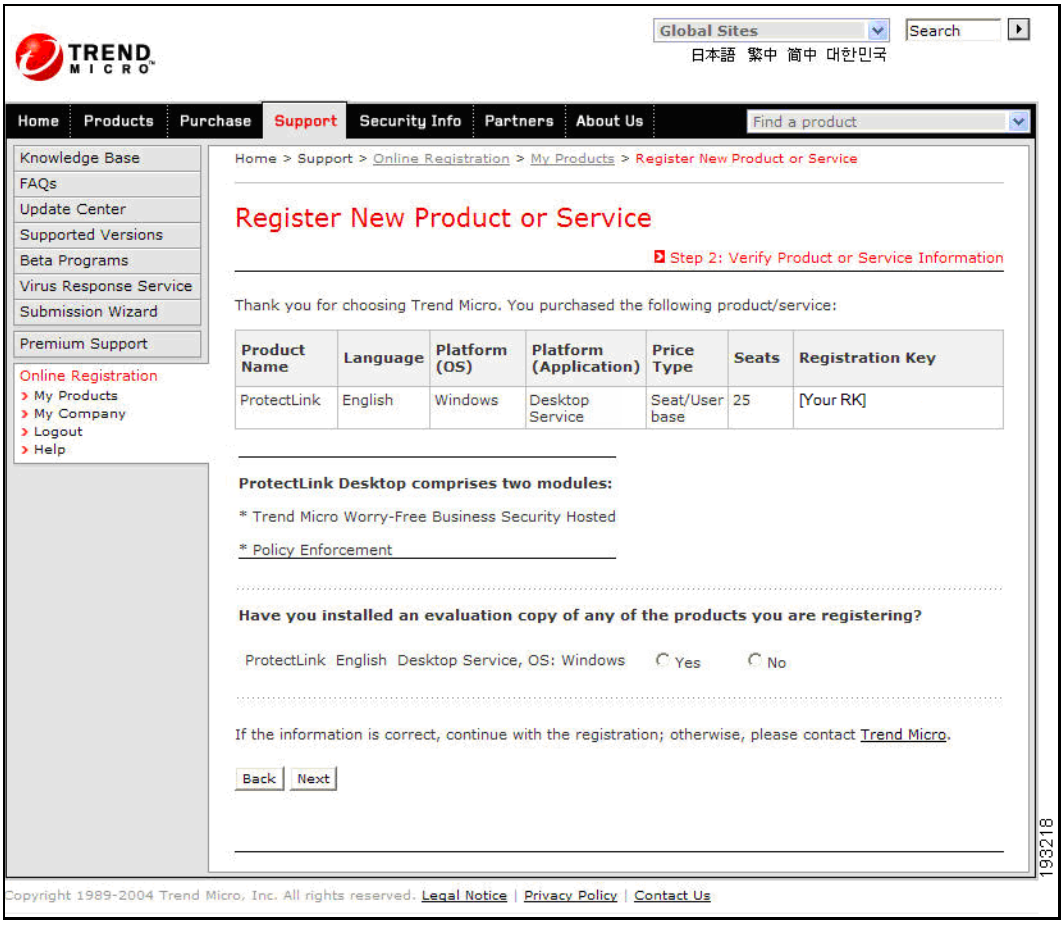
ÉTAPE 5 Cliquez sur le bouton **Register New Product/Add Seat** situé au-dessus du tableau.

La page Register New Product > Step 1: Enter Registration Key s'affiche.



ÉTAPE 6 Saisissez la **clé d'enregistrement** et la **date d'achat**, puis cliquez sur **Next**.

La page Register New Product > Step 2: Verify Product or Service Information s'affiche et indique les nouveaux postes dans le tableau d'enregistrement.

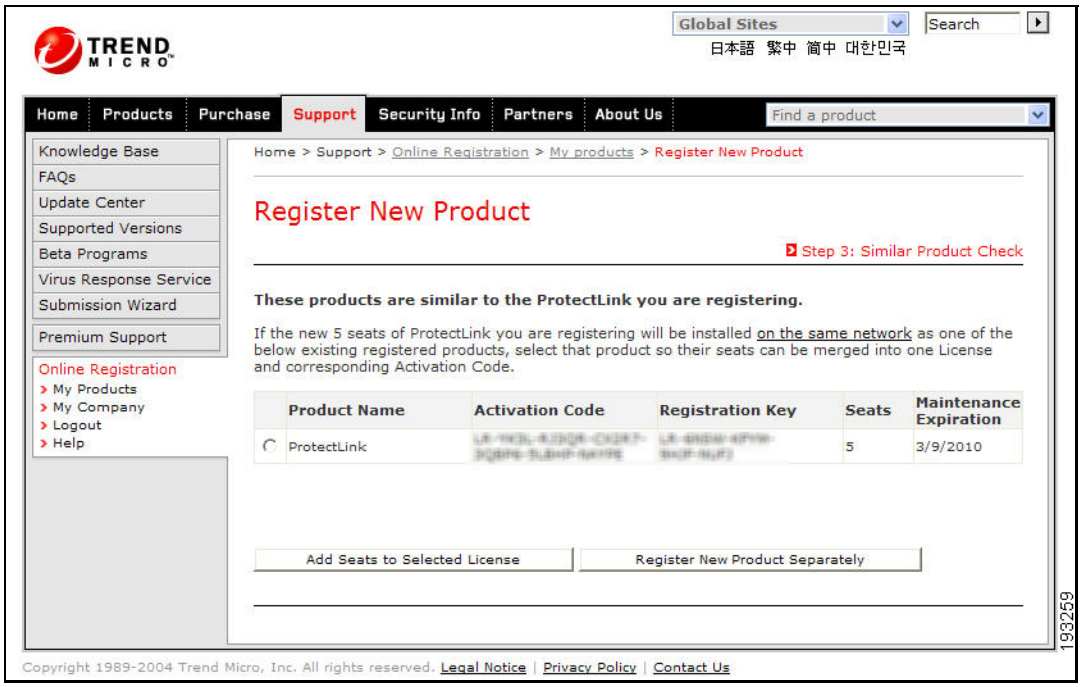


ÉTAPE 7 Vérifiez les informations sur le produit ou service.

ÉTAPE 8 Cliquez sur **Yes** ou sur **No** pour répondre à la question : Have you installed an evaluation copy of any of the products you are registering?

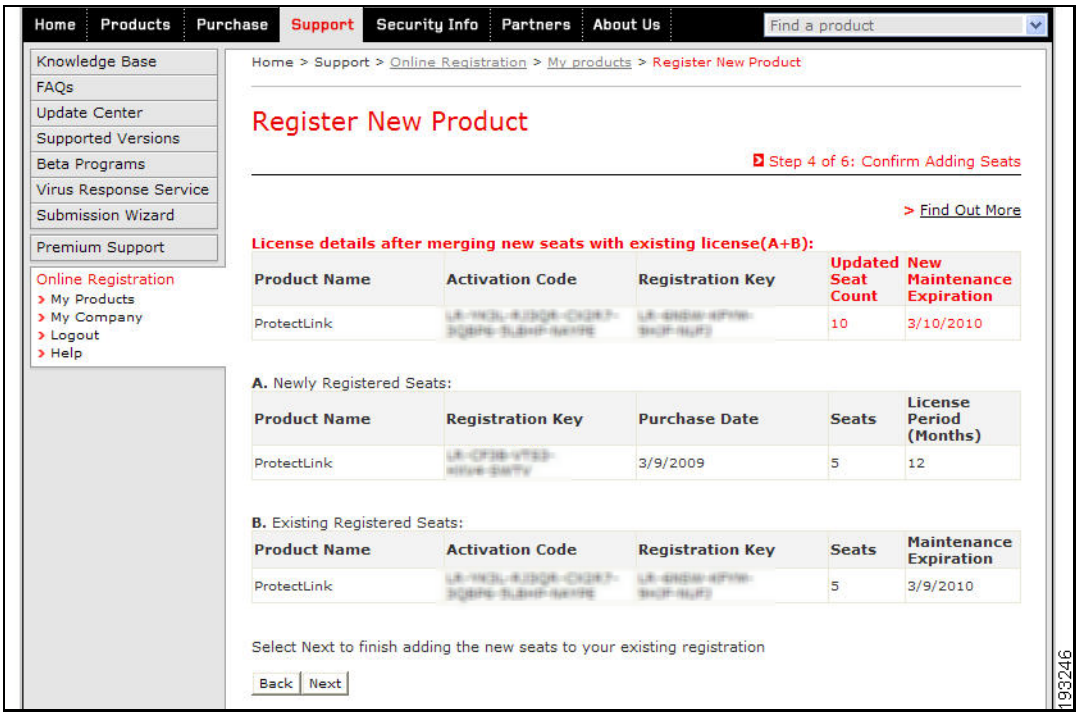
ÉTAPE 9 Si les informations sont correctes, cliquez sur **Next**.

La page Register New Product > Step 3: Similar Product Check s'affiche.



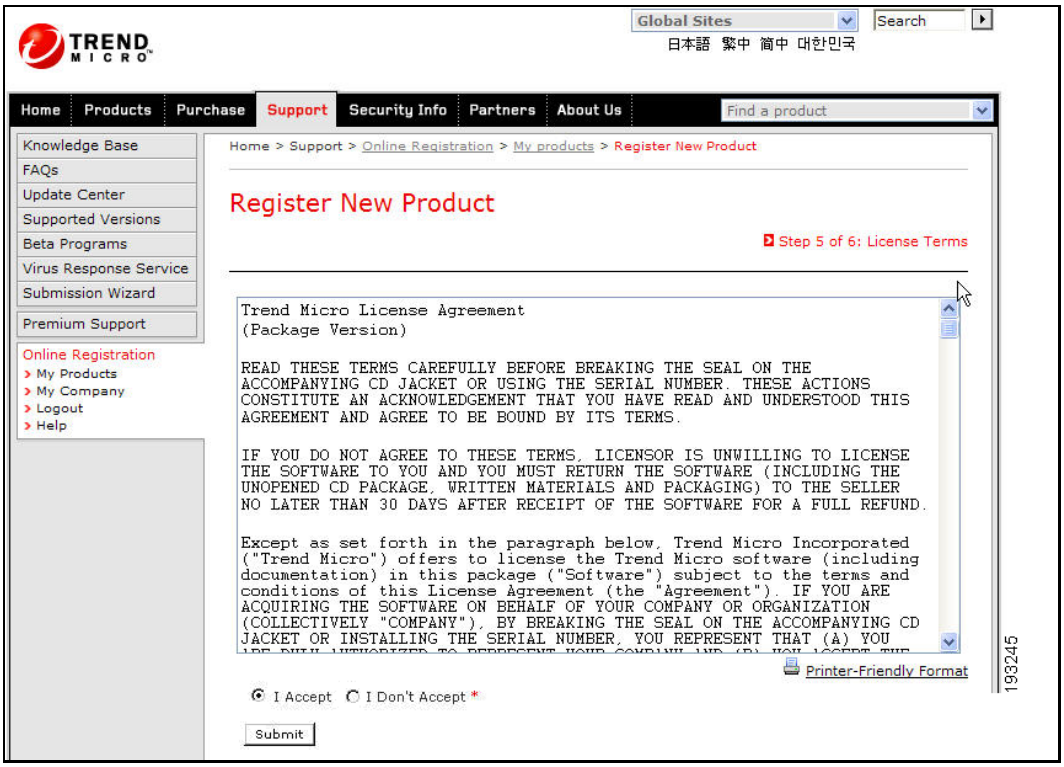
ÉTAPE 10 Sélectionnez la licence requise, puis cliquez sur **Add Seats to Selected License**.

La page Register New Product > Step 4 of 6: Confirm Adding Seats s'affiche.



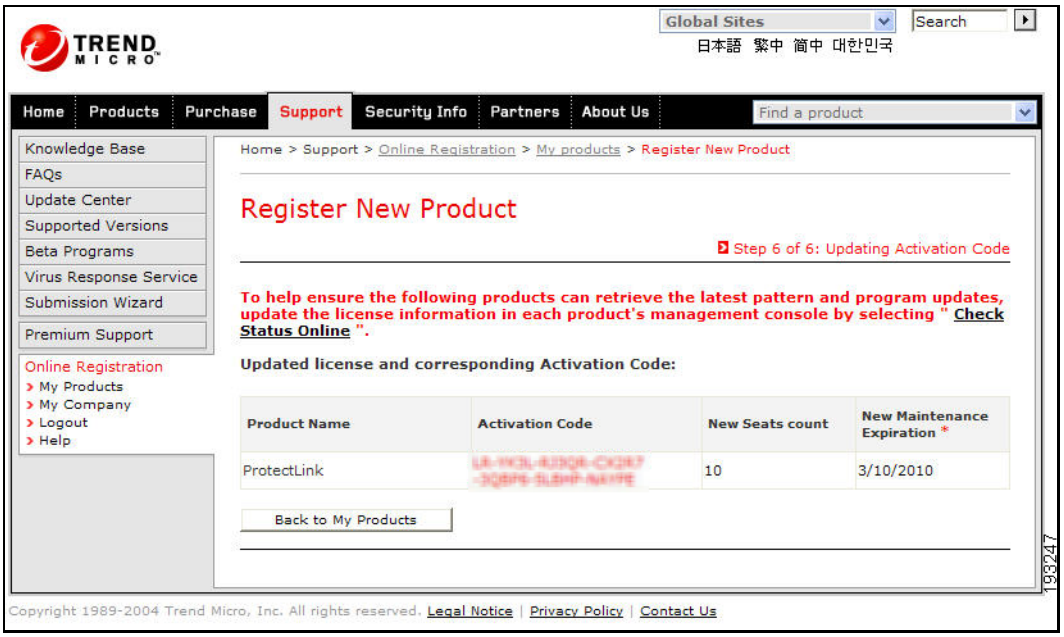
ÉTAPE 11 Cliquez sur **Next** pour confirmer les changements surlignés en rouge.

La page Register New Product > Step 4 of 6: License Terms s'affiche.



ÉTAPE 12 Cliquez sur **I Accept**, puis sur **Submit**.

La page Register New Product > Step 6 of 6: Updating Activation Code s'affiche.



ÉTAPE 13 Une fois ces étapes terminées, votre compte ProtectLink Endpoint est mis à jour et prêt à protéger de nouveaux postes.

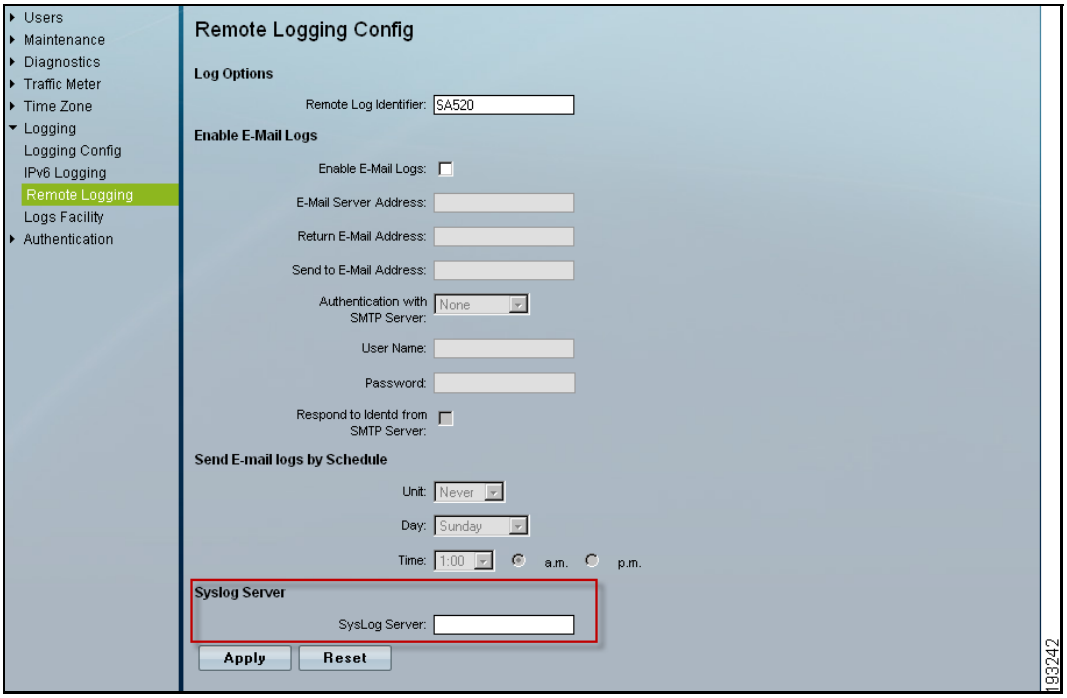
Activer le journal système > Journal des événements de blocage d'appels sortants

ProtectLink Endpoint peut fournir un journal système (Syslog) ainsi qu'un journal des événements de blocage d'appels sortants pour tous les événements bloqués. Activez ces fonctionnalités pour mettre à jour les journaux.

Pour activer le journal système et le journal des événements de blocage d'appels sortants, procédez comme suit :

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **Administration**, puis sur le lien **Logging > Remote Logging**.



ÉTAPE 3 Dans la section **Syslog Server** saisissez **le nom ou l'adresse IP** du serveur Syslog.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 5 Une fois que vous avez les données du journal, cliquez sur **View Log** pour afficher les journaux.

La page Log s'affiche. Vous pouvez y consulter les journaux All, System, Access, Firewall et VPN page par page.

4

Utilisation du portail Web pour l'administration

Utilisez le portail Web pour les tâches administratives suivantes :

Lancement du portail Web

Vous pouvez lancer le portail Web à partir de l'utilitaire de configuration du périphérique de sécurité. Le portail Web offre un accès aux récapitulatifs, aux paquets, aux rapports et aux fonctions d'administration de WFBS-H.

ÉTAPE 1 Lancez l'utilitaire de configuration du périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Dans la barre de menus, cliquez sur **ProtectLink**, puis sur **Web Protection > Desktop Protection** dans l'arborescence de navigation.

ÉTAPE 3 Sur la page ProtectLink Endpoint, cliquez sur le lien WFBS-H pour accéder à l'adresse URL suivante :

https://wfbs-h.trendmicro.com/wfbsh/protectlinklogin.aspx

ÉTAPE 4 Lorsque la page de connexion du portail Web WFBS-H s'affiche, saisissez l'identifiant de connexion et le mot de passe, puis cliquez sur **Log on**.

Vous pouvez désormais commencer à utiliser le portail Web.

Utilisation des récapitulatifs

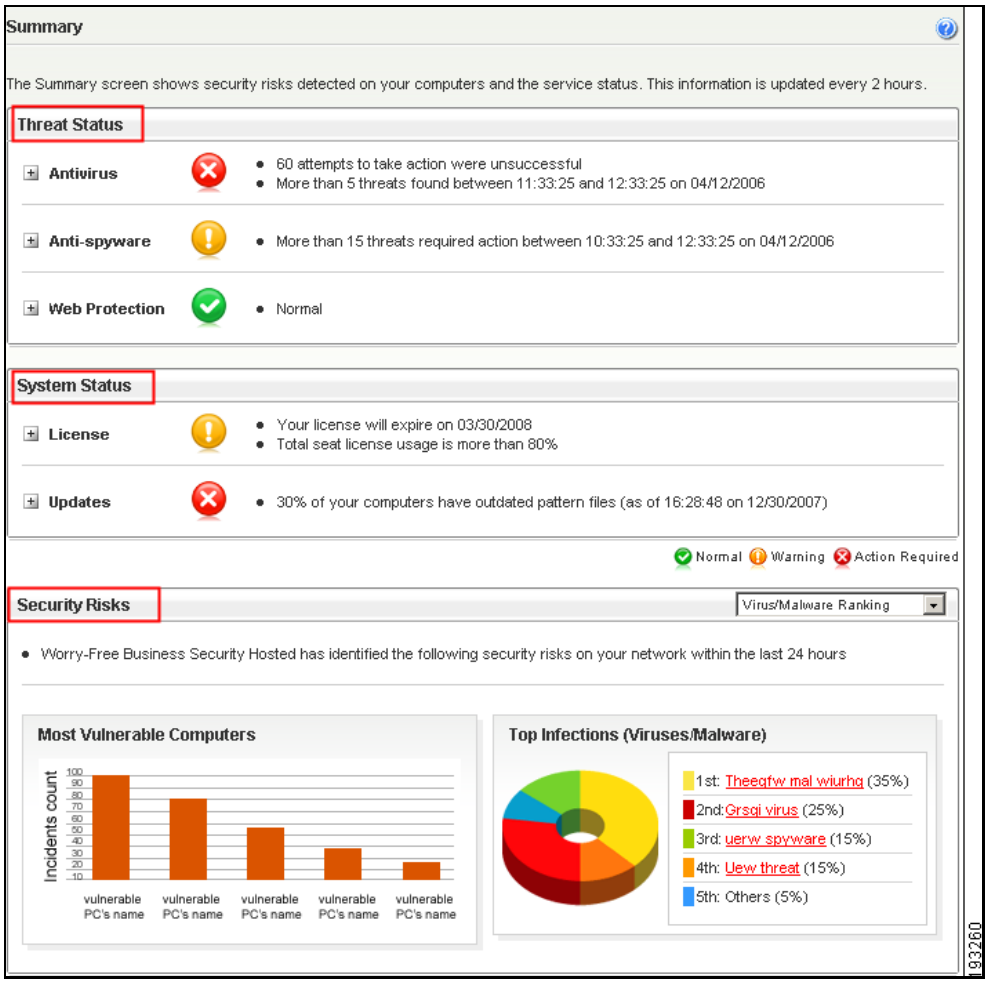
Ouvrez la page Summary pour afficher les risques de sécurité détectés sur les ordinateurs et l'état du service.

Pour ouvrir la page Summaries :

ÉTAPE 1 Lancez le portail Web WFBS-H.

REMARQUE Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Summary**.



REMARQUE WFBS-H met à jour les informations récapitulatives toutes les deux heures.

ÉTAPE 3 Cliquez sur les boutons et les liens de la page pour consulter davantage d'informations.

Reportez-vous aux rubriques suivantes pour obtenir davantage de détails :

- **Icônes de notification, page 57**
- **État de la menace, page 58**
- **État du système, page 59**
- **Risques pour la sécurité, page 60**

Icônes de notification

Les icônes de notification de la page Summary indiquent l'état du service Worry-Free Business Security Hosted de l'ordinateur et vous avertissent lorsqu'un virus ou un logiciel espion est détecté.

Le tableau suivant décrit l'état des icônes de notification.

Tableau 1 Icônes de notification

Icône	Description état
	**Normal** : aucune action requise.
	**Warning :** en général, une icône de mise en garde signifie qu'il existe de nombreux ordinateurs vulnérables ayant rapporté un trop grand nombre d'incidents liés à des virus, des logiciels malveillants ou des logiciels espions.
	**Action Required :** prenez des mesures pour éviter des risques supplémentaires sur le réseau.

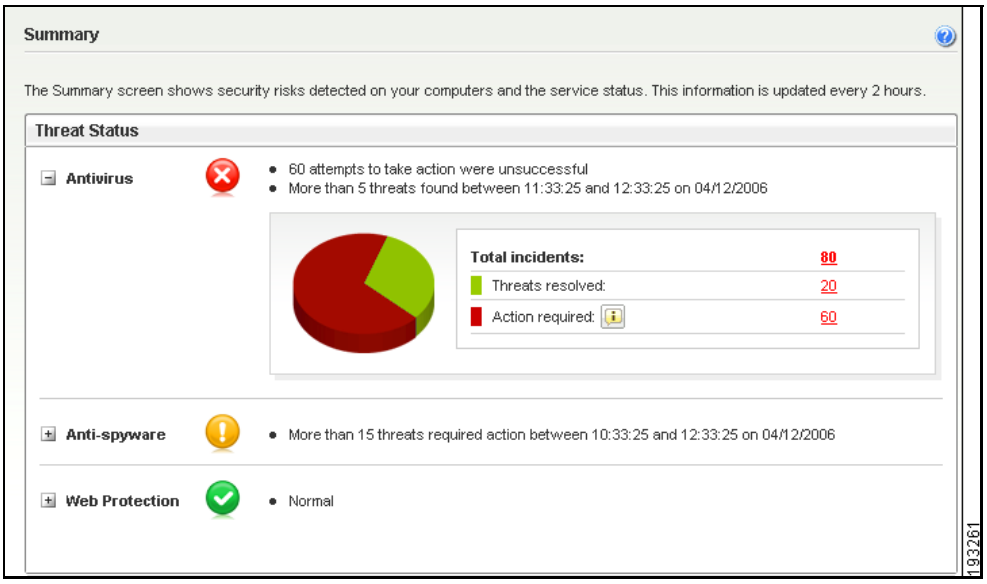
État de la menace

La section Threat Status de la page Summary fournit le nombre total d'incidents trouvés sur le réseau, le nombre de menaces supprimées ainsi que le nombre de menaces qui nécessitent une action. Cette section comprend les sous-sections suivantes :

- Antivirus
- Anti-spyware
- Web Protection

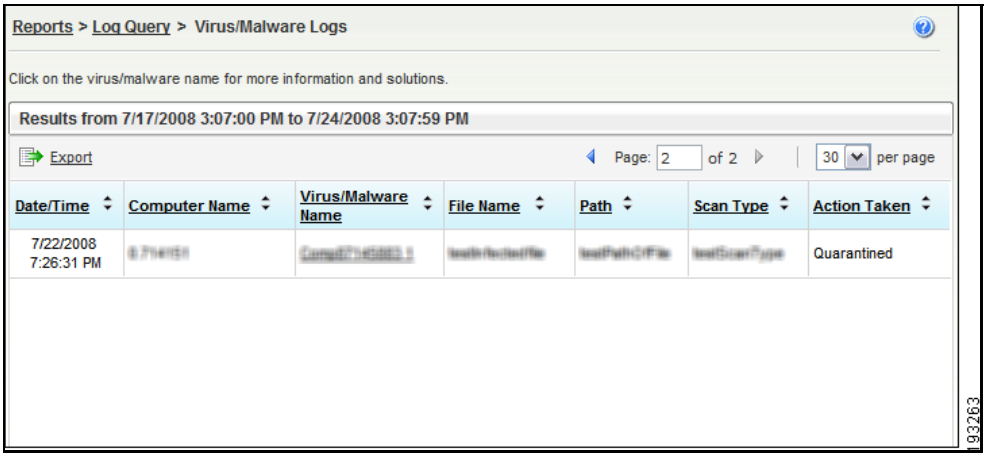
Pour consulter les détails concernant un type de menace particulier, cliquez sur ⊞ situé à côté du sous-titre. La **Figure 1** montre un exemple des informations affichées.

Figure 1 État des menaces pour la section Antivirus



Pour consulter les informations détaillées, notamment le nom de l'ordinateur et le nombre de menaces trouvées, cliquez sur le nombre d'incidents. La **Figure 2** montre un exemple des informations affichées.

Figure 2 Page Detailed Virus/Malware Status



Le journal généré comporte des informations relatives aux noms des virus, des programmes malveillants ou des logiciels espions trouvés dans l'intervalle de temps indiqué et les mesures prises. Cliquez sur le nom du virus, du programme malveillant ou du logiciel espion pour obtenir davantage d'informations et de solutions.

État du système

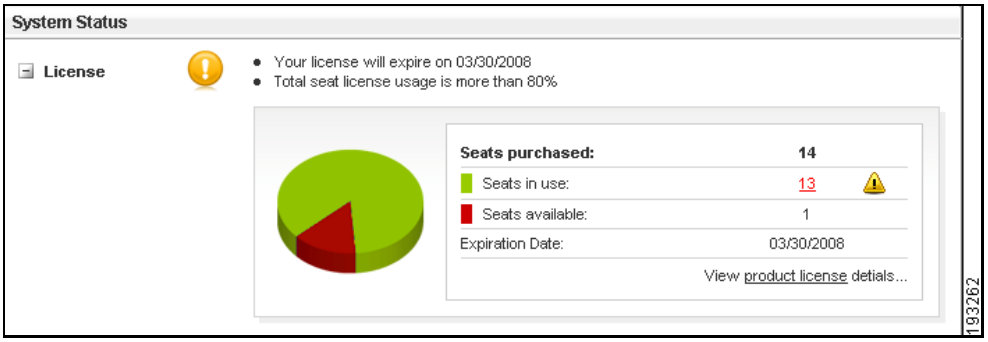
Dans la section System Status de la page Summary, vous pouvez consulter l'état de la licence et des mises à jour de fichiers.

- **Licenses** : cette section comporte des informations relatives au nombre de postes achetés, utilisés et disponibles. Elle fournit également des informations sur la date d'expiration de la licence.
- **Updates** : le récapitulatif des mises à jour fournit les mises à jour pour les ordinateurs obsolètes du réseau.

  REMARQUE Les ordinateurs obsolètes sont des ordinateurs n'ayant pas bénéficié des dernières mises à jour des types de virus à partir de WFBS-H.

Pour afficher les informations sur la licence, cliquez sur ⊞ situé à côté du sous-titre **License**. Une représentation graphique détaillée s'affiche avec des informations relatives au nombre de postes achetés, utilisés et disponibles, ainsi qu'à la date d'expiration. La **Figure 3** montre un exemple des informations affichées.

Figure 3 Option License dans la section System Status



Vous pouvez effectuer les tâches suivantes :

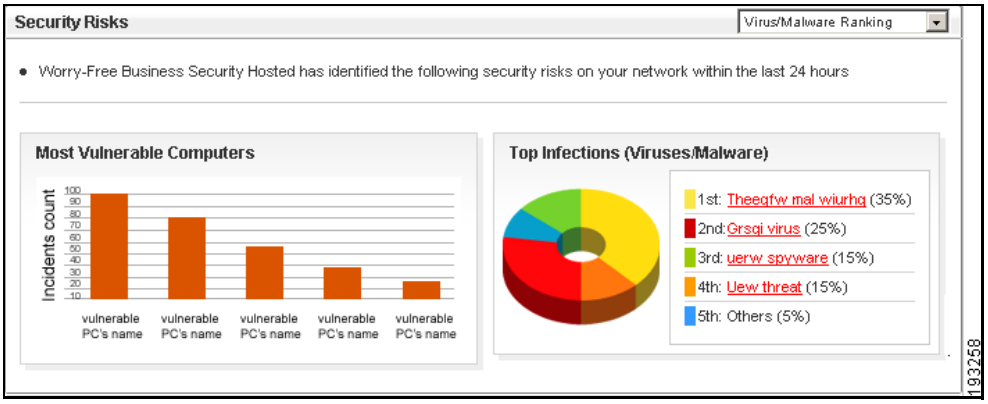
- Cliquez sur le nombre de postes souligné pour afficher les détails relatifs au nom de chaque ordinateur et à la version du logiciel WFBS-H Agent installé.
- Cliquez sur le lien **product license** pour consulter les détails relatifs à la licence.

Risques pour la sécurité

La section Security Risks de la page Summary affiche les niveaux de risques pour la sécurité découverts sur le réseau. Elle affiche une liste des infections les plus courantes, qui peut comprendre des virus ou des programmes malveillants, des logiciels espions ou des adresses URL malveillantes. Cette section comprend également une représentation graphique des ordinateurs les plus vulnérables du réseau. Vous pouvez contrôler l'affichage en sélectionnant l'une des options dans la liste déroulante de l'en-tête de la section :

- Virus/Malware Ranking
- Spyware/Grayware Ranking
- Malicious URLs Ranking

Figure 4 Section Security Risks



Utilisation des paquets

Les paquets sont des programmes qui installent les agents sur les ordinateurs clients. Utilisez WFBS-H pour créer, configurer et télécharger des paquets sur les ordinateurs du réseau.

REMARQUE Une fois que vous avez installé un paquet, il faut environ une heure avant que les agents commencent à envoyer des rapports à WFBS-H.

Reportez-vous aux rubriques suivantes :

- **Création de nouveaux paquets, page 62**
- **Téléchargement de paquets existants, page 64**
- **Suppression de paquets existants, page 64**

ATTENTION Les utilisateurs peuvent désinstaller l'agent sans mot de passe.

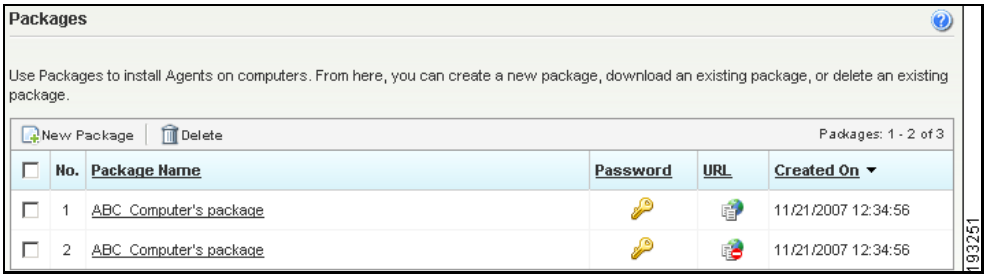
Création de nouveaux paquets

Vous pouvez créer de nouveaux paquets pour stocker des paramètres de connexion différents. Pour créer un nouveau paquet :

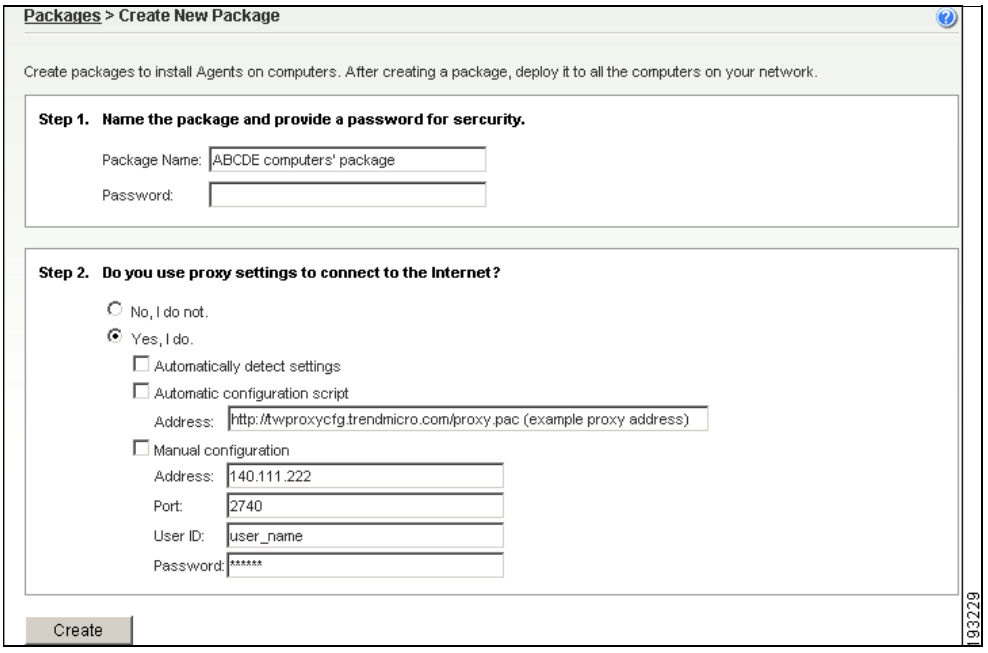
ÉTAPE 1 Lancez le portail Web WFBS-H.

> **REMARQUE** Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Packages**.



ÉTAPE 3 Cliquez sur le bouton **New Package** situé au-dessus du tableau.



ÉTAPE 4 Saisissez les informations suivantes :

- **Package Name** : saisissez un nom de paquet.
- **Password** : saisissez un mot de passe à utiliser lors de l'extraction du paquet.

- **Do you use proxy settings to connect to the Internet?** :
  - Si vous n'utilisez pas de paramètres proxy, cliquez sur **No, I do not**.
  - Si vous utilisez des paramètres proxy, cliquez sur **Yes, I do**. Les options de configuration s'affichent.
- Si vous utilisez des paramètres proxy, sélectionnez les paramètres proxy requis pour que les agents puissent communiquer avec le serveur WFBS-H :
  - **Automatically detect settings :** le programme d'installation de l'agent détecte automatiquement les paramètres requis pour l'installation du paquet.
  - **Automatic configuration script :** WFBS-H met à jour l'emplacement du script de configuration dans le champ Address. Il utilise le script de configuration à partir de cette adresse URL pour installer le paquet.
  - **Manual configuration** : WFBS-H met à jour la configuration proxy suivante dans le champ Manual configuration.
- Si vous optez pour la configuration manuelle, saisissez les informations suivantes :
  - **Server IP Address** : saisissez l'adresse IP du serveur proxy. Vous pouvez obtenir l'adresse IP du serveur proxy à partir des paramètres d'Internet Explorer.
  - **Port** : saisissez le numéro de port utilisé par le serveur proxy pour la connexion des clients.
  - **User ID** : saisissez le nom du compte utilisé par l'ordinateur client pour se connecter au serveur proxy.
  - **Password :** saisissez le mot de passe correspondant à l'identifiant utilisateur.

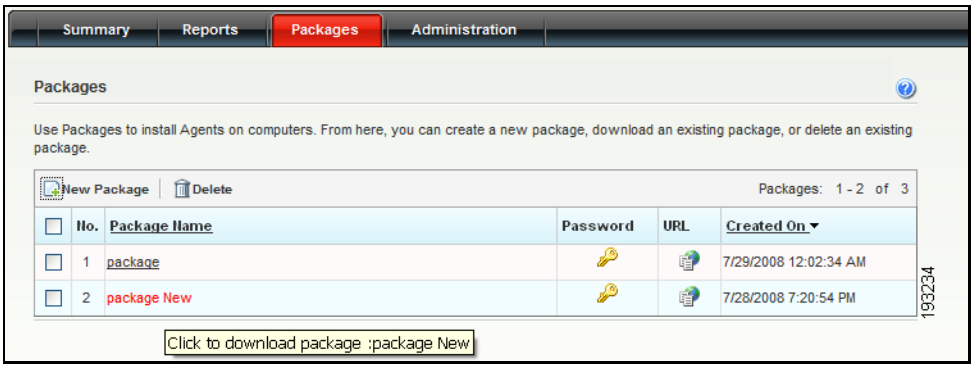
ÉTAPE 5 Cliquez sur **Create**.

Un lien pour le nouveau paquet avec le nom indiqué est créé. Cliquez sur le lien du nom du paquet pour le télécharger.

Téléchargement de paquets existants

Après la création d'un paquet, suivez ces étapes pour télécharger ces paquets sur les ordinateurs que vous souhaitez protéger :

ÉTAPE 1 Lancez le portail Web, puis cliquez sur l'onglet **Packages** pour consulter cette page.



ÉTAPE 2 Recherchez le paquet que vous souhaitez télécharger, puis cliquez sur le lien dans la colonne Package Name.

La boîte de dialogue **File Download** s'affiche.

ÉTAPE 3 Cliquez sur **Save** pour enregistrer le paquet sur votre ordinateur.

ÉTAPE 4 Installez ces paquets sur les ordinateurs que vous souhaitez protéger.

> **REMARQUE** Pour les ordinateurs sous Windows Vista, installez le paquet avec les droits administrateurs (à l'aide de l'option **Exécuter en tant qu'administrateur**).

Suppression de paquets existants

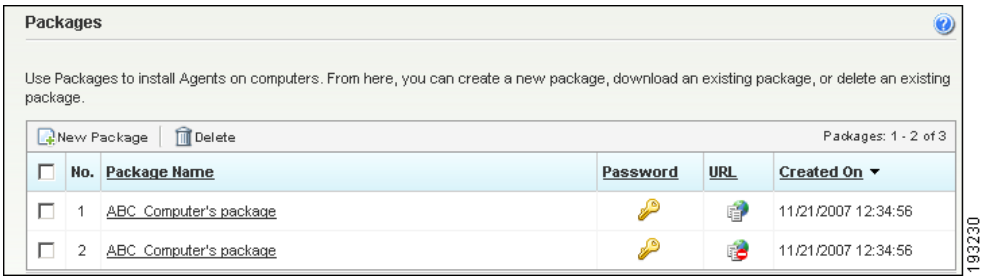
Suivez ces étapes pour supprimer un paquet existant :

ÉTAPE 1 Lancez le portail Web WFBS-H.

> **REMARQUE** Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Packages**.

ÉTAPE 3 Cochez la case de chacun des paquets que vous souhaitez supprimer. Pour sélectionner tous les paquets, cochez la case située en haut de la première colonne.



ÉTAPE 4 Cliquez sur le bouton **Delete** situé au-dessus du tableau.

Utilisation des rapports

Worry-Free Business Security Hosted vous permet de créer et d'afficher des rapports qui contiennent des informations détaillées relatives aux menaces détectées. Les rapports comprennent également un classement permettant d'identifier les ordinateurs les plus vulnérables. WFBS-H génère les rapports sous la forme d'un fichier PDF.

Vous pouvez générer une requête de journal depuis la page Reports. Une requête de journal affiche les informations relatives aux virus ou aux programmes malveillants, aux logiciels espions ou aux URL malveillantes détectés sur le réseau pendant la période indiquée. Elle fournit également des informations détaillées sur le nom des ordinateurs, des menaces et des fichiers concernés. Elle répertorie également le type d'analyse et la mesure prise pour cette menace.

Reportez-vous aux rubriques suivantes :

- **Création de rapports, page 66**
- **Suppression de rapports existants, page 69**
- **Génération d'une requête de journal, page 69**

Création de rapports

Vous pouvez créer un rapport pour des fichiers et des données collectés au cours des 90 derniers jours.

REMARQUE WFBS-H stocke les fichiers et les données pendant 90 jours au maximum.

Vous pouvez créer des rapports pour une période ou un fuseau horaire spécifique selon vos besoins. Les rapports contiennent les informations suivantes :

Heure, date et fuseau horaire pour lesquels le rapport est généré.

- **Virus/Malware Summary** :
  - Les activités, le nombre d'incidents et le pourcentage de virus ou programmes malveillants ;
  - Les classements des virus ou programmes malveillants en fonction du nombre et du pourcentage d'incidents ;
  - Une représentation graphique des activités.
- Most Vulnerable Computers to Virus/Malware Infection :
  - Une représentation graphique du nombre de virus ou programmes malveillants pour chaque ordinateur ;
  - Des classements en fonction du nombre et le pourcentage d'incidents.
- **Spyware/Grayware Summary** :
  - Les activités, le nombre d'incidents et le pourcentage de logiciels espions ;
  - Les classements des logiciels espions en fonction du nombre et du pourcentage d'incidents ;
  - Une représentation graphique des activités.
- **Most Vulnerable Computers to Spyware/Grayware** :
  - Une représentation graphique du nombre de logiciels espions pour chaque ordinateur ;
  - Les classements des ordinateurs en fonction du nombre et du pourcentage d'incidents.

- **Malicious URL Summary** : classe les adresses URL malveillantes en fonction du nombre d'incidents et du pourcentage.
- **Top Computers Accessing Malicious URLs** :
  - Les classements des ordinateurs en fonction du nombre d'adresses URL malveillantes ouvertes ;
  - Une représentation graphique du nombre d'adresses URL pour chaque ordinateur.

Suivez ces étapes pour créer un nouveau rapport :

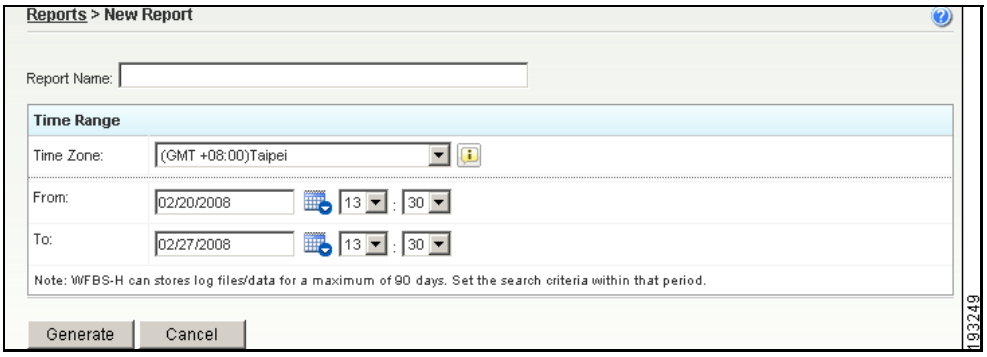
ÉTAPE 1 Lancez le portail Web WFBS-H.

REMARQUE Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Reports**.

La page Reports s'affiche.

ÉTAPE 3 Cliquez sur le bouton **New report** situé au-dessus du tableau.



ÉTAPE 4 Saisissez les informations suivantes :

- **Report Name :** saisissez un nom descriptif pour ce rapport ;
- **Time Range** : choisissez le fuseau horaire, les dates et les heures pour le contenu que vous souhaitez inclure dans le rapport ;
  - **Time Zone** : choisissez le fuseau horaire approprié à l'emplacement ;
  - **From** : choisissez la date de début du contenu du rapport en cliquant sur l'icône du calendrier. Saisissez la date de début à l'aide des listes déroulantes des heures (0 à 24) et des minutes (0 à 60) ;
  - **To** : choisissez la date de fin du contenu du rapport en cliquant sur l'icône du calendrier. Saisissez la date de fin à l'aide des listes déroulantes des heures (0 à 24) et des minutes (0 à 60).

ÉTAPE 5 Cliquez sur **Generate**. Une fois le rapport créé avec succès, cliquez sur le nom du rapport pour le consulter. WFBS-H nécessite Adobe Acrobat Reader 7.0 ou une version ultérieure pour consulter les rapports.

ÉTAPE 6 Si nécessaire, enregistrez le rapport localement.

Suppression de rapports existants

ATTENTION Il n'est pas possible de récupérer des rapports supprimés. Cisco vous conseille de télécharger les rapports avant de les supprimer.

Suivez ces étapes pour supprimer un rapport existant :

ÉTAPE 1 Lancez le portail Web WFBS-H.

REMARQUE Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Reports**.

ÉTAPE 3 Sur la page **Reports**, cochez la case de chacun des rapports que vous souhaitez supprimer. Pour sélectionner tous les rapports, cochez la case située en haut de la première colonne.

ÉTAPE 4 Cliquez sur le bouton **Delete** situé au-dessus du tableau.

Génération d'une requête de journal

Une requête de journal affiche les informations relatives aux virus ou aux logiciels malveillants, aux logiciels espions ou aux URL malveillantes détectés sur le réseau pendant la période indiquée. Elle fournit également des informations détaillées relatives au nom des ordinateurs, des menaces, des fichiers, du type d'analyse et de la mesure prise vis-à-vis de cette menace particulière.

Les données sont exportées au format CSV (Comma Separated Values, valeurs séparées par des virgules), qui peut être ouvert pour une analyse dans plusieurs tableurs et programmes de base de données tiers.

WFBS-H peut établir une requête de journal pour les types suivants :

- virus ou programmes malveillants ;
- logiciels espions ;
- URL malveillantes.

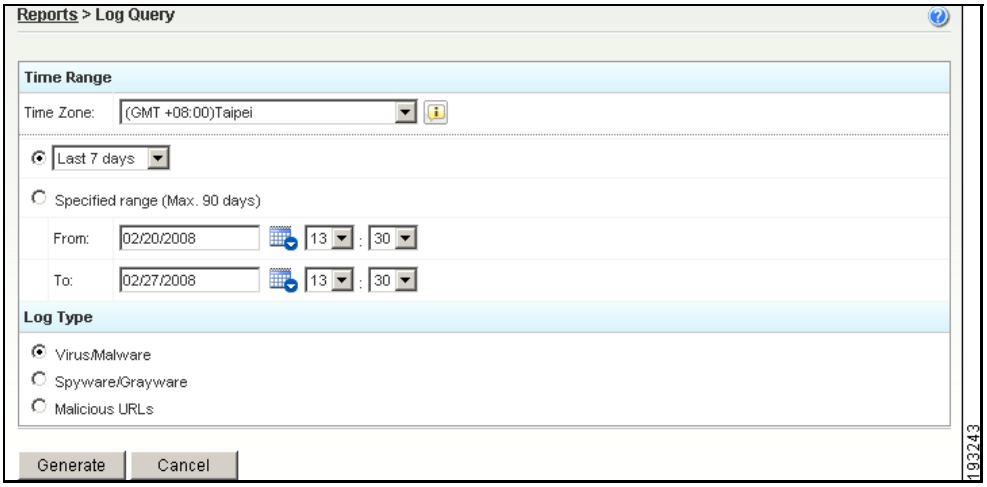
Suivez ces instructions pour générer une requête de journal :

ÉTAPE 1 Lancez le portail Web WFBS-H.

REMARQUE Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Reports**.

ÉTAPE 3 Cliquez sur le bouton **Log Query** situé au-dessus du tableau.



ÉTAPE 4 Dans la section **Time Range**, saisissez les paramètres suivants pour la requête :

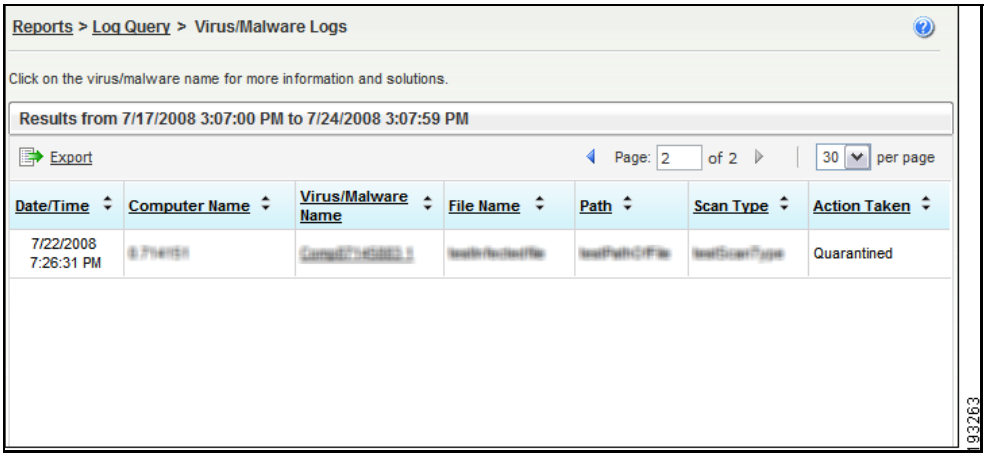
- **Time Zone** : choisissez le fuseau horaire approprié à l'emplacement ;
- **Plage** : utilisez la liste déroulante ou indiquez une plage ;
  - **Liste déroulante** : choisissez **All dates**, **Today**, **Last 7 days** ou **Last 30 days** ;
  - **Specified Range** : cliquez sur le bouton, puis saisissez la plage des dates en indiquant les valeurs pour **From** et **To** . Choisissez les dates en cliquant sur les icônes du calendrier. Saisissez l'heure à l'aide des listes déroulantes des heures (0 à 24) et des minutes (0 à 60).

    REMARQUE L'option Last 7 days est sélectionnée par défaut.

ÉTAPE 5 Dans la section **Log Type**, sélectionnez le type de menace à inclure dans le journal : **Virus/Malware, Spyware/Grayware** ou **Malicious URLs**.

ÉTAPE 6 Cliquez sur **Generate**. Un journal correspondant au type et à l'intervalle de temps sélectionnés s'affiche.

Le journal généré comporte des informations relatives aux noms des virus, des programmes malveillants ou des logiciels espions trouvés dans l'intervalle de temps indiqué et les mesures prises.



REMARQUE Par défaut; vous pouvez consulter 10 enregistrements par page. Vous pouvez sélectionner le nombre d'enregistrements que vous souhaitez consulter à partir de la liste par page. Vous pouvez également consulter les pages à l'aide de l'option de pagination.

ÉTAPE 7 Cliquez sur le bouton **Export** situé au-dessus du tableau pour exporter les données au format CSV.

Administration de Cisco ProtectLink Endpoint

Worry-Free Business Security Hosted ne nécessite qu'une administration minimale. À partir de la page Administration, vous pouvez :

- Consulter les informations relatives aux produits, à la licence et au compte. Vous pouvez consulter la date d'expiration de la licence et renouveler le contrat de service pour protéger vos ordinateurs des menaces les plus récentes ;
- Ajouter ou renouveler le service pour des services WFBS-H existants grâce au lien Renewal/Additional Service de la page Administration. La page Administration affiche les informations relatives au code d'activation, à la version du produit, au nombre de postes achetés, à l'état de l'enregistrement et à la date d'expiration de la licence.

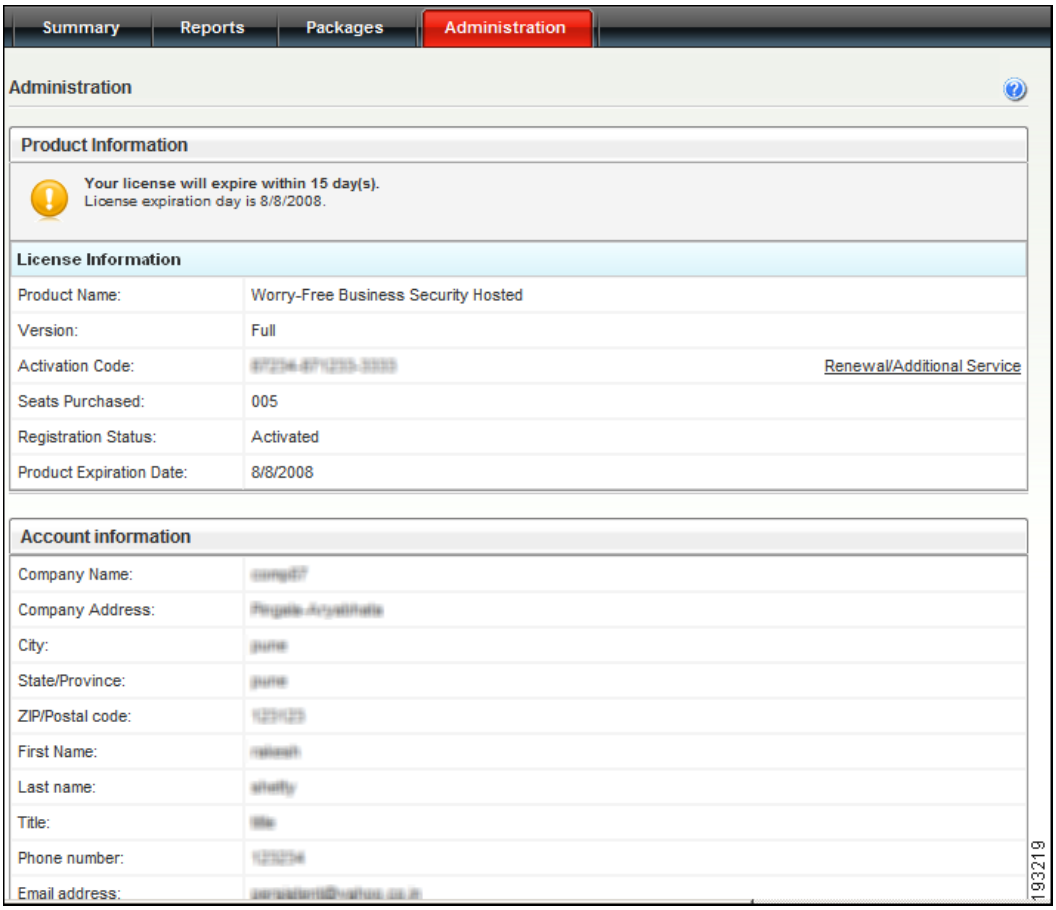
Gestion des licences

Suivez ces étapes pour renouveler ou ajouter un service :

ÉTAPE 1 Lancez le portail Web WFBS-H.

> **REMARQUE** Pour obtenir plus d'informations, reportez-vous à **Lancement du portail Web, page 55**.

ÉTAPE 2 Cliquez sur l'onglet **Administration**.



ÉTAPE 3 Cliquez sur le lien **Renewal/Additional Service** situé à côté du code d'activation.

Le site Web d'enregistrement s'affiche. Vous pouvez renouveler votre licence à partir de ce site Web.

Utilisation de l'outil de configuration de proxy WFBS-H Agent

Si les paramètres du proxy ont changé, utilisez l'outil de configuration de proxy pour configurer les paramètres du proxy d'un agent.

REMARQUE Sur des ordinateurs utilisant Windows Vista, exécutez ce programme en tant qu'administrateur.

Suivez ces étapes pour configurer les paramètres du proxy d'un agent :

ÉTAPE 1 Sur l'ordinateur, cliquez sur le bouton **Démarrer de Windows**.

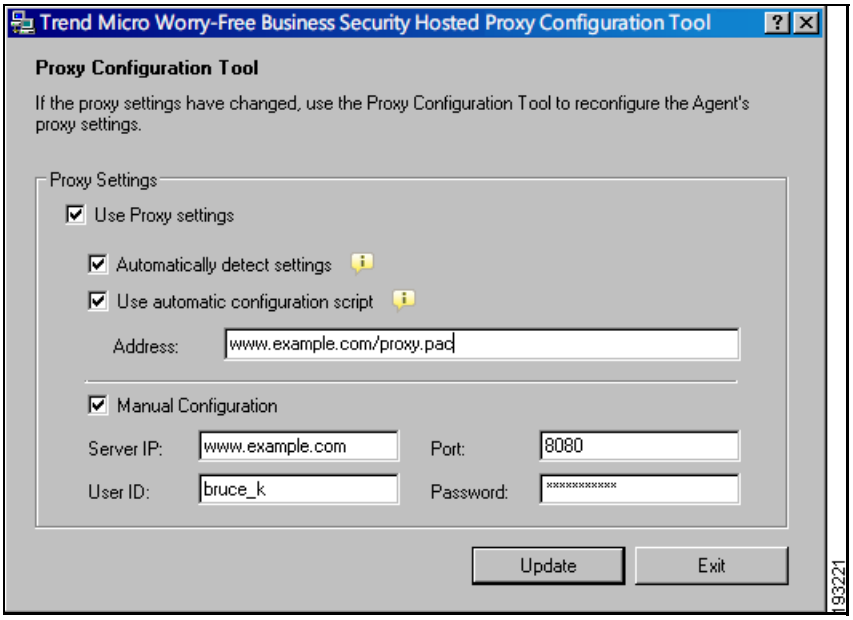
ÉTAPE 2 Choisissez **Poste de travail**, puis le lecteur sur lequel vous avez installé les fichiers, en général le disque local (C:).

Une fenêtre s'ouvre et affiche les fichiers et les dossiers du lecteur sélectionné.

ÉTAPE 3 Ouvrez **Programmes > Trend Micro > RAgent**.

ÉTAPE 4 Double-cliquez sur **ProxyCfg.exe**.

La fenêtre Worry-Free Business Security Hosted Agent Proxy Configuration Tool s'affiche.



ÉTAPE 5 Configurez les options de configuration requises :

- **Automatically detect settings** : l'agent récupère les paramètres à partir du DHCP et du DNS.
- **Use automatic configuration script** : saisissez l'emplacement du script de configuration dans la zone de texte Address.
- **Use HTTP Proxy** : indiquez l'IP du serveur, le port, l'identifiant utilisateur et le mot de passe pour le proxy HTTP.
- **Automatic configuration may override manual settings** : désactivez la configuration automatique pour assurer l'utilisation des paramètres manuels.

ÉTAPE 6 Cliquez sur **Apply.** Les modifications prennent effet immédiatement.

5

Terminologie

La sécurité informatique est en évolution constante. Les administrateurs et les professionnels de la sécurité des informations inventent et adoptent une grande variété de termes et de phrases permettant de décrire les risques potentiels ou les incidents indésirables que subissent les ordinateurs et les réseaux. La partie suivante est une présentation de ces termes et de leur signification, tels qu'ils sont utilisés dans ce document :

- **Virus/Programme malveillant, page 76**
- **Logiciel espion/programme espion, page 78**

Virus/Programme malveillant

Un virus informatique est un programme qui a la particularité unique de pouvoir se reproduire. Les virus peuvent s'attacher à presque tous les types de fichier exécutable et se répandent sous la forme de fichiers copiés et envoyés d'une personne à une autre. En plus de leur capacité à se reproduire, certains virus informatiques peuvent également provoquer des dégâts en transmettant une charge virale. Bien que ces charges se limitent parfois à afficher des messages ou des images, elles peuvent également détruire des fichiers, reformater le disque dur ou provoquer d'autres dégâts.

ProtectLink Endpoint détecte les virus ou les programmes malveillants. L'action recommandée par Cisco en cas de virus ou de programme malveillant est le nettoyage.

Prenez connaissance des termes supplémentaires associés aux virus et programmes malveillants :

- Portes dérobées : une porte dérobée permet de contourner l'authentification standard, de sécuriser l'accès à distance à un ordinateur et/ou d'obtenir l'accès à des informations tout en restant indétectable ;
- Macrovirus : les macrovirus sont spécifiques aux applications concernées. Ces virus se trouvent dans des fichiers pour des applications telles que Microsoft Word (.doc) ou Microsoft Excel (.xls). Par conséquent, ils peuvent être détectés dans des fichiers contenant des extensions semblables à celles des applications utilisant des macros, telles que .doc, .xls et .ppt. S'ils ne sont pas éliminés, les virus de macro se répandent dans les fichiers de données de l'application et peuvent finir par infecter des centaines de fichiers ;
- Programme malveillant : un programme malveillant est un logiciel conçu pour infiltrer ou endommager un système informatique sans le consentement de son propriétaire ;
- Dissimulateur d'activité : un dissimulateur d'activité est un ensemble de programmes conçu pour corrompre le contrôle légitime d'un système informatique par ses utilisateurs. Généralement, un dissimulateur d'activité complique l'installation du système et essaie d'empêcher sa suppression en compromettant la sécurité standard de ce système ;
- Chevaux de Troie : un cheval de Troie est un programme malveillant qui ressemble à une application inoffensive. Contrairement aux virus, les chevaux de Troie ne peuvent pas se reproduire mais ils peuvent être tout aussi dangereux. Une application qui prétend éliminer les virus de votre ordinateur alors qu'il en introduit est un exemple de cheval de Troie ;
- Vers : un ver informatique est un programme (ou ensemble de programmes) autonome capable de propager des copies fonctionnelles de lui-même ou de ses segments à d'autres systèmes informatiques. La propagation se fait généralement via les connexions réseau ou les pièces jointes des e-mails. Contrairement aux virus, les vers n'ont pas besoin de s'attacher aux programmes hôtes.

Logiciel espion/programme espion

ProtectLink Endpoint détecte les logiciels ou les programmes espions. L'action recommandée par Cisco en cas de logiciel ou de programme espion est le nettoyage.

- Logiciel espion : un logiciel espion est un logiciel informatique installé sur un ordinateur sans que l'utilisateur n'en soit averti ou n'y ait consenti et qui rassemble et transmet des informations personnelles ;
- Programme espion : un programme espion est un programme qui exécute des actions non désirées ou non autorisées. Il s'agit du terme général utilisé pour faire référence aux logiciels espions, logiciels publicitaires, numéroteurs, blagues, outils d'accès à distance et tous les autres fichiers et programmes indésirables. Selon son type, il peut ou non inclure un code malveillant se reproduisant ;
- Logiciel publicitaire : un logiciel publicitaire est un paquet logiciel qui lit, affiche ou télécharge automatiquement du matériel publicitaire sur un ordinateur après l'installation du logiciel ou pendant l'utilisation de l'application ;
- Robots : un robot est un programme qui fonctionne comme un agent pour un utilisateur ou pour un autre programme ou qui imite une activité humaine. Une fois exécutés, les robots peuvent se reproduire, se compresser et répandre des copies d'eux-même. Les robots peuvent permettre de coordonner une attaque automatisée sur des ordinateurs en réseau ;
- Numéroteurs : les numéroteurs permettent aux connexions à bas débit de se connecter à Internet. Les numéroteurs malveillants sont conçus pour se connecter avec des numéros à tarif élevé au lieu de se connecter directement au FAI. Les fournisseurs de ces numéroteurs malveillants empochent l'excédent dépensé. D'autres utilisations possibles de ces numéroteurs sont la transmission des informations personnelles et le téléchargement de logiciels malveillants ;
- Outils de piratage : un outil de piratage est un programme ou un ensemble de programmes conçu pour aider au piratage ;
- Enregistreurs de frappe : un enregistreur de frappe est un logiciel informatique qui enregistre toutes les frappes de l'utilisateur. Ces informations peuvent ensuite être récupérées et utilisées à des fins personnelles par le pirate.

6

Courrier électronique post-enregistrement et post-activation

Lors de l'enregistrement à Cisco ProtectLink EndPoint, des e-mails vous donnant des instructions sur la prochaine étape vous sont automatiquement envoyés après l'enregistrement et l'activation. Vous trouverez ci-dessous des exemples de ces e-mails.

Ce chapitre contient les sections suivantes :

Enregistrement et activation du courrier électronique—ProtectLink Endpoint

```
Objet : enregistrement de Cisco ProtectLink Endpoint réussi

Bienvenue chez Cisco !

Vous venez de vous enregistrer auprès du service ProtectLink(TM) Endpoint, un
service de sécurité hébergé en ligne fourni par Trend Micro(TM) Worry-
Free(TM) Business Security Hosted.

ProtectLink Endpoint se compose de deux modules :
* Worry-Free Business Security - Hosted
* Policy Enforcement
Worry-Free Business Security – Hosted a été activée. Consultez les
instructions suivantes pour activer l'activation de la politique :

1. Depuis la page de configuration du périphérique de sécurité, cliquez sur
ProtectLink puis sur I have my Activation Code (AC) and want to activate
ProtectLink services.
2. Activez Policy Enforcement à l'aide du code d'activation suivant :
ProtectLink Endpoint Service:
```

informations de connexion
* URL de la console Web ProtectLink Endpoint : WFBS-H.trendmicro.com
* Nom d'utilisateur : #LOGINID#
* Mot de passe : #PWD#

Pour vous connecter à la console Worry-Free Business Security - Hosted :
1. Entrez l'url de la console ProtectLink Endpoint pour accéder à la page de connexion.
2. Utilisez les informations de connexion ci-dessus pour vous connecter à la console.

Pour des détails supplémentaires, consultez les ressources ci-dessous :

* Guide de l'administrateur ProtectLink - <Link>
Conseil : consultez le chapitre 2 du guide de l'administrateur pour commencer à utiliser ProtectLink Endpoint.

* Page de renvoi ProtectLink Endpoint : www.trendmicro.com/go/wfbsh

Si vous êtes confrontés à des problèmes techniques lors de l'utilisation de votre produit, contactez l'assistance technique Cisco.
www.cisco.com/support/

Cordialement,
Cisco

Ce message a été envoyé automatiquement par les services d'inscription de Cisco. Ce compte est inactif. Veuillez ne pas répondre à ce message.

Activation de la politique d'entreprise

Bienvenue chez Cisco !

Félicitations. Vous venez d'activer la politique d'entreprise de Cisco ProtectLink Endpoint.

L'application de la politique est désormais activée. Depuis la page de configuration du périphérique de sécurité, cliquez sur ProtectLink > Desktop Protection > Policy Enforcement pour personnaliser les paramètres.

Pour consulter ou modifier votre profil client ou pour vous enregistrer d'autres produits Cisco ProtectLink, rendez-vous sur le site :
olr.trendmicro.com/registration/

Identifiant de connexion : #Logon ID#

Pour des détails supplémentaires, consultez les ressources ci-dessous :

*Guide de l'administrateur ProtectLink - <New Link>
Conseil : consultez le chapitre 2 du guide de l'administrateur pour commencer à utiliser ProtectLink Endpoint.

Si vous êtes confrontés à des problèmes techniques lors de l'utilisation de votre produit, contactez l'assistance technique Cisco.
www.cisco.com/support/

Cordialement,
Cisco

Ce message a été envoyé automatiquement par les services d'inscription de Cisco. Ce compte est inactif. Veuillez ne pas répondre à ce message.

A

Pour en savoir plus

Cisco offre une large gamme de ressources pour aider votre entreprise et vos clients à tirer parti au mieux de Cisco ProtectLink Endpoint.

Assistance technique	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Assistance technique et documentation en ligne (identification obligatoire)	www.cisco.com/support
Coordonnées du service d'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargement de logiciels (identifiant de connexion obligatoire)	Accédez à la page tools.cisco.com/support/downloads, puis saisissez la référence (modèle) dans le champ Software Search.
Documentation sur les produits	
Documentation technique	www.cisco.com/en/US/products/ps9952/tsd_products_support_series_home.html
Cisco Small Business	
Site Cisco Partner Central pour les PME (identifiant de connexion partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace