GUIDE D'ADMINISTRATION

Cisco Small Business

Cisco ProtectLink™ Web et Gateway 1.0

OL-24288-01

Table des matières

1

Introduction

Ce chapitre comprend les rubriques suivantes :

Versions de Cisco ProtectLink

Ce guide explique la configuration et le déploiement des versions suivantes de Cisco ProtectLink :

Cisco fournit également Cisco ProtectLink Endpoint. Pour de plus amples informations sur Cisco ProtectLink Endpoint, reportez-vous au *Guide d'administration de Cisco ProtectLink Endpoint 1.0*.

Cisco 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
- Un filtrage des adresses URL afin de contrôler l'accès des employés à des sites Web non productifs

Cisco ProtectLink Web est un sous-ensemble de Cisco ProtectLink Gateway et 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.

Cisco ProtectLink Gateway

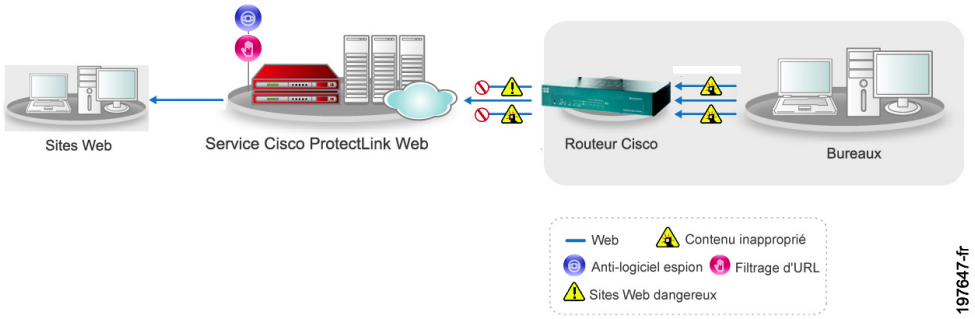
Cisco ProtectLink Gateway offre au routeur ou au périphérique de sécurité Cisco Small Business les fonctionnalités de sécurité Web de Cisco ProtectLink Web et les combine au système de sécurité de la messagerie électronique afin d'éviter le courrier indésirable, les virus et les tentatives d'hameçonnage.

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

Fonctionnement de ProtectLink Web

La **Figure 2** affiche le flux du trafic sur sites Web lors d'un accès à Internet via le service Cisco ProtectLink Web et le routeur ou le périphérique de sécurité. Le routeur ou le périphérique de sécurité bloque les menaces provenant des sites Web.

Figure 1 Fonctionnement de ProtectLink Web



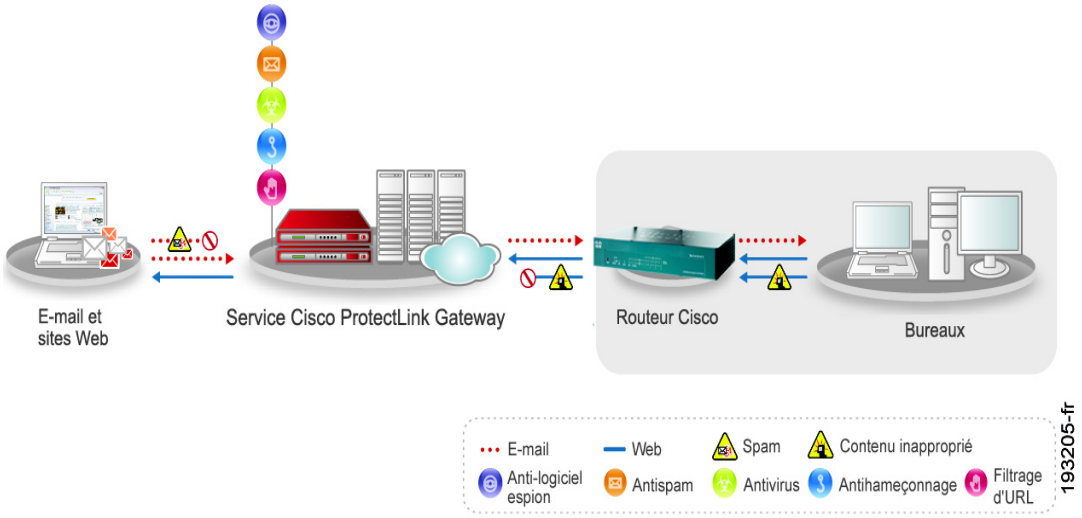
Pour de plus amples informations à propos de Cisco ProtectLink Web, accédez à l'adresse URL suivante :

www.cisco.com/go/protectlink

Protection des courriers électroniques par ProtectLink Gateway

La Figure 2 affiche le flux du trafic d'e-mails lors d'un accès à Internet via le service Cisco ProtectLink Web et le routeur ou le périphérique de sécurité.

Figure 2 Fonctionnement de ProtectLink Gateway



Le service ProtectLink Gateway Service bloque les menaces par courrier électronique dans le nuage grâce aux fonctions de Trend Micro IMHS.

La Figure 2 indique également la manière dont Cisco ProtectLink Gateway fournit un filtrage du Web et une protection contre ses menaces.

Pour de plus amples informations à propos de Cisco ProtectLink Gateway, accédez à l'adresse URL suivante :

www.cisco.com/go/protectlink

Filtrage du Web et protection contre les menaces

Cisco ProtectLink Web/Gateway offre un filtrage du Web et une protection contre ses menaces.

Le filtrage du Web vous permet de :

- Gérer l'accès à Internet.

  Vous pouvez par exemple créer des politiques qui interdisent l'accès à des sites Web que votre société considère être sans rapport avec le travail.

- Créer des filtres en fonction de catégories, d'intervalles de temps et des jours de la semaine.

  Par exemple, vous pouvez créer des filtres qui interdisent l'accès à certains sites Web de 8h du matin à midi (08:00 à 12:00) et de 13h à 17h (13:00 à 17:00).

La protection contre les menaces Web protège votre réseau en bloquant l'accès aux sites Web malveillants. Elle réalise les actions suivantes :

- Classe les sites Web en temps réel.

  Cisco ProtectLink Web/Gateway recourt à une technologie d'évaluation dynamique afin de classer les sites Web pendant que les utilisateurs accèdent à Internet.

- Bloque les sites Web malveillants en temps réel.

  Cisco ProtectLink Web/Gateway utilise une volumineuse base de données pour établir la réputation ou l'évaluation d'une adresse URL requise. Puis il compare l'évaluation avec les catégories limitées définies par votre société. S'il trouve une correspondance, ProtectLink Web/Gateway interdit l'accès au site Web. ProtectLink Web/Gateway évalue également le risque potentiel pour la sécurité de toutes les adresses URL requises en interrogeant la base de données de sécurité Web au moment de chaque requête HTTP.

Selon le score de réputation du site Web et le niveau de sécurité configuré, Web Protection bloque les sites Web dont la menace est connue ou suspectée.

- **Reputation Score** : ce score détermine si un site Web représente une menace ou non. Cisco calcule le score à l'aide de mesures propriétaires. Selon le score, Cisco classe une adresse URL comme « susceptible de représenter une menace Web », « très susceptible de représenter une menace Web » ou « menace Web ». Cisco considère une adresse URL comme étant sûre si son score excède le niveau de sécurité configuré, comme indiqué ci-dessous.
- **Security Levels** : le niveau de sécurité configuré et le score de réputation permettent de déterminer si Web Protection autorise ou bloque l'accès à une adresse URL. Sélectionnez l'un des niveaux suivants :
  - **High** : bloque un plus grand nombre de menaces de sites Web, mais augmente le risque de faux positifs.
  - **Medium** : bloque la plupart des menaces de sites Web et n'engendre pas un trop grand nombre de faux positifs. Ce paramètre est recommandé.
  - **Low** : bloque moins de menaces de sites Web, mais réduit le risque de faux positifs.

Lorsque ProtectLink Web/Gateway bloque un site Web, il envoie un message de notification au navigateur afin d'informer l'utilisateur que l'accès au site est refusé, conformément à la politique de la société.

REMARQUE Si la base de données d'évaluation des adresses URL ne renvoie pas de résultats d'évaluation à temps, l'accès à l'adresse URL est autorisé par défaut.

Les chiffres suivants, **Figure 3** et **Figure 4**, représentent le flux des tâches au sein de ce processus.

Figure 3 Flux des tâches de Web Protection : partie 1

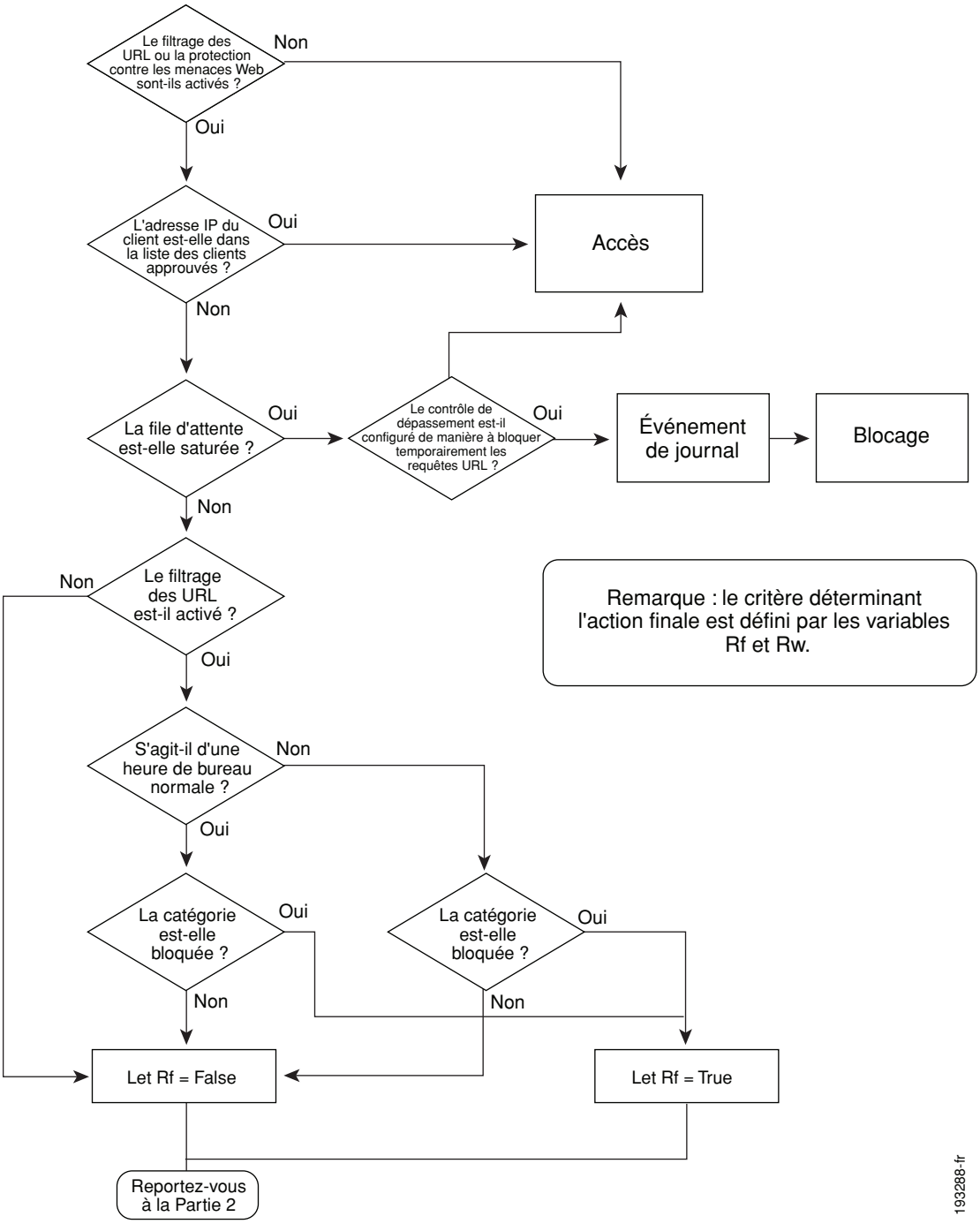
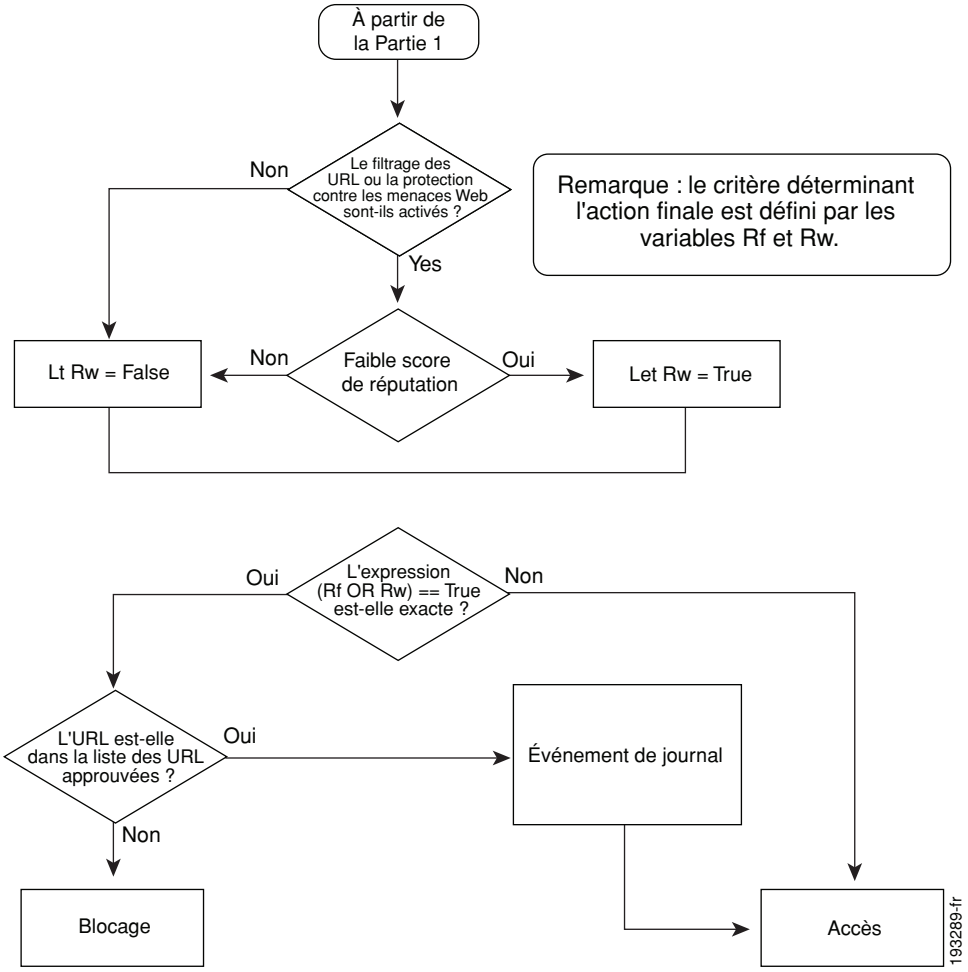


Figure 4 Flux des tâches de Web Protection : partie 2



Email Protection

Cette section comprend les rubriques suivantes :

REMARQUE Cette section s'applique uniquement à Cisco ProtectLink Gateway. Cisco ProtectLink Web n'offre pas de protection de messagerie électronique.

Principe de fonctionnement de Email Protection

Cisco ProtectLink Gateway fournit Email Protection par l'intermédiaire de Trend Micro IMHS, un service de sécurité hébergé rentable aux performances élevées qui protège les entreprises contre le courrier indésirable, les virus et le contenu inapproprié avant qu'ils n'atteignent le réseau.

Email Protection opère de la manière suivante lorsqu'un courrier électronique est envoyé à votre société via une adresse électronique :

1. Le serveur du courrier de l'expéditeur recherche le nom de domaine spécifié dans l'adresse électronique.
2. Comme le réseau est protégé par IMHS, l'enregistrement Mail eXchange (MX) du domaine provoque la redirection du courrier électronique vers IMHS.
3. Les serveurs IMHS acceptent le message et procèdent pour vous à un filtrage en fonction des messages et des politiques.
4. Si un message peut-être remis, les serveurs IMHS l'acheminent à vos serveurs de messagerie électronique.

En outre, il existe deux couches de protection :

- **Filtrage des e-mails au niveau de la connexion en fonction de la réputation, page 13**
- **Filtrage des courriers électroniques en fonction du contenu, page 13**

Filtrage des e-mails au niveau de la connexion en fonction de la réputation

Lorsqu'un serveur de messagerie électronique tente de se connecter à un serveur Email Protection, ce dernier interroge les services de réputation de messagerie (ERS, Email Reputation Services) afin de déterminer si l'adresse IP de l'expéditeur est digne de confiance.

Email Protection effectue un premier niveau de filtrage avant de recevoir le véritable message. Le contenu du message n'est pas examiné à ce stade.

Les tâches suivantes sont réalisées pendant le processus de Email Protection :

- Si l'adresse IP du serveur d'envoi est une source reconnue de courrier indésirable, elle est marquée comme n'étant pas digne de confiance. Le service Email Protection rejette systématiquement les tentatives de connexion à partir de cette adresse IP.
- Si l'ordinateur de l'expéditeur fait partie d'un botnet ou s'il s'agit d'un ordinateur zombie (deux termes de jargon désignant des réseaux ou des ordinateurs qui envoient automatiquement des courriers électroniques malveillants), l'adresse IP se trouve dans la base de données dynamique ERS. La base de données dynamique ERS identifie les sources de courrier indésirables lorsqu'ils apparaissent et les suit tant qu'ils sont actifs. Email Protection informe le serveur d'envoi que le serveur est momentanément indisponible.
- Si le serveur est légitime, le serveur tente de renvoyer le message au serveur de messagerie électronique de destination.

Filtrage des courriers électroniques en fonction du contenu

Lorsque le message a passé la première couche de protection, Email Protection examine le contenu du message afin de déterminer si celui-ci est un courrier indésirable ou s'il contient une menace. Le service hébergé intègre des fonctions anti-courrier indésirable avec des technologies antivirus, anti-hameçonnage et anti-espion.

Email Protection au sein d'un service standard

Email Protection de ProtectLink Gateway est fourni en tant que service standard via Trend Micro IMHS. Email Protection de ProtectLink Gateway offre les fonctions suivantes en tant que service standard :

- Une console de gestion simplifiée, mise à jour et ajustée par Cisco qui comporte des valeurs de protection prédéfinies par défaut.
- Une protection anti-courrier indésirable, antivirus et anti-hameçonnage à plusieurs niveaux pour le trafic de courrier électronique entrant, avec une gestion optimisée pour une sécurité totale et nécessitant une administration réduite.
- L'administrateur est en mesure de créer rapidement des « listes blanches » d'utilisateurs approuvés désignés par un domaine ou une adresse électronique.
- Accès à des rapports, au suivi de courrier électronique et à l'administration des mots de passe. La mise en quarantaine d'utilisateurs finaux sur Internet est également disponible pour une gestion simplifiée.

2

Déploiement de Cisco ProtectLink Web/ Gateway

Ce chapitre décrit la méthode de déploiement de Cisco ProtectLink Web/ Gateway :

Configuration système requise pour ProtectLink Web

Avant de déployer ProtectLink Web, vérifiez que le système répond aux conditions requises pour la protection de messagerie électronique et la protection Web indiquées ci-dessous.

Configuration requise pour ProtectLink Gateway

Avant de déployer ProtectLink Gateway, vérifiez que le système répond aux conditions requises suivantes :

- Navigateur Web

  Microsoft Internet Explorer 6.x ou 7.0 ou Mozilla Firefox 2.x ou 3.0

- Connexion Internet

Email Protection

Email Protection ne requiert pas d'achat de matériel supplémentaire (sauf la passerelle et le routeur de messagerie électronique) pour vos locaux. Tout le matériel d'analyse est situé hors site, dans les centres d'opération réseau sécurisés de Trend Micro. Un ordinateur personnel avec un accès à Internet est requis pour accéder à la console d'administration de Email Protection :

- Navigateur Web : Microsoft™ Internet Explorer 6.x ou 7.0 ou Mozilla™ Firefox™ 2.x ou 3.0.
- Connexion Internet.
- Accès aux enregistrements MX sur le serveur DNS afin de réacheminer les messages électroniques vers les serveurs de Trend Micro. Contactez votre fournisseur d'accès à Internet pour de plus amples informations ou pour obtenir une assistance relative à la configuration.

ATTENTION Ne redirigez pas l'enregistrement MX tant que vous n'avez pas reçu la confirmation que votre compte est créé. Si vous redirigez l'enregistrement MX avant la configuration de votre compte, vos messages électroniques pourraient être perdus.

Web Protection

Web Protection ne nécessite aucun matériel supplémentaire (sauf votre routeur) dans vos locaux.

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.

Utilisation de la page d'accueil de ProtectLink dans l'utilitaire de configuration

L'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité comporte une page avec des liens vers le site Web de ProtectLink. Ces liens facilitent l'achat, l'enregistrement et l'activation des produits ProtectLink.

Pour ouvrir la page avec les liens vers le site Web de ProtectLink :

- (Uniquement pour les périphériques de sécurité de la gamme SA 500) Cliquez sur **Administration > License Management**.

  La page License Management s'affiche.

- (Uniquement pour les routeurs de la gamme Cisco RV) Cliquez sur **ProtectLink** dans la barre de menus. Pour certains modèles, cliquez également sur **ProtectLink** dans l'arborescence de navigation.

  La page d'accueil de ProtectLink s'affiche.

REMARQUE Il est possible que les fenêtres de configuration soient différentes en fonction des modèles de routeur. En outre, les fenêtres peuvent s'afficher dans un ordre différent de celui présenté dans ce chapitre. Pour de plus amples informations sur l'utilitaire de configuration, reportez-vous à la documentation fournie avec le routeur ou le périphérique de sécurité. En outre, pour de plus amples informations sur une fenêtre, reportez-vous à l'aide en ligne de l'utilitaire de configuration.

Enregistrement de ProtectLink Web/Gateway

Enregistrez votre service pour l'activer et abonnez-vous pour accéder au portail Web de l'administration en ligne.

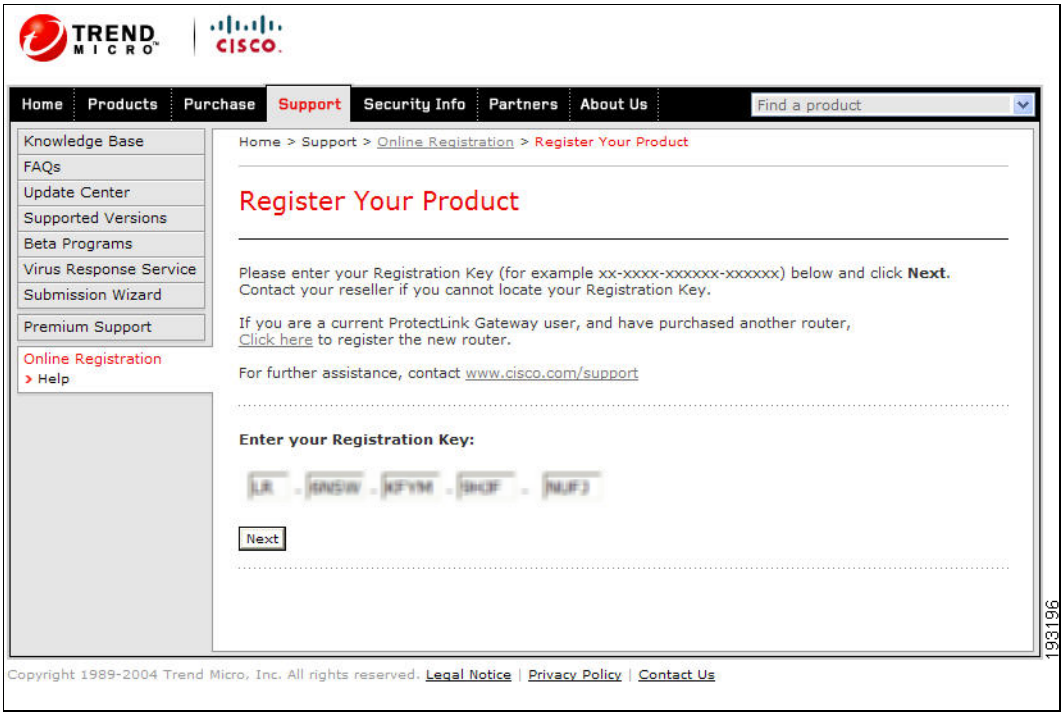
REMARQUE (Uniquement pour ProtectLink Gateway) L'activation complète du service nécessite l'entrée de la liste des domaines que vous souhaitez rediriger pour l'hébergement sur IMHS. IMHS devient alors l'hôte de messagerie principal pour la partie de protection de messagerie électronique du service ProtectLink Gateway. Si vous ne disposez pas de ces informations, vous pouvez enregistrer dès à présent le service et ajouter les informations manquantes par la suite. Vous recevrez les instructions dans un courrier électronique après l'enregistrement.

Enregistrement du service :

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

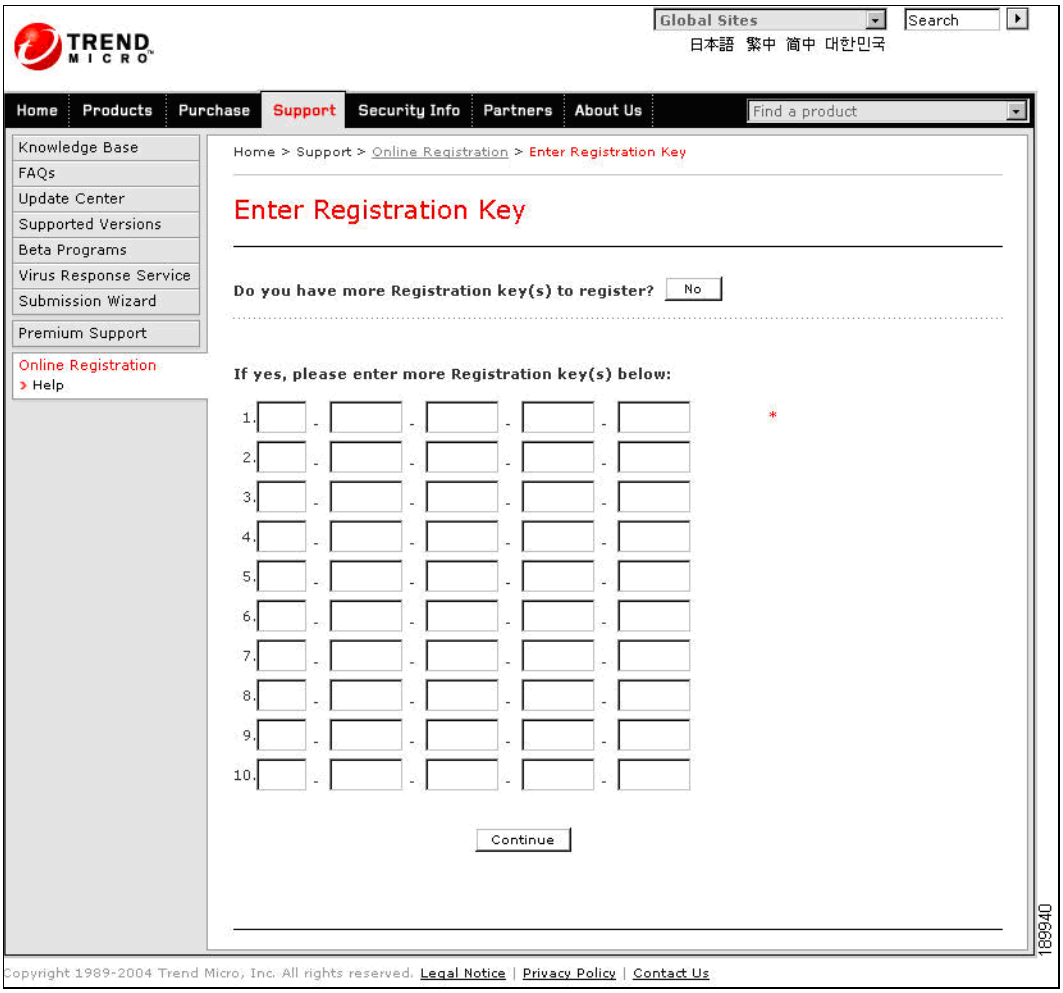
ÉTAPE 2 Ouvrez la page d'accueil ou la page License Management de ProtectLink, comme indiqué dans la section **Utilisation de la page d'accueil de ProtectLink dans l'utilitaire de configuration, page 17**.

Si vous ne disposez pas d'un compte ProtectLink, la fenêtre Register Your Product s'ouvre dans l'utilitaire de configuration.



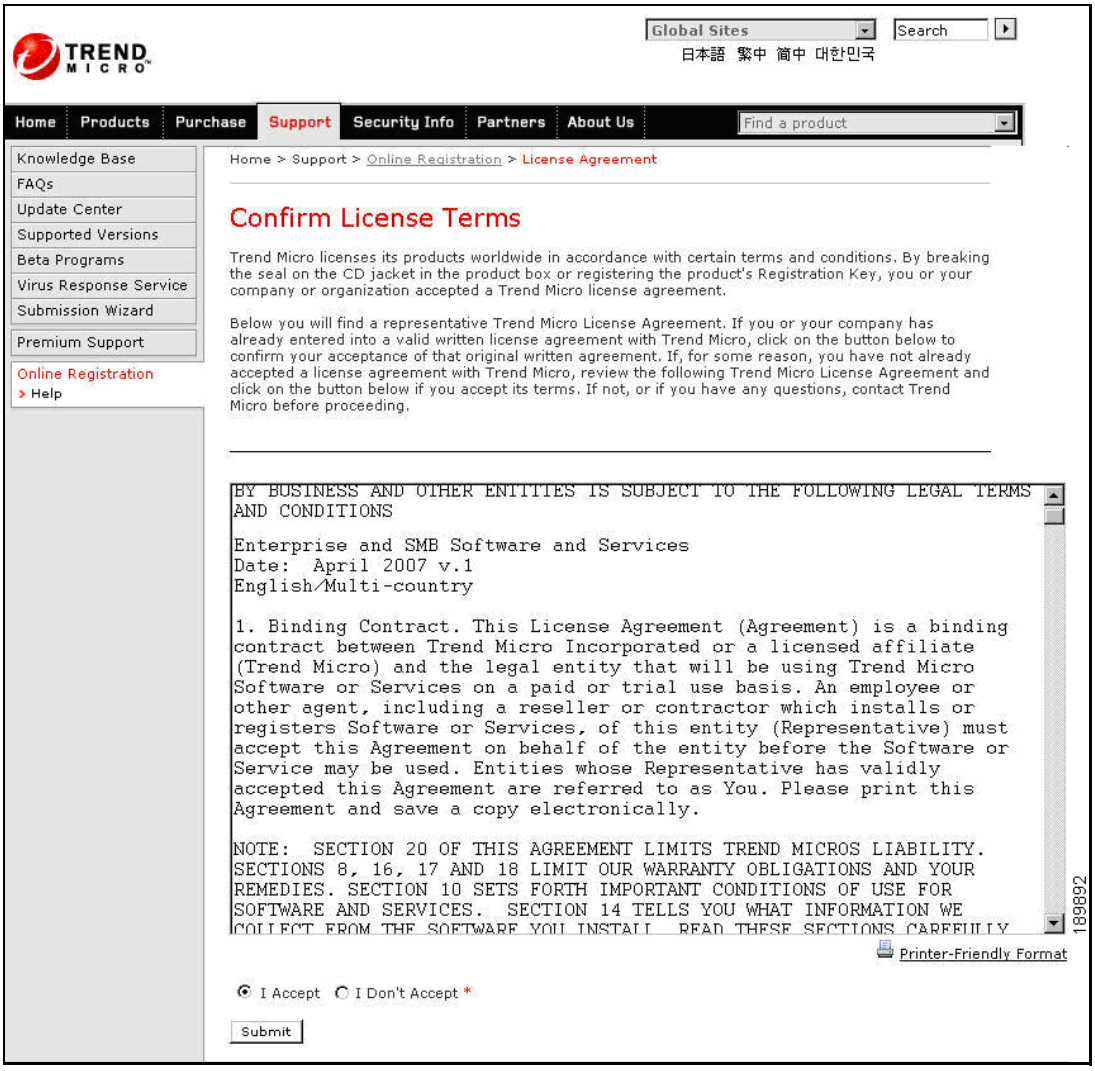
ÉTAPE 3 Saisissez la **clé d'enregistrement**, puis cliquez sur **Next**.

La page Enter Registration Key s'affiche.

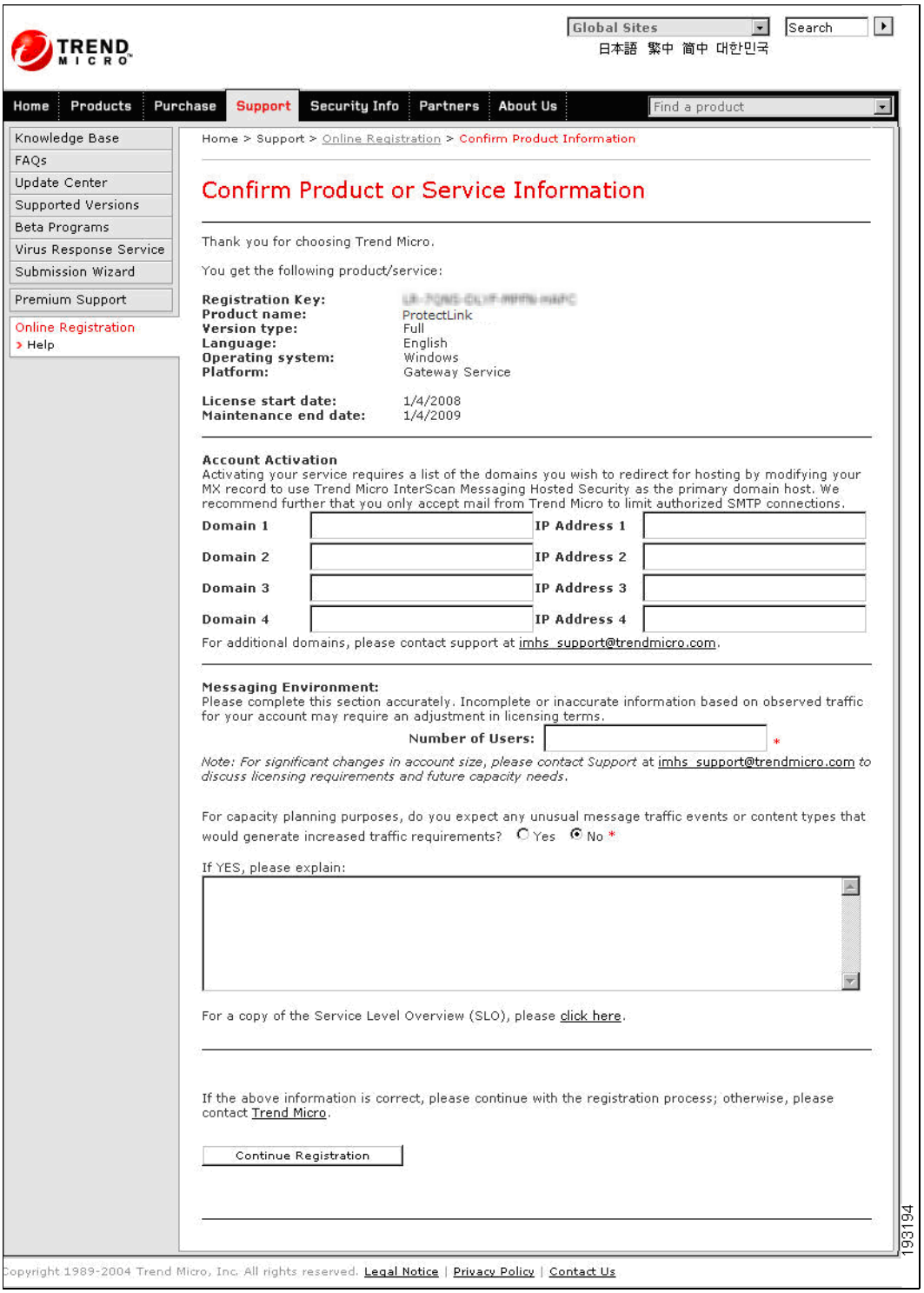


ÉTAPE 4 Le cas échéant, saisissez des **clés d'enregistrement** supplémentaires, puis cliquez sur **Continue**.

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 sur **Submit**. La page Confirm Product or Service Information s'affiche.



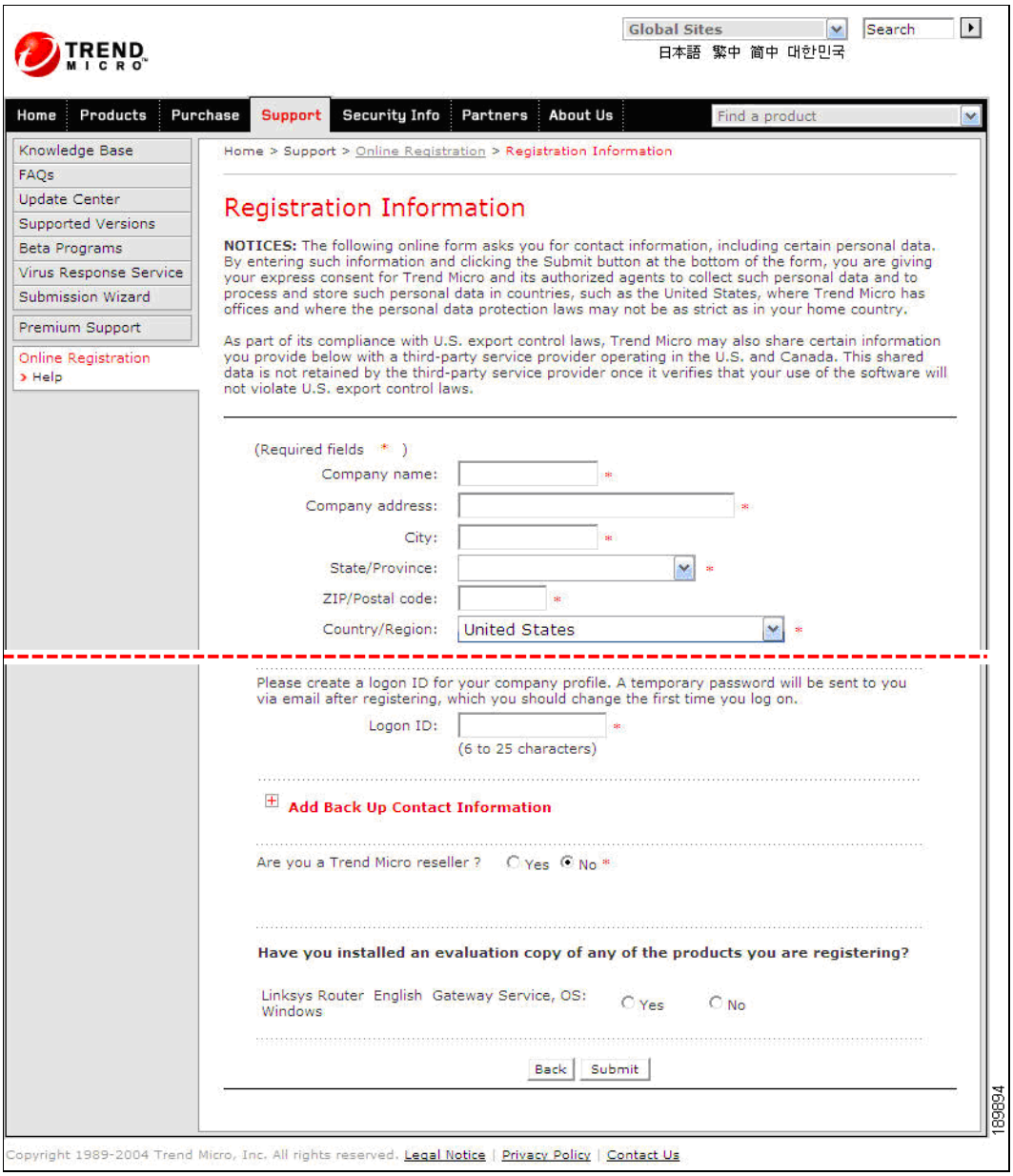
ÉTAPE 6 Dans la section **Do you have Domain/IP address now?**, sélectionnez l'une des options suivantes :

- **Yes** : sélectionnez cette option si vous êtes prêt à saisir la liste des domaines que vous souhaitez rediriger pour l'hébergement sur IMHS. Pour activer intégralement le service, vous devez saisir la liste de vos domaines. Puis saisissez chaque domaine ou adresse IP. Si vous devez saisir plus de quatre noms de domaine ou adresses IP, contactez l'assistance Cisco.
- **No** : sélectionnez cette option si vous n'êtes pas prêt à saisir la liste des domaines maintenant. Dans ce cas, le système utilise des paramètres temporaires. Vous pouvez mettre à jour ces informations par la suite en contactant l'assistance Cisco.

ÉTAPE 7 Dans la section **Messaging Environment**, saisissez les informations suivantes :

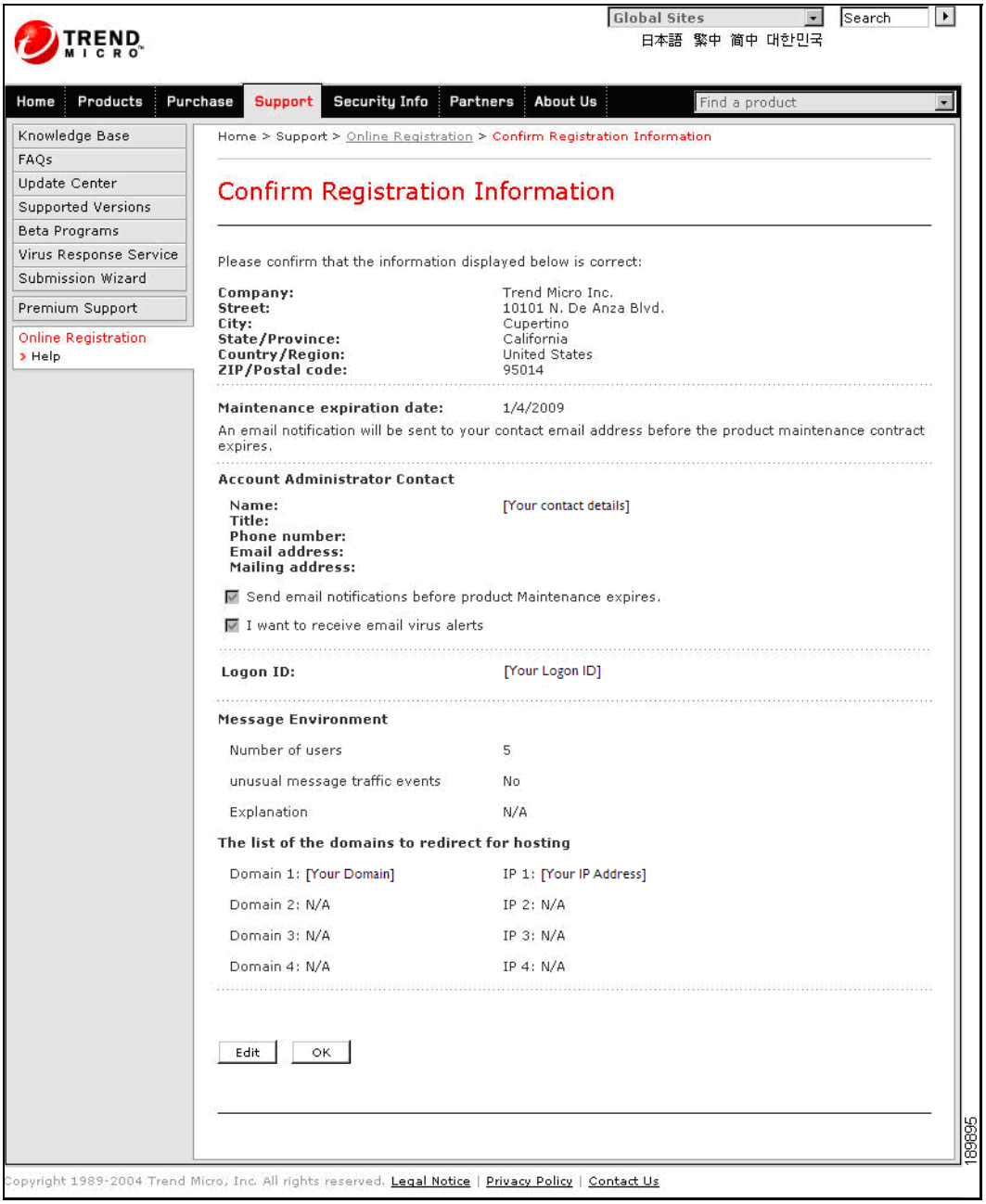
- **Number of Users** : saisissez le nombre d'utilisateurs ayant souscrit à ce service conformément au contrat d'achat.
- Répondez à la question concernant la planification des capacités en sélectionnant l'une des options suivantes :
  - **Yes** : sélectionnez cette option si vous prévoyez un trafic inhabituel de messages ou de types de contenu qui pourrait être à l'origine d'une augmentation des exigences relatives au trafic. Saisissez l'explication de votre situation dans la zone de saisie de texte.
  - **No** : sélectionnez cette option si vous ne prévoyez pas de trafic anormal de messages ni de types de contenu inhabituels.

La page Registration Information s'affiche.



ÉTAPE 8 Saisissez l'intégralité de vos coordonnées, y compris votre adresse électronique et l'identifiant de connexion du profil de votre société, puis cliquez sur **Submit**.

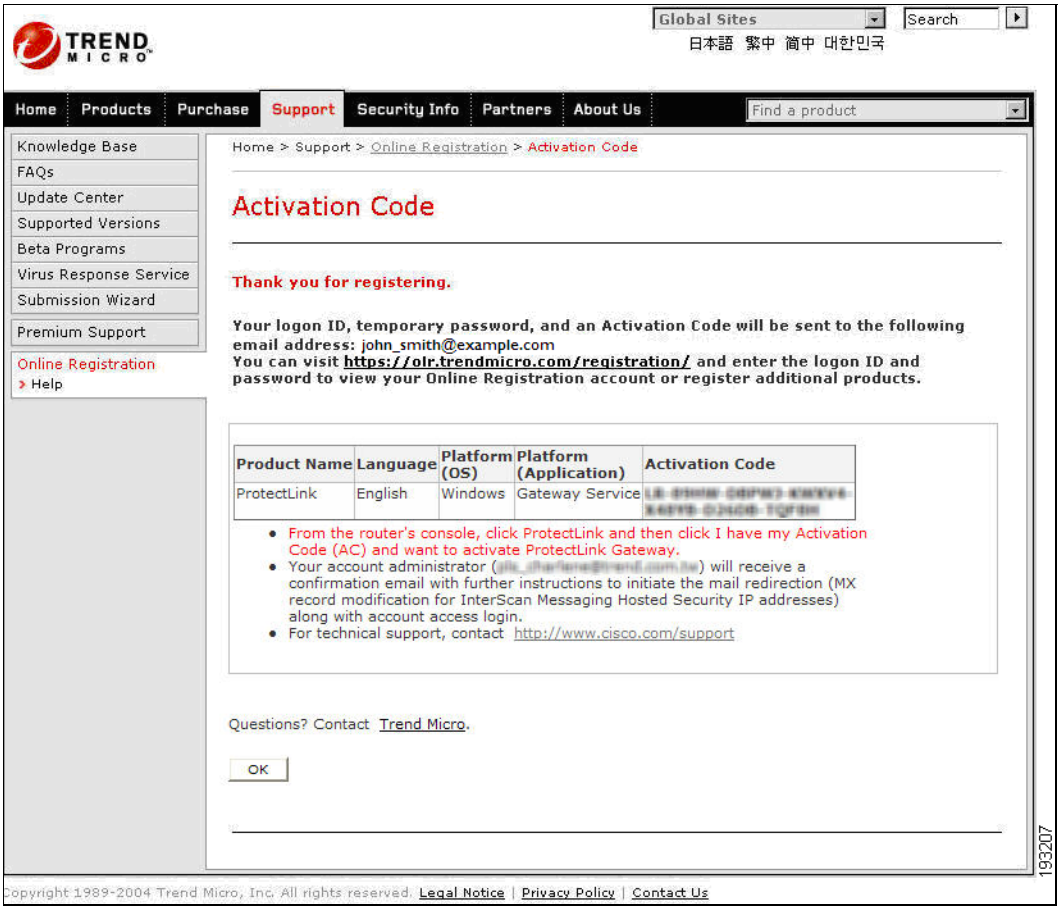
La page Confirm Registration s'affiche, avec vos coordonnées et vos domaines.



ÉTAPE 9 Vérifiez que les informations sont correctes.

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

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



ÉTAPE 10 Par la suite, vous pouvez accéder à https://olr.trendmicro.com/registration/ pour consulter votre compte en ligne ou pour enregistrer des produits Cisco ProtectLink supplémentaires.

ÉTAPE 11 Cliquez sur **OK** pour terminer le processus d'enregistrement.

Activation de ProtectLink Web/Gateway

Après avoir terminé l'enregistrement de ProtectLink Web/Gateway, vous recevrez dans les 24 à 48 heures un courrier électronique indiquant la réussite de l'enregistrement du service.

Ce courrier électronique vous fournit un code d'activation confirmant votre identifiant de connexion et octroyant un mot de passe temporaire à votre société. Vous devez modifier le mot de passe après vous être connecté.

Ce courrier électronique contient également des instructions concernant l'attribution d'une adresse IP de redirection à vos domaines de messagerie électronique et à votre serveur de messagerie électronique, si vous n'avez pas effectué cette action pendant le processus d'enregistrement.

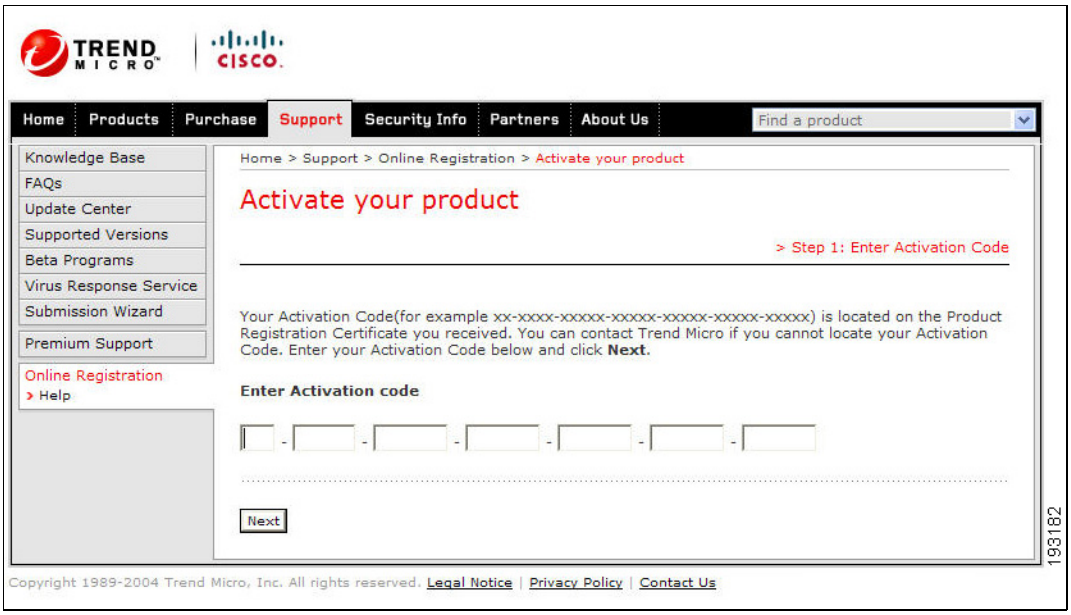
Pour activer le service ProtectLink Web/Gateway :

ÉTAPE 1 Démarrez l'utilitaire de configuration pour le routeur ou le périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Ouvrez la page d'accueil de ProtectLink, comme indiqué dans la section **Utilisation de la page d'accueil de ProtectLink dans l'utilitaire de configuration, page 17**.

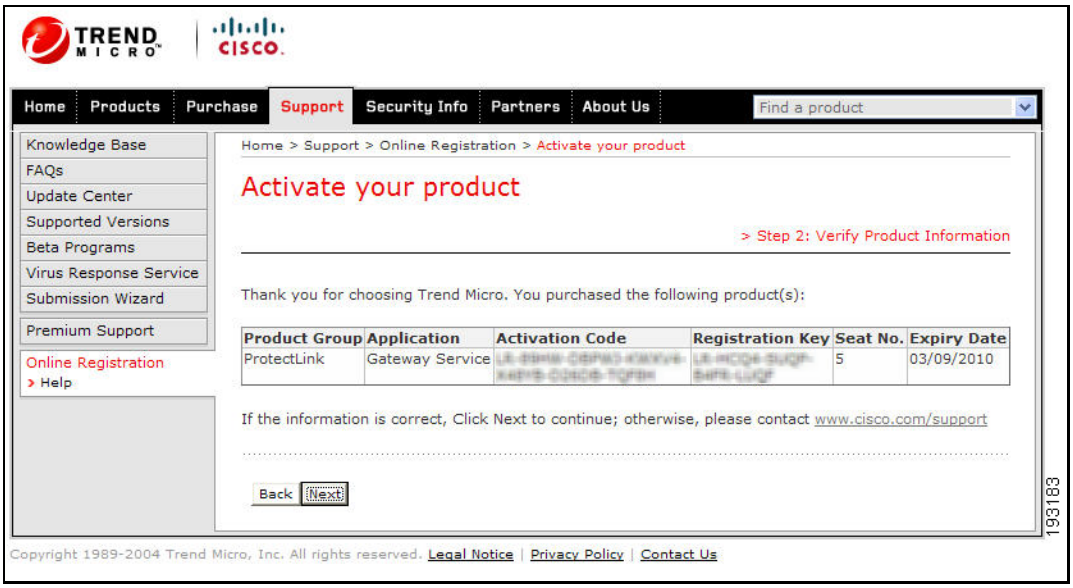
ÉTAPE 3 En bas de la page, cliquez sur le lien pour activer votre service. Ce lien peut être **I have my Activation Code (AC) and want to activate ProtectLink Web/Gateway** ou **Use the Activation Code (AC) to activate ProtectLink services**.

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



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

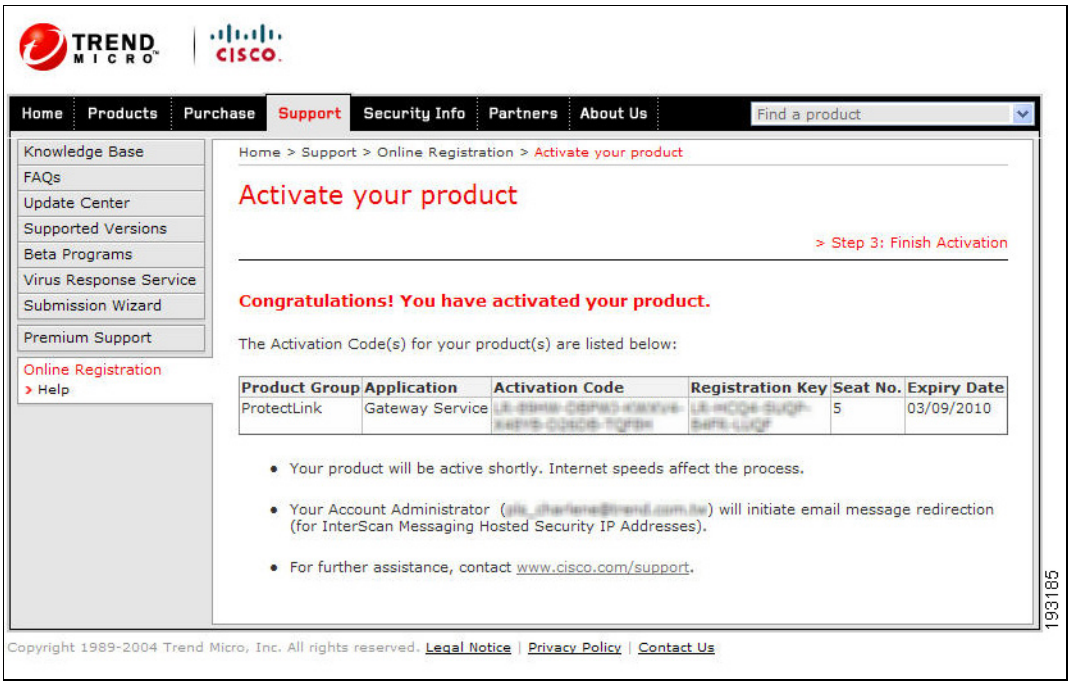
La fenêtre Activate Your Product > Step 2: Verify Product Information s'affiche.



ÉTAPE 5 Vérifiez que les informations de produit sont correctes.

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

Si un message indique que vous devez corriger les informations, cliquez sur **Back**, puis saisissez à nouveau le code d'activation.



La fenêtre Activate Your Product > Step 3: Finish Activation s'affiche.

Vous venez d'activer le produit. Votre service sera actif d'ici au prochain jour ouvrable.

Redirection du courrier électronique via ProtectLink Gateway

Après réception des informations d'activation, Trend Micro vous envoie des courriers électroniques supplémentaires.

- Le courrier électronique Web Protection Activation fournit un identifiant de connexion et un mot de passe temporaire, ainsi que des instructions permettant à votre société de personnaliser Web Protection.
- Le courrier électronique Email Protection Activation comprend votre nom d'utilisateur IMHS et un mot de passe temporaire permettant d'accéder au portail Web IMHS, ainsi que des instructions sur la manière de rediriger votre enregistrement Mail Exchange (MX).
- Si votre compte Email Protection est correctement configuré, un courrier électronique test est envoyé pour vérifier que les messages électroniques peuvent circuler correctement via les serveurs de Trend Micro.

REMARQUE Si vous n'avez pas fourni le nom de domaine ou l'adresse IP de votre serveur de messagerie électronique au cours de l'enregistrement, votre compte Email Protection n'est pas créé. Suivez les instructions du courrier électronique post-enregistrement pour fournir ces détails. Ne redirigez pas votre enregistrement MX tant que vous n'avez pas reçu le courrier électronique test indiquant que votre compte est correctement créé. Si vous redirigez l'enregistrement MX avant la configuration complète de votre compte, vos messages électroniques pourraient être perdus.

3

Configuration de Cisco ProtectLink Web/ Gateway

Une fois votre compte activé, configurez votre routeur pour la protection Web, selon les instructions détaillées dans les sections suivantes :

- **Configuration des clients approuvés, page 32**
- **Configuration des URL approuvées, page 34**
- **Configuration du contrôle de dépassement, page 36**
- **Configuration de la protection contre les menaces Web (réputation Web), page 37**
- **Configuration du filtrage d'URL, page 38**
- **Activation du journal système et du journal des blocages d'appels sortants, page 41**

REMARQUE Il est possible que les fenêtres de configuration soient différentes en fonction des modèles de routeur. En outre, les fenêtres peuvent s'afficher dans un ordre différent de celui présenté dans ce chapitre. Pour de plus amples informations sur l'utilitaire de configuration, reportez-vous à la documentation fournie avec le routeur ou le périphérique de sécurité. En outre, pour de plus amples informations sur une fenêtre, reportez-vous à l'aide en ligne de l'utilitaire de configuration.

Configuration des clients approuvés

La liste des clients approuvés répertorie les ordinateurs dont l'accès au Web n'est pas restreint. ProtectLink approuve toutes les requêtes d'URL provenant des adresses IP spécifiées.

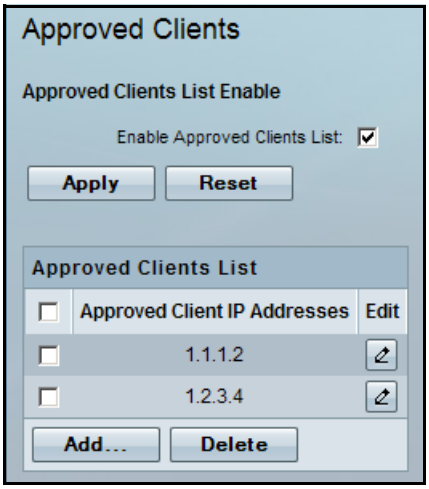
Les paramètres de protection Web ne s'appliquent pas aux requêtes Internet des ordinateurs dont l'adresse IP figure sur cette liste.

Pour configurer la liste des clients approuvés :

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 (Pour les routeurs RV042/82/16) Cliquez sur **ProtectLink** dans la barre de menus.

La fenêtre Web Protection apparaît. La liste des clients approuvés s'affiche en bas de la page.



ÉTAPE 3 (Pour les routeurs de série SA500) Cliquez sur **ProtectLink** dans la barre de menus, puis sélectionnez successivement **Global Settings > Approved Clients** dans l'arborescence de navigation pour afficher la liste des clients approuvés.

ÉTAPE 4 Pour activer la liste des clients approuvés, cochez la case **Enable Approved Clients List**, puis cliquez sur **Apply** ou **Save Settings**.

ÉTAPE 5 Pour ajouter un nouveau client, ou plusieurs clients dans une plage d'adresses IP, cliquez sur **Add**.

REMARQUE **Autres options disponibles** : pour modifier une entrée, cliquez sur le bouton en forme de stylet dans la colonne **Edit**. Pour supprimer une entrée, cochez la case correspondante et cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

ÉTAPE 6 Pour identifier le ou les clients, 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 renseignez pas ce champ. S'il y a une plage d'adresses IP (Range), saisissez ici la dernière d'entre elles. ProtectLink approuvera toutes les 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 7 Cliquez sur **Apply** ou **Save Settings**. Les informations saisies apparaissent dans la liste des clients approuvés.

REMARQUE Si votre utilitaire de configuration comprend tous les paramètres de protection Web sur une seule page, vous pouvez enregistrer les paramètres après avoir configuré toutes les fonctions désirées apparaissant sur la page.

Configuration des URL approuvées

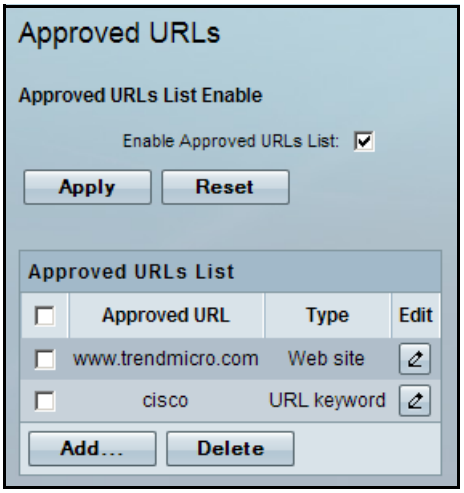
La liste des URL approuvées répertorie les sites Web dont l'accès n'est jamais refusé. Les sites approuvés sont définis par des URL spécifiques ou par des mots-clés dans les URL.

Pour configurer les URL approuvées :

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Cliquez sur **ProtectLink** dans la barre de menus, puis sélectionnez successivement **Global Settings > Approved URLs** dans l'arborescence de navigation.

REMARQUE Si votre utilitaire de configuration ne comporte pas d'arborescence de navigation gauche, cliquez sur **ProtectLink** puis sélectionnez l'option **Web Protection**. Ensuite, faites défiler jusqu'à la section **Approved URLs** de la page. La présentation de la page peut être différente de l'illustration.



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

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

REMARQUE **Autres options disponibles** : pour modifier une entrée, cliquez sur le bouton en forme de stylet dans la colonne **Edit**. Pour supprimer une entrée, cochez la case correspondante et cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

ÉTAPE 5 Pour spécifier une URL exacte ou un mot-clé, saisissez les informations suivantes :

- **URL** : saisissez l'URL exacte du site (par exemple, *www.yahoo.com*) ou une URL partielle à utiliser comme mot-clé (par exemple, *yahoo*).
- **Match Type** : sélectionnez l'une des options suivantes :
  - **Web site** : sélectionnez cette option si vous voulez autoriser l'accès uniquement à l'URL exacte saisie dans le champ URL. Par exemple, si vous avez saisi *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** : sélectionnez cette option si vous souhaitez autoriser l'accès à toute URL comprenant le mot-clé saisi dans le champ URL. Par exemple, si vous avez saisi *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** ou **Save Settings** pour enregistrer les paramètres. Les informations saisies apparaissent dans la liste des clients approuvés.

REMARQUE Si votre utilitaire de configuration comprend tous les paramètres de protection Web sur une seule page, vous pouvez enregistrer les paramètres après avoir configuré toutes les fonctions désirées apparaissant sur la page.

Configuration du contrôle de dépassement

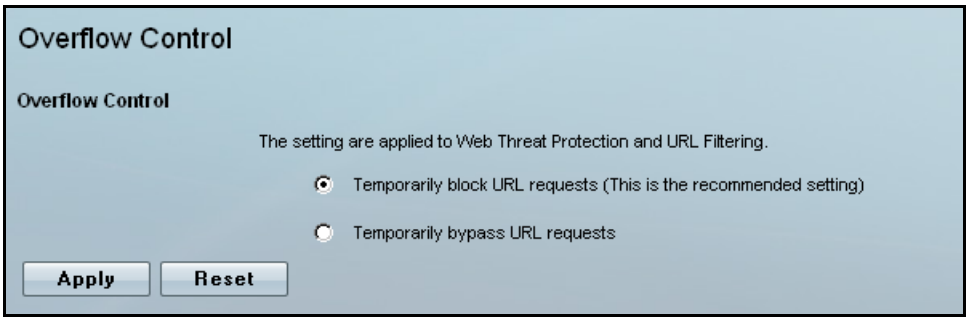
Le contrôle de dépassement détermine la manière dont ProtectLink traite les requêtes d'URL en excès. Lors de périodes de dépassement, vous pouvez soit bloquer les requêtes, soit contourner le filtrage des URL. L'option par défaut est le blocage des requêtes ; elle est recommandée pour assurer que le filtrage des URL continue à protéger votre activité lors des périodes d'activité intense.

Pour configurer le contrôle du dépassement :

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Cliquez sur **ProtectLink** dans la barre de menus, puis sélectionnez successivement **Web Protection > Overflow Control** dans l'arborescence de navigation.

> **REMARQUE** Si votre utilitaire de configuration ne comporte pas d'arborescence de navigation gauche, cliquez sur **ProtectLink** puis sélectionnez l'option **Web Protection**. Ensuite, faites défiler jusqu'à la section **Overflow Control** de la page. La présentation de la page peut être différente de l'illustration.



ÉTAPE 3 Sélectionnez l'une des options suivantes :

- **Temporarily block URL requests** : cette option permet de gérer le dépassement en bloquant temporairement toutes les nouvelles requêtes de site Web. Cette configuration est recommandée.
- **Temporarily bypass URL requests** : cette option permet de gérer le dépassement en contournant temporairement le filtrage d'URL des nouvelles requêtes de sites Web.

ÉTAPE 4 Cliquez sur **Apply** ou **Save Settings** pour enregistrer les paramètres.

REMARQUE Si votre utilitaire de configuration comprend tous les paramètres de protection Web sur une seule page, vous pouvez enregistrer les paramètres après avoir configuré toutes les fonctions désirées apparaissant sur la page.

Configuration de la protection contre les menaces Web (réputation Web)

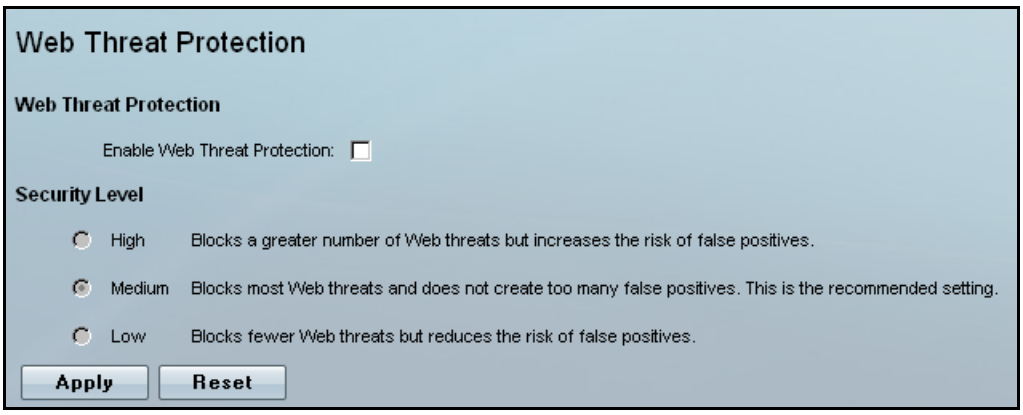
Si vous activez la fonction de protection contre les menaces Web (ou réputation Web), vous pouvez choisir le niveau de sécurité souhaité.

Pour configurer la protection contre les menaces Web :

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Cliquez sur **ProtectLink** dans la barre de menus, puis sélectionnez successivement **Web Protection > Web Threat Protection** dans l'arborescence de navigation.

REMARQUE Si votre utilitaire de configuration ne comporte pas d'arborescence de navigation gauche, cliquez sur **ProtectLink** puis sélectionnez l'option **Web Protection**. Ensuite, faites défiler jusqu'à la section **Web Reputation** de la page. La présentation de la page peut être différente de l'illustration.



ÉTAPE 3 Pour activer cette fonction :

- Cochez la case **Enable Web Threat Protection** .

  REMARQUE Sur certains modèles, cette case apparaît en haut de la page Web Protection.

- Sélectionnez **Security Level for Web Reputation** :

  - **High** : bloque un plus grand nombre de menaces du Web mais augmente le risque de faux positifs. En d'autres termes, cette option risque de bloquer des sites Web qui sont fiables.
  - **Medium** : bloque la plupart des menaces du Web et ne crée pas trop de faux positifs. Cette configuration est recommandée.
  - **Low** : bloque un nombre plus restreint de menaces, mais réduit le risque de faux positifs.

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

REMARQUE Si votre utilitaire de configuration comprend tous les paramètres de protection Web sur une seule page, vous pouvez enregistrer les paramètres après avoir configuré toutes les fonctions désirées apparaissant sur la page.

Configuration du filtrage d'URL

Utilisez le filtrage d'URL pour limiter l'accès à des URL spécifiques. Différentes options de filtrage d'URL peuvent être définies pour les heures ouvrées et les heures de fermeture.

Pour configurer le filtrage d'URL :

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Cliquez sur **ProtectLink** dans la barre de menus, puis sélectionnez successivement **Web Protection > URL Filtering** dans l'arborescence de navigation.

> **REMARQUE** Si votre utilitaire de configuration ne comporte pas d'arborescence de navigation gauche, cliquez sur **ProtectLink** puis sélectionnez l'option **Web Protection**. Ensuite, faites défiler jusqu'à la section **URL Filtering** de la page. La présentation de la page peut être différente de l'illustration.

ÉTAPE 3 Pour activer le filtrage d'URL, cochez la case **Enable URL Filtering**.

ÉTAPE 4 Dans le tableau **Filtered Categories**, sélectionnez les catégories et heures auxquelles s'appliquera le filtrage.

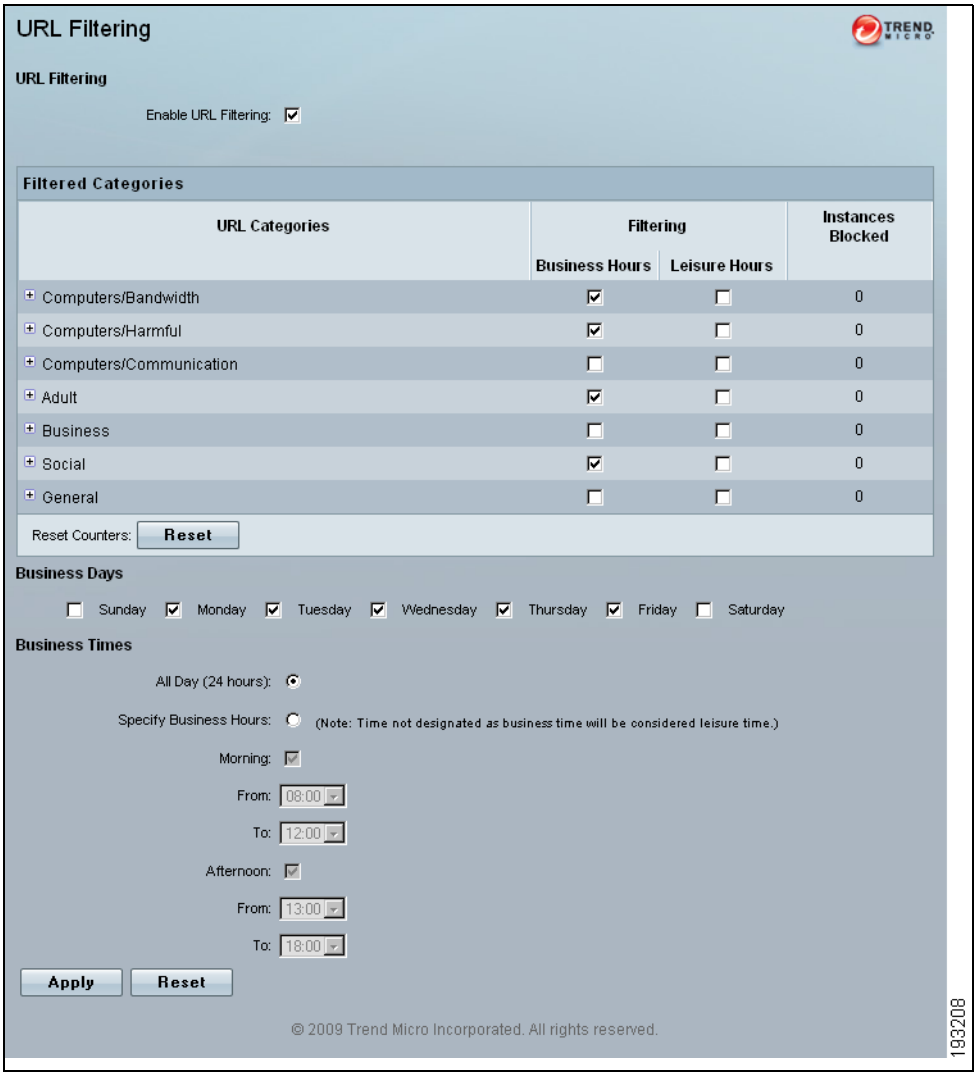
- **Filtered Categories** : pour voir les sous-catégories, cliquez sur le signe **+** en regard du nom de la catégorie.
- **Business Hours** : pour chaque catégorie ou sous-catégorie, cochez la case correspondante afin d'activer le filtrage d'URL pendant les jours et heures ouvrés que vous allez définir sur cette page.
- **Leisure Hours** : pour chaque catégorie ou sous catégorie, cochez la case correspondante afin d'activer le filtrage d'URL pendant les heures de fermeture. Les heures de fermeture représentent les jours et les heures non compris dans les champs **Business Days** et **Business Times**.

ÉTAPE 5 Définissez les heures ouvrées durant lesquelles le filtrage d'URL doit être appliqué, en sélectionnant des valeurs dans les champs **Business Days** et **Business Times** :

- **Business Days** : cochez la case de chaque jour à inclure dans les heures ouvrées. Les jours non sélectionnés seront considérés comme heures de fermeture en ce qui concerne le filtrage d'URL.
- **Business Times** : sélectionnez parmi les options suivantes :
  - **All Day (24 hours)** : choisissez cette option pour inclure toutes les heures du jour spécifié dans les heures ouvrées.
  - **Specify Business Hours** : choisissez cette option si vous souhaitez définir des périodes spécifiques pour les heures ouvrées. Ensuite, choisissez des périodes dans les sections **Morning** et **Afternoon**. Toutes les heures non comprises dans ces intervalles seront considérées comme heures de fermeture en ce qui concerne le filtrage d'URL.

Morning : cochez cette case pour définir des heures en matinée (avant midi). Spécifiez l'intervalle des heures ouvrées en matinée à l'aide des listes déroulantes **From** et **To**.

Afternoon : cochez cette case pour définir des heures en après-midi. Spécifiez l'intervalle des heures ouvrées en après-midi à l'aide des listes déroulantes **From** et **To**.



ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Si votre utilitaire de configuration comprend tous les paramètres de protection Web sur une seule page, vous pouvez enregistrer les paramètres après avoir configuré toutes les fonctions désirées apparaissant sur la page.

Activation du journal système et du journal des blocages d'appels sortants

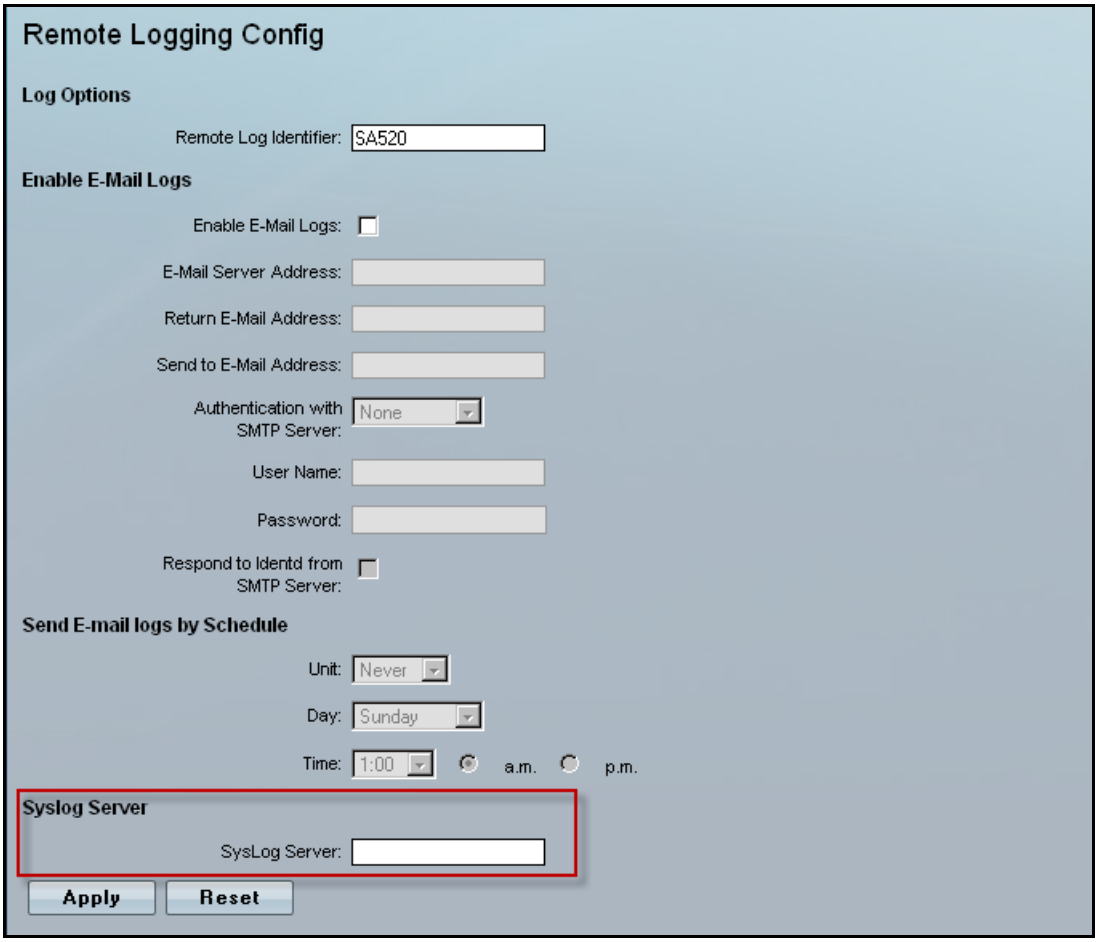
ProtectLink Web/Gateway peut fournir un journal système (syslog) ainsi qu'un journal des blocages d'appels sortants pour tous les événements bloqués. Activez ces fonctionnalités pour mettre à jour les journaux.

Pour activer le journal système et le journal des blocages d'appels sortants :

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

ÉTAPE 2 Cliquez sur **Administration** sur la barre de menus, puis sélectionnez successivement **Logging > Remote Logging** dans l'arborescence de navigation. La page Remote Logging Config apparaît.

> **REMARQUE** Si votre utilitaire de configuration ne comporte pas d'arborescence de navigation gauche, cliquez sur **Administration** puis sélectionnez l'option **Log**. Ensuite, faites défiler jusqu'à la section **Syslog** de la page. La présentation de la page peut être différente de l'illustration.



ÉTAPE 3 Dans le champ **Syslog Server**, saisissez le nom ou l'adresse IP du serveur syslog.

REMARQUE Si votre utilitaire de configuration comporte une case à cocher pour activer le syslog, cochez-la.

ÉTAPE 4 Cliquez sur **Apply** ou **Save Settings** pour enregistrer les paramètres.

ÉTAPE 5 Pour consulter les journaux, utilisez l'une des méthodes suivantes selon votre modèle.

- Dans un utilitaire de configuration comportant l'arborescence de navigation gauche, cliquez sur **Status** dans la barre de menus, puis sélectionnez successivement **View Logs > Policy Enforcement Logs** dans l'arborescence.
- Dans un utilitaire de configuration comportant la page **Administration > Log**, cliquez sur le bouton **View Log** en bas de page.

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

4

État et renouvellement de la licence

À l'aide de l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, vous pouvez consulter les informations sur l'état de votre licence ProtectLink et renouveler cette licence.

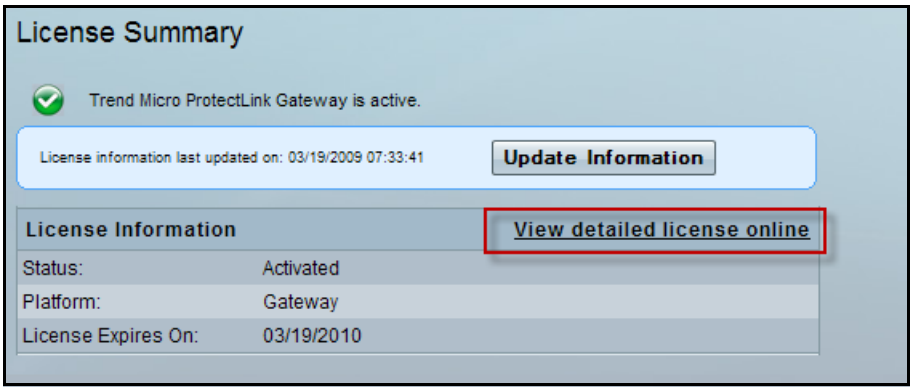
Consulter l'état de la licence

Pour consulter les informations concernant la licence :

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

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

REMARQUE Si votre utilitaire de configuration ne contient pas d'arborescence du côté gauche, cliquez sur **ProtectLink** puis choisissez **License** pour afficher le tableau concernant la licence. La présentation de la page peut être différente de l'illustration.



L'état de la licence est indiqué par l'icône d'état et le message d'état près du haut de la page.

- Cisco ProtectLink Service est actif.

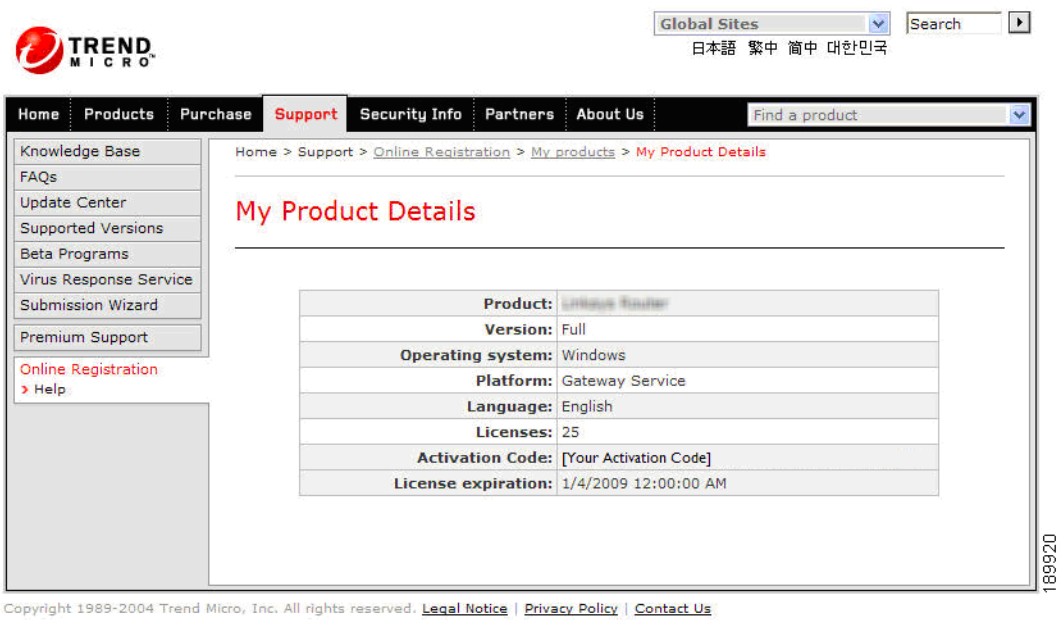
- Cisco ProtectLink Service expirera dans 30 jours.

- Cisco ProtectLink Service 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 web My Product Details apparaît.



Renouveler la licence

Pour renouveler une licence, qu'il s'agisse d'une licence de 12 mois achetée ou d'une licence d'essai de 30 jours, vous devez acheter une clé d'enregistrement (RK, Registration Key).

Une fois cette clé d'enregistrement obtenue, suivez les étapes ci-dessous pour obtenir un nouveau code d'activation (CA).

ÉTAPE 1 Ouvrez une session sur le routeur.

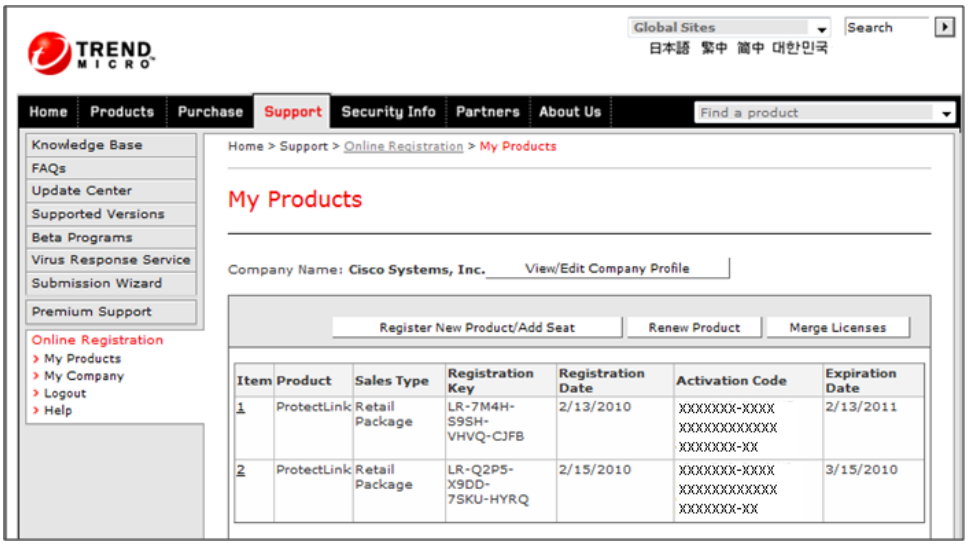
ÉTAPE 2 Cliquez sur l'onglet **ProtectLink**.

ÉTAPE 3 Cliquez sur l'onglet **License**.

ÉTAPE 4 Cliquez sur **Add a seat**.

ÉTAPE 5 Connectez-vous au serveur d'enregistrement TrendMicro à l'aide de votre ID utilisateur ProtectLink.

ÉTAPE 6 Au besoin, ouvrez la fenêtre My Products (Support > Online Registration > My Products).



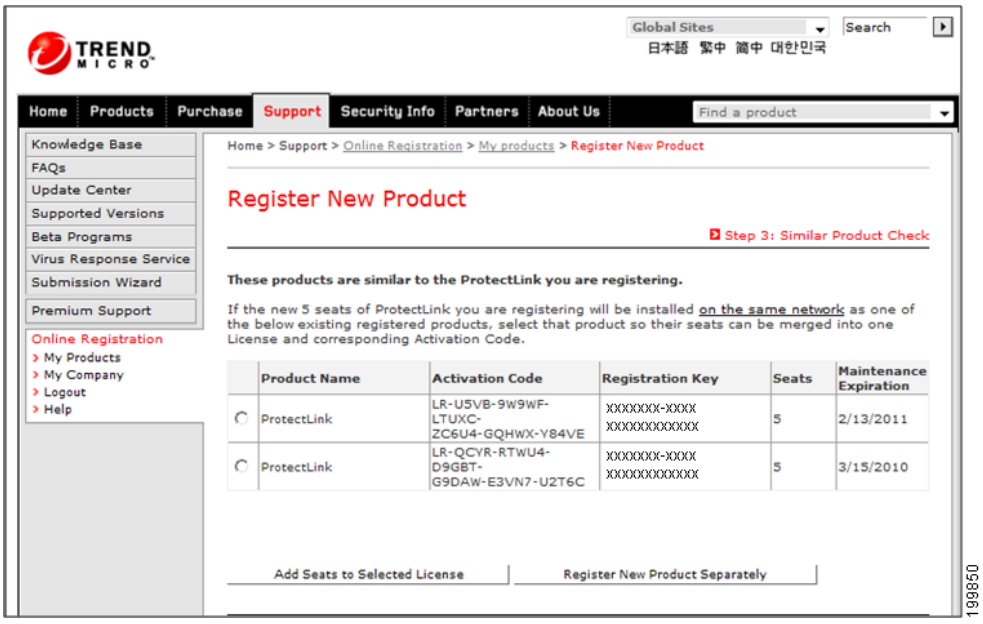
ÉTAPE 7 Cliquez sur **Register New Product/Add Seat**.

REMARQUE Ne cliquez *pas* sur **Renew Product**.

ÉTAPE 8 Saisissez la nouvelle RK (Registration Key, clé d'enregistrement) que Cisco vous a envoyée.

ÉTAPE 9 Cliquez sur **Next**.

ÉTAPE 10 Cliquez sur **Register New Product Separately**.



TrendMicro Registration Server génère un nouveau CA (code d'activation).

Une fois ce nouveau CA obtenu, suivez les étapes des sections suivantes pour renouveler la licence de votre routeur.

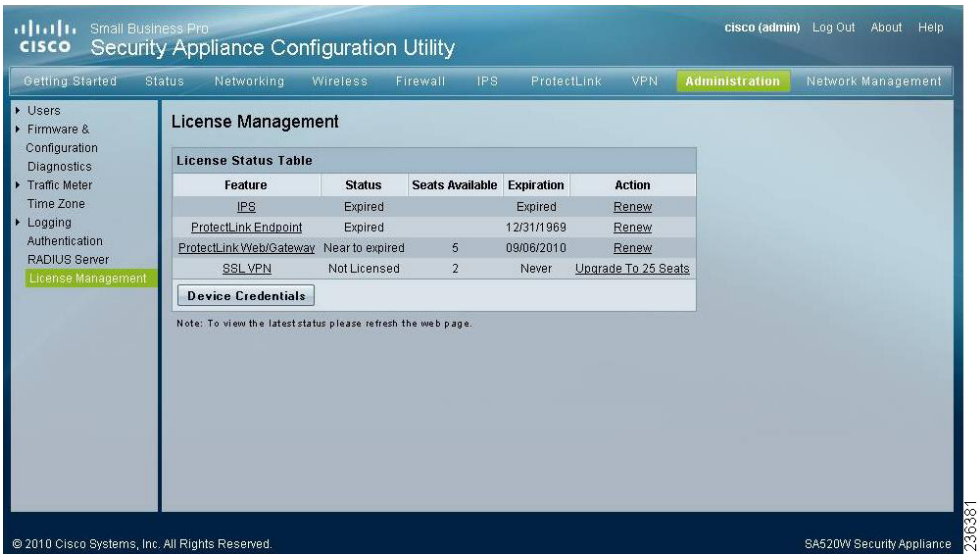
- **« Renouveler la licence des routeurs de la gamme SA 500 », page 47**
- **« Renouveler la licence des routeurs de la gamme RV », page 52**

Renouveler la licence des routeurs de la gamme SA 500

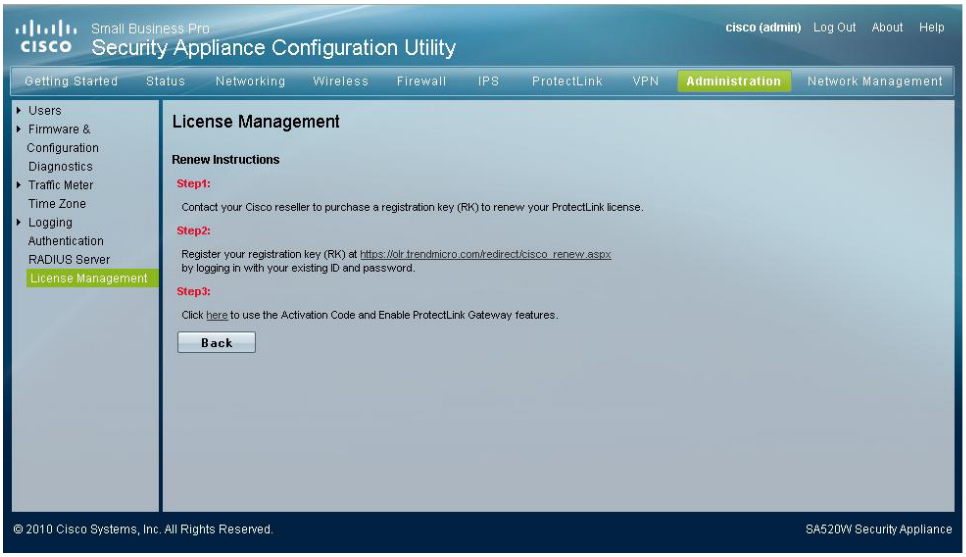
Pour renouveler la licence des routeurs de la gamme SA 500, suivez les étapes suivantes :

ÉTAPE 1 Connectez-vous à l'utilitaire de configuration du périphérique de sécurité SA500.

ÉTAPE 2 Cliquez sur **License Management** pour ouvrir la fenêtre permettant la gestion des licences.

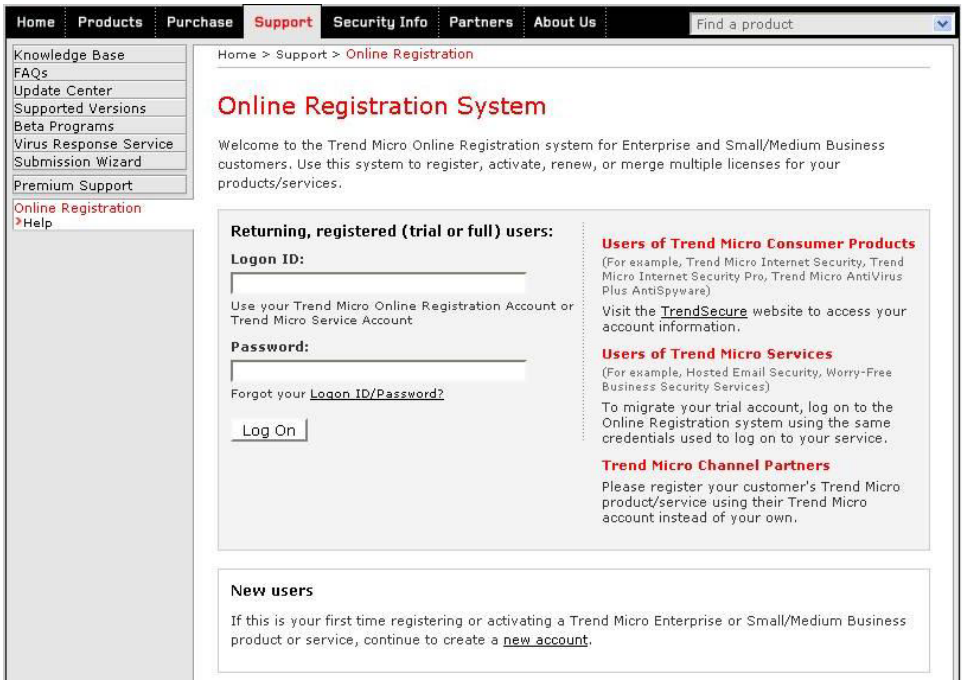


ÉTAPE 3 Dans la fenêtre License Management, cliquez sur le lien de l'étape 2 pour enregistrer votre clé d'enregistrement.

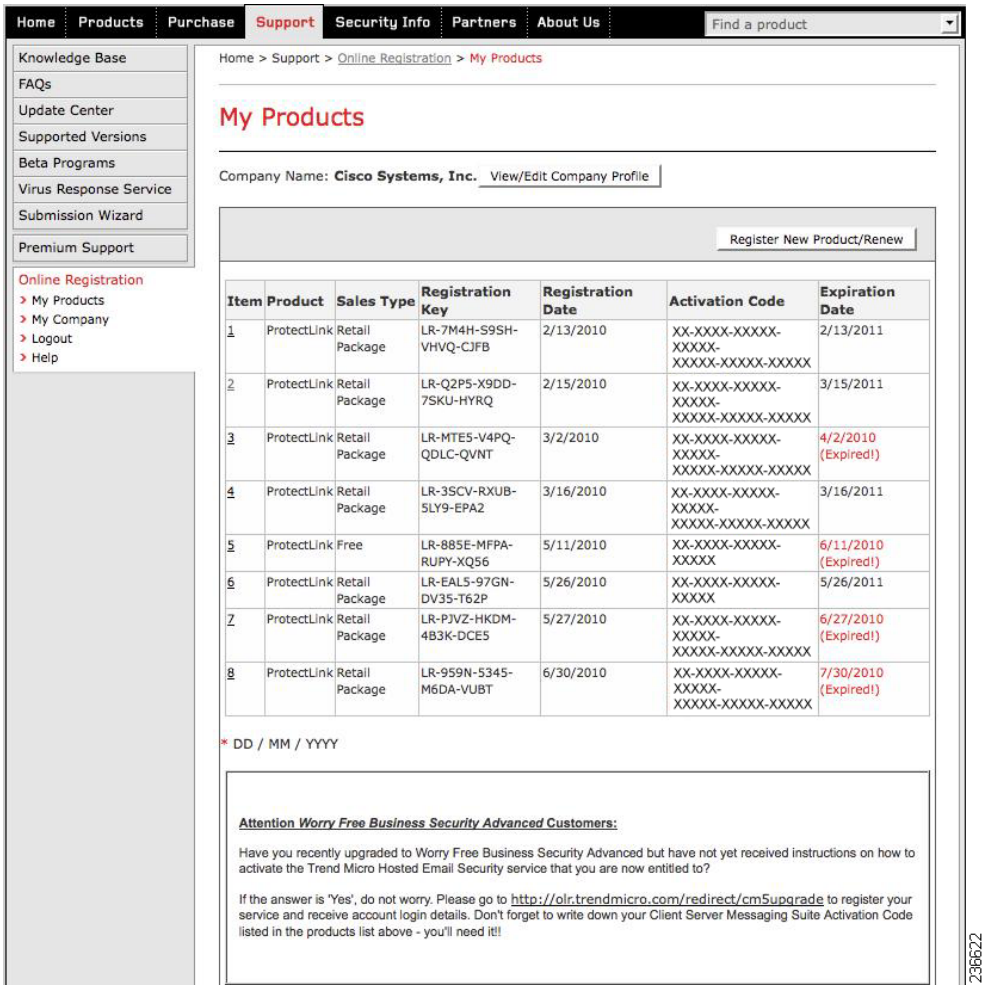


Ce lien ouvre la fenêtre ProtectLink Online Registration du site Web TrendMicro.

ÉTAPE 4 Dans la fenêtre Online Registration, connectez-vous avec votre compte ProtectLink existant.

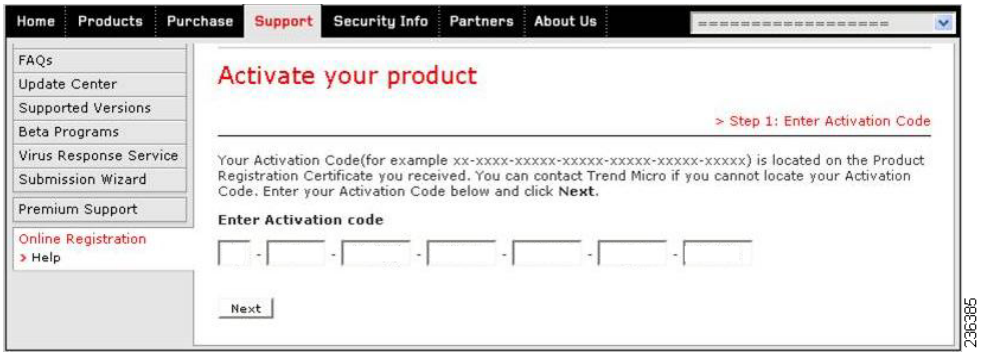


Une fois la connexion établie, une fenêtre semblable à la fenêtre suivante devrait apparaître :



REMARQUE Vous devez posséder un compte Trend distinct pour chaque périphérique.

ÉTAPE 5 Cliquez sur **Register New Product/Add Seat**.



ÉTAPE 6 Saisissez la nouvelle clé d'enregistrement et suivez les instructions en ligne.

ÉTAPE 7 Cliquez sur **Next**.

Une fois le processus d'enregistrement terminé, un code d'activation apparaît à l'écran. Vous recevez également un e-mail de TrendMicro contenant ce nouveau code d'activation. TrendMicro envoie l'e-mail à l'adresse associée à votre compte ProtectLink.

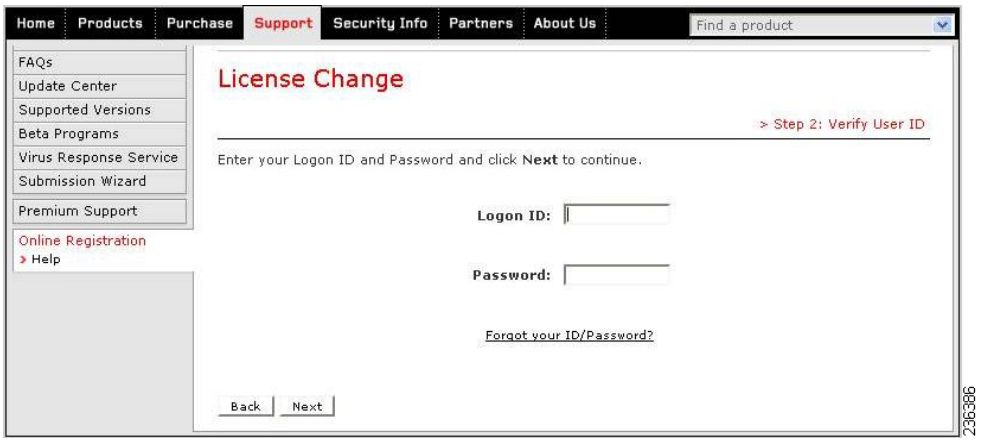
ÉTAPE 8 Après avoir obtenu le nouveau code d'activation, déconnectez-vous.

ÉTAPE 9 Retournez à la fenêtre License Management de l'utilitaire de configuration du SA500.

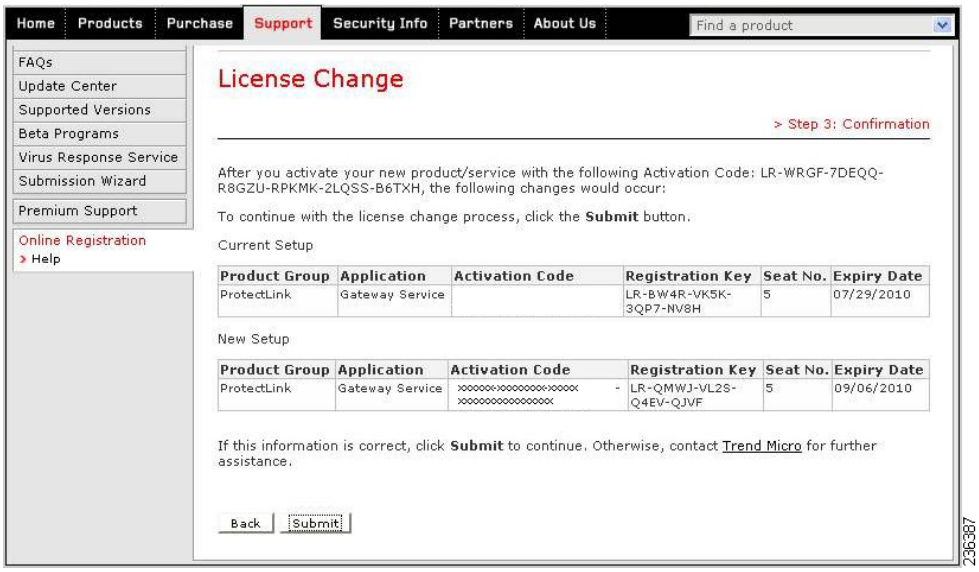
ÉTAPE 10 Dans la fenêtre License Management, cliquez sur le lien de l'étape 3 pour enregistrer votre clé d'enregistrement.

Ce lien permet d'ouvrir la fenêtre License Change du site Web ProtectLink.

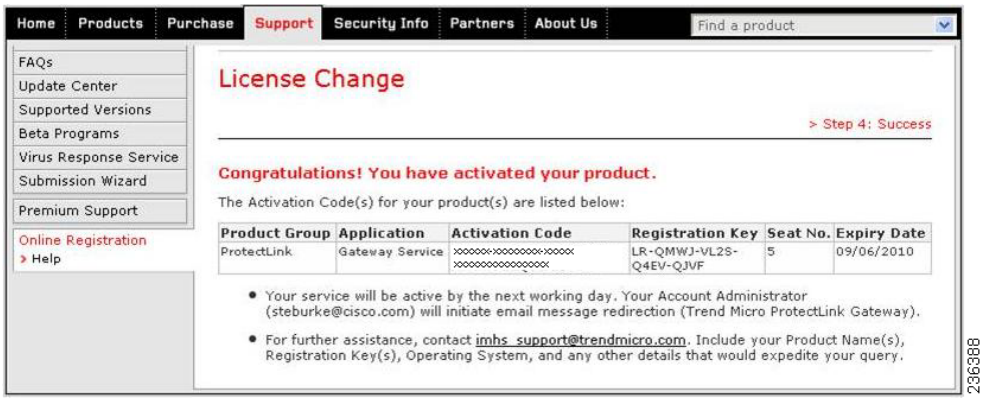
ÉTAPE 11 Dans la fenêtre de modification des licences, connectez-vous à l'aide des mêmes informations de connexion que celles utilisées pendant l'enregistrement.



ÉTAPE 12 Confirmez la nouvelle configuration puis, pour poursuivre le processus de modification de la licence, cliquez sur **Submit**.



Une fois l'enregistrement effectué, la fenêtre suivante apparaît :



Le périphérique SA500 détecte la nouvelle licence en quelques minutes.

REMARQUE Bien qu'il soit indiqué dans la fenêtre que le service ProtectLink sera activé le jour suivant, il ne faut en réalité que quelques minutes pour que TrendMicro active le service.

Renouveler la licence des routeurs de la gamme RV

Pour renouveler la licence des routeurs RVS4000, WRVS4400N et RV042/82/16, suivez les étapes suivantes.

ÉTAPE 1 Connectez-vous au routeur que vous souhaitez mettre à niveau :

REMARQUE Le routeur doit être configuré sur LAN pour pouvoir effectuer cette étape.

- Pour vous connecter à un routeur RVS4000 ou WRVS4400N, saisissez l'URL suivante dans le champ Adresse de votre navigateur :

  http://*router_address*/new_purchase.htm

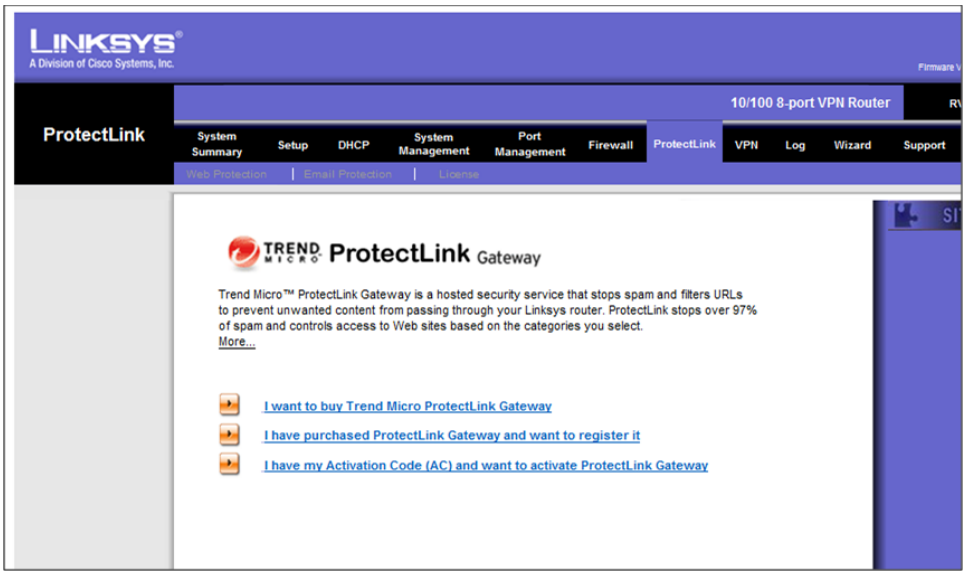
  Remplacez *router_address* par l'adresse de votre routeur (par exemple, 192.168.1.1).

- Pour vous connecter à un routeur RV042/82/16, saisissez l'URL suivante dans le champ Adresse de votre navigateur :

  http://*router_address*/Security_Protection_new_purchase.htm

  Remplacez *router_address* par l'adresse de votre routeur (par exemple, 192.168.1.1).

Une fenêtre de ce type apparaît :



ÉTAPE 2 Dans la fenêtre ProtectLink Home, cliquez sur **I have my Activation Code (AC) and want to activate ProtectLink Gateway** pour enregistrer le produit en ligne.

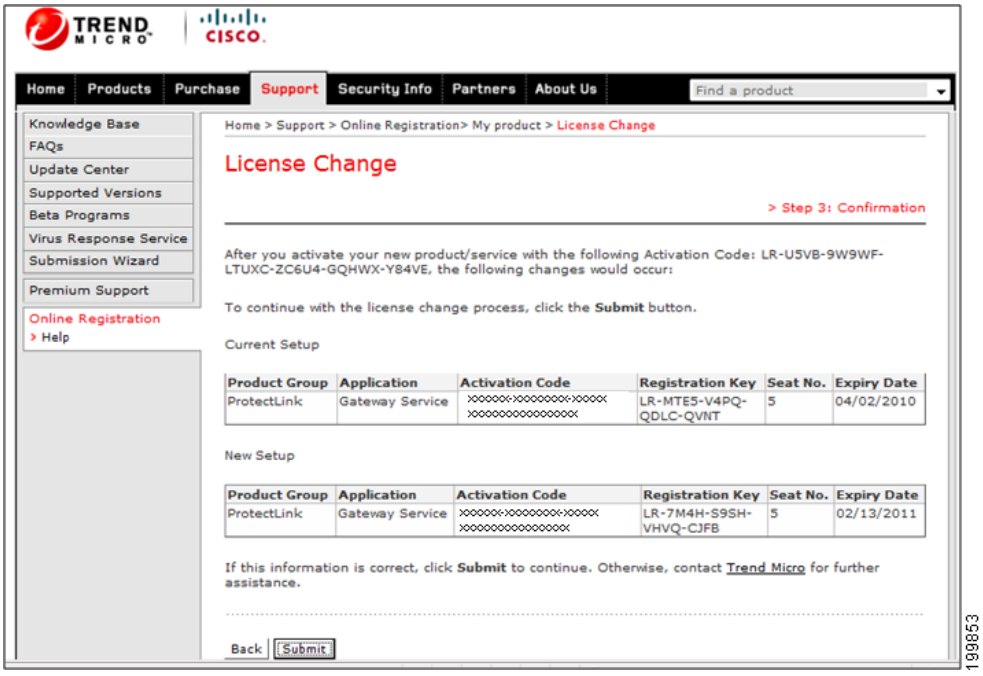
ÉTAPE 3 Saisissez le nouveau code d'activation puis cliquez sur **Next**.

ÉTAPE 4 Dans le champ Logon ID, saisissez votre ID utilisateur.

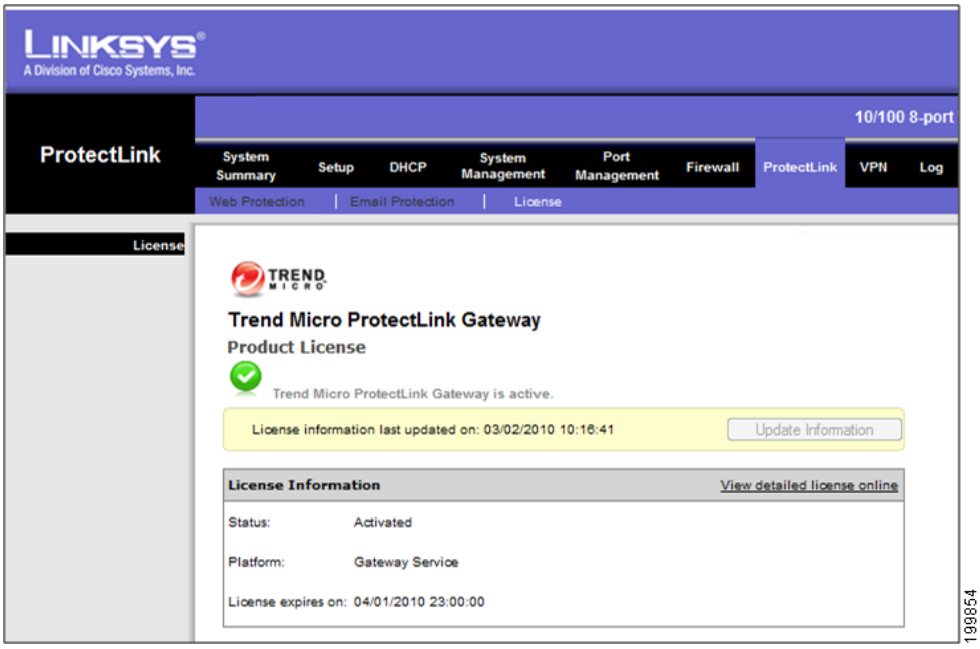
ÉTAPE 5 Dans le champ Password, saisissez votre mot de passe.

ÉTAPE 6 Cliquez sur **Next**.

ÉTAPE 7 Dans la fenêtre License Change, vérifiez votre configuration puis cliquez sur **Submit**.



ÉTAPE 8 Dans l'utilitaire de configuration du routeur, cliquez sur l'onglet **ProtectLink** et vérifiez l'état de la licence.



5

Configuration et gestion du système de protection de la messagerie

REMARQUE Ce chapitre concerne uniquement Cisco ProtectLink.

Utilisez le portail Web pour configurer et gérer la protection de la messagerie :

Lancement du portail Web pour la protection de la messagerie

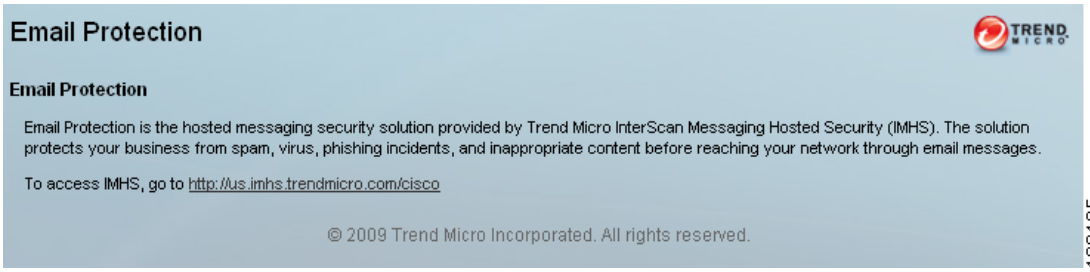
Depuis l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, lancez le portail Web de Trend Micro IMHS.

ÉTAPE 1 Lancez d'abord l'utilitaire de configuration de votre routeur ou de votre périphérique de sécurité, puis connectez-vous.

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

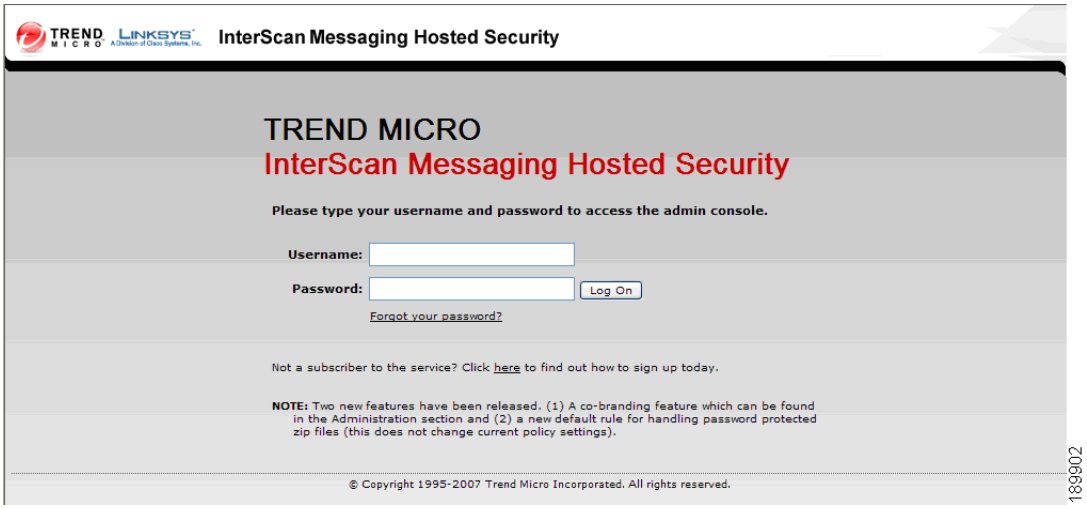
> **REMARQUE** Si votre utilitaire de configuration n'a pas de barre de navigation à gauche, cliquez sur **ProtectLink**, puis sélectionnez l'option **Email Protection**.

La page Email Protection apparaît.



ÉTAPE 3 Cliquez sur le lien affiché sur la page afin de lancer le portail Web de Trend Micro IMHS : https://us.imhs.trendmicro.com/cisco.

La page de connexion à Trend Micro IMHS apparaît.



ÉTAPE 4 Saisissez le nom d'utilisateur et le mot de passe reçus lors de l'activation de la passerelle Cisco ProtectLink, puis cliquez sur **Log On**.

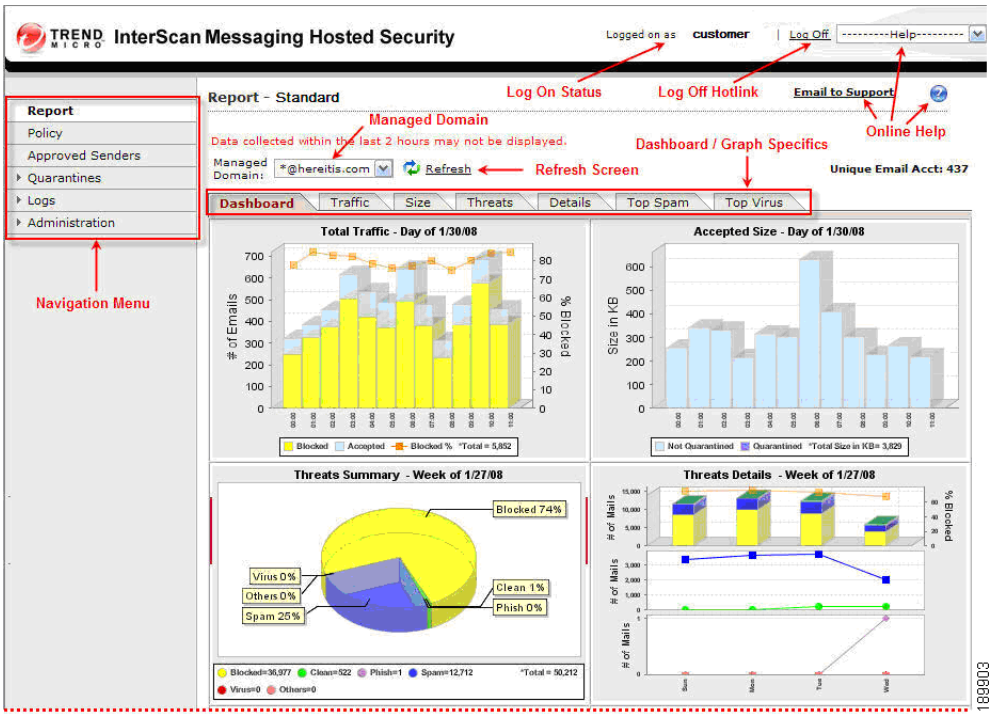
Le portail Web IMHS apparaît, et l'option **Report > Dashboard** s'affiche.

REMARQUE Après votre première connexion à IMHS, Cisco vous recommande de changer votre mot de passe afin de garantir la sécurité de votre compte IMHS. Pour obtenir plus d'informations, reportez-vous à la section **« Modification du mot de passe d'un utilisateur », page 76**.

Fonctionnalités du portail Web IMHS

Le portail Web IMHS permet de créer des rapports, de consulter des fichiers journaux, d'effectuer des tâches administratives et de modifier des politiques. La console est illustrée dans la **Figure 1**.

Figure 1 Portail Web IMHS



Sur la page affichée ci-dessus, l'interface utilisateur comprend les outils suivants :

- **Navigation Menu** : cliquez sur les éléments du menu Navigation Menu pour accéder aux pages de travail du portail Web IMHS. Lorsque vous cliquez sur les éléments de menus déroulants, ils s'ouvrent et affichent des éléments de sous-menus supplémentaires.
- **Dashboard / Tab Graph Specifics** : cliquez sur un graphique du tableau de bord ou de l'un des onglets pour afficher des détails sur l'action IMHS spécifique.
- **Managed Domain** : le domaine affiché sur le tableau de bord est le domaine actuel. Vous pouvez sélectionner un domaine différent dans le menu contextuel Managed Domain.
- **Online Help** : l'aide est disponible de trois manières, via le menu contextuel Online Help, via le bouton contextuel **?** et via le lien **Email to support email**. Vous pouvez télécharger les manuels IMHS et avoir accès aux autres outils d'aide via le menu contextuel Online Help.
- **Log On Status** : affiche le nom du compte connecté.
- **Log Off Link** : cliquez sur le lien **Log Off** pour vous déconnecter du portail Web IMHS.
- **Refresh page** : cliquez sur le lien **Refresh** pour actualiser la page.

REMARQUE Ce guide ne décrit pas en détail toutes les fonctionnalités de la protection de la messagerie de IMHS. Pour obtenir des informations détaillées, reportez-vous au guides *Trend Micro InterScan Gateway Hosted Security 1 Getting Started Guide* et *Trend Micro InterScan Gateway Hosted Security 1 End User Guide* disponibles à l'adresse :
www.trendmicro.com/download/.

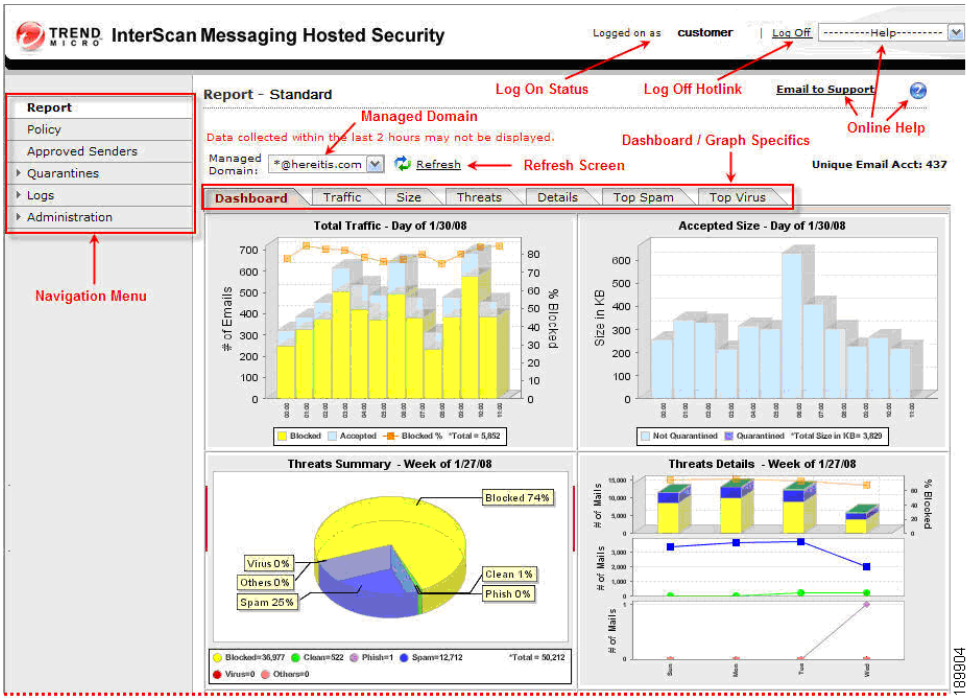
Affichage des rapports

Plusieurs rapports sont disponibles pour vous aider à analyser les résultats de la protection de messagerie.

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

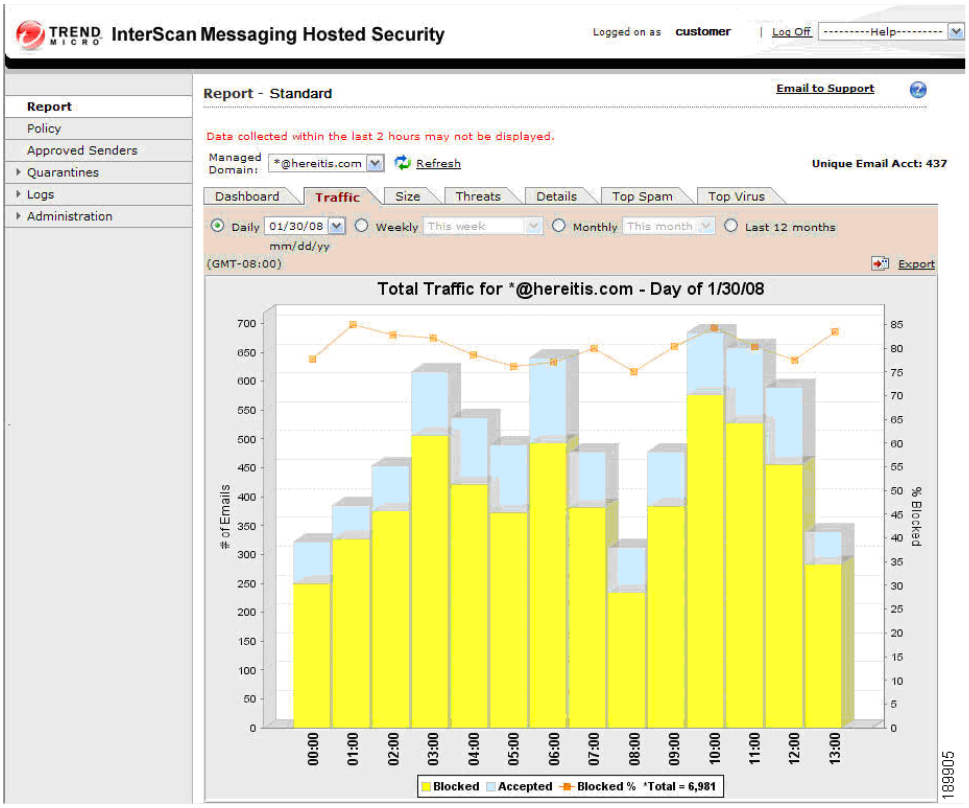
> **REMARQUE** Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

La page **Report > Dashboard** apparaît par défaut. Cette page est également accessible lorsque vous sélectionnez **Reports** dans le menu de navigation.



ÉTAPE 2 Pour obtenir des informations sur des actions IMHS spécifiques, cliquez sur l'onglet ou l'image appropriée sur la page Dashboard. Par exemple, cliquez sur l'image **Traffic** ou **Total Traffic** pour afficher des détails.

La page détaillée apparaît. Consultez l'exemple suivant de la page Total Traffic.



Le Tableau 1 décrit les graphiques de la page Dashboard et des onglets.

Tableau 1 Graphiques de la page Dashboard et des pages des onglets

Nom du graphique	Nom de l'onglet	Description
Total Traffic	Traffic	Affiche le trafic total (messages bloqués et messages acceptés) pour le domaine sélectionné.
Accepted Size	Size	Affiche la taille totale (en Ko) du trafic de messages acceptés pour le domaine sélectionné.
Threats Summary	Threats	Affiche le pourcentage des types de messages spécifiques qui composent le trafic de messagerie du domaine sélectionné.
Threats Details	Details	Affiche les détails de la distribution du trafic de messagerie du domaine de messagerie sélectionné.
Top Spam Recipients	Top Spam	Affiche les destinataires recevant le plus de courrier indésirable pour le domaine de messagerie sélectionné.
Top Virus Recipients	Top Virus	Affiche les destinataires recevant le plus de messages infectés par des virus pour le domaine de messagerie sélectionné.

Utilisation des politiques

Une politique IMHS est un ensemble de règles défini pour un domaine de messagerie existant. Plusieurs règles peuvent exister pour chaque domaine (politique), mais une seule et unique politique peut exister pour un domaine particulier. Les politiques prédéfinies régissant votre système de protection de messagerie sont accessibles dans le menu Policy.

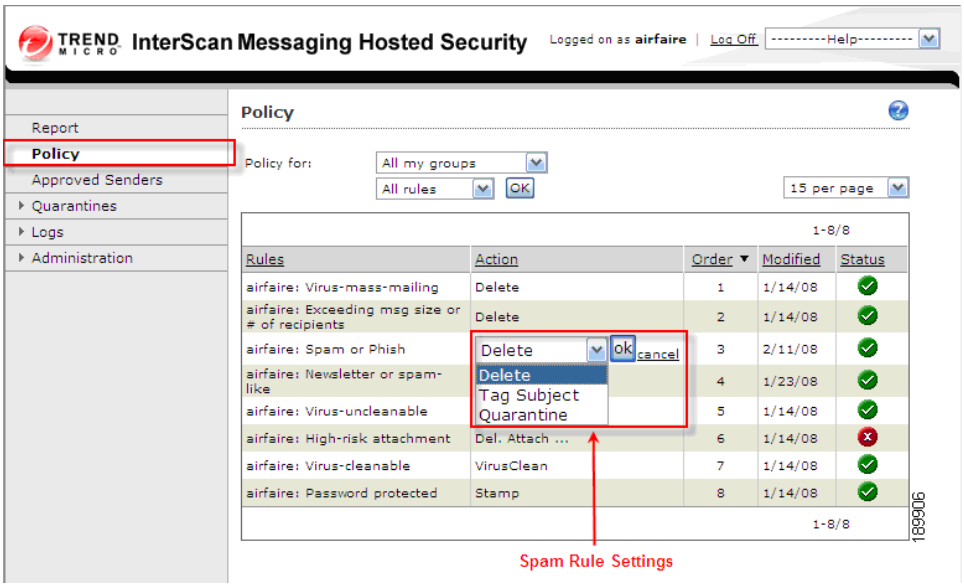
ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Policies** dans le menu de navigation.

La page Policy apparaît et affiche une liste des règles prédéfinies ainsi que leur état.

Figure 2 Paramètres de politique IMHS / Règles concernant le courrier indésirable



REMARQUE Les administrateurs sont autorisés à consulter les règles qui s'appliquent à leur organisation. Les clients ProtectLink ont un accès en lecture seule. Ils peuvent consulter la politique par défaut et modifier les règles « courrier indésirable ou phishing » et « bulletin d'information ou semblable à du courrier indésirable ». L'administrateur peut modifier l'action par défaut prise sur les messages identifiés comme courrier indésirable ; il peut sélectionner l'option Delete, Tag Subject ou Quarantine, tel qu'illustré dans le menu contextuel de configuration des paramètres concernant le courrier indésirable.

ÉTAPE 3 Utilisez les fonctions suivantes, selon vos besoins :

- A l'aide des en-têtes de colonne, modifiez l'ordre de tri. Les règles sont répertoriées dans un tableau et triées dans l'ordre selon lequel elles s'appliquent lors de l'analyse effectuée par IMHS. Vous pouvez changer l'ordre de tri de chaque tableau, en cliquant sur un en-tête de colonne. Si vous souhaitez modifier l'ordre des informations dans le tableau, cliquez sur l'un des en-têtes de colonne. Les informations sont triées selon un ordre croissant.
- Reportez-vous aux icônes de la colonne Status pour connaître l'état d'une règle.

Icône	État
	Règle activée
	Règle désactivée

Les paramètres de la politique par défaut de ProtectLink (IMHS Standard) sont répertoriés dans le **Tableau 2**.

Tableau 2 Paramètres de la politique par défaut du service standard

Règle	Description
Règle 1	Cette règle sert à protéger l'utilisateur contre les virus diffusés lors de campagnes utilisant des listes de diffusion. Si un message est identifié comme contenant un virus ne pouvant être effacé et que le message affiche un comportement de publipostage, le message est effacé dans sa totalité, virus compris.
Règle 2 : Exceeding message size or allowed number of recipients.	Cette règle sert à protéger le système contre les attaques de Déni de service (DOS) et les bombes de compression. Si la taille du message entrant dépasse la limite par défaut de 10 Mo ou que celui-ci a été envoyé à plus de 50 destinataires au sein de l'organisation, le message est supprimé.
Règle 3 : Spam or Phish	Cette règle sert à attraper les courriers indésirables ou les messages d'hameçonnage. L'action par défaut consiste à supprimer tous les messages identifiés comme courrier indésirable ou tentative d'hameçonnage. Tous les clients IMHS ont la possibilité de modifier l'action par défaut. Il est vivement recommandé de n'utiliser que les actions Delete ou Quarantine pour cette règle. Tous les messages mis en quarantaine sont conservés pendant sept jours dans l'espace réservé à la quarantaine accessible par Web d'IMHS.
Règle 4 : Virus-uncleanable	Cette règle sert à protéger l'utilisateur des virus. Si un message est identifié comme contenant un virus ne pouvant être effacé, la pièce jointe infectée est supprimée du message avant sa livraison.
Règle 5 : High-risk attachment	Désactivée pour les clients standard.

Tableau 2 Paramètres de la politique par défaut du service standard (suite)

Règle (suite)	Description (suite)
Règle 6 : Virus-cleanable	Cette règle sert à protéger l'utilisateur des virus. Si un message est identifié comme contenant un virus pouvant être effacé, le virus est supprimé du message avant sa livraison. Si la procédure de nettoyage du virus échoue, la pièce jointe infectée est supprimée.
Règle 7 : Newsletter or spam-like	Cette règle sert à attraper les messages qui ne sont pas forcément indésirables pour tous les utilisateurs, tels que les bulletins d'informations. L'action par défaut pour ces messages ressemblant à du courrier indésirable consiste à les marquer (Tag Subject) en tant que Spam. Il est vivement recommandé de n'utiliser que les actions Tag Subject ou Quarantine pour cette règle. Tous les messages mis en quarantaine sont conservés pendant sept jours dans l'espace réservé à la quarantaine accessible par Web d'IMHS.
Règle 8 : Password-protected zipped file attachments	Cette règle sert à autoriser les utilisateurs expérimentés à configurer l'action prise pour les messages qui comportent en pièce jointe des fichiers compressés protégés par mot de passe. Par défaut, ce type de message est transféré au destinataire, et une notification est ajoutée au corps du message, pour indiquer que le fichier joint n'a pas été vérifié.

Gestion des expéditeurs approuvés

Pour chaque domaine que vous gérez, vous pouvez définir des expéditeurs approuvés (adresses de messagerie ou domaines). Les messages reçus de ces expéditeurs approuvés ne seront pas sujets à toutes les vérifications normalement effectuées sur les messages entrants.

- ERS ne bloquera aucun message provenant d'expéditeurs (ou de domaines) spécifiés.
- Les règles heuristiques qui concernent le courrier indésirable d'après le contenu du message, ne s'appliqueront pas aux messages reçus de ces expéditeurs ou domaines spécifiés.
- Les règles concernant les virus, le contenu et les pièces jointes s'appliqueront.

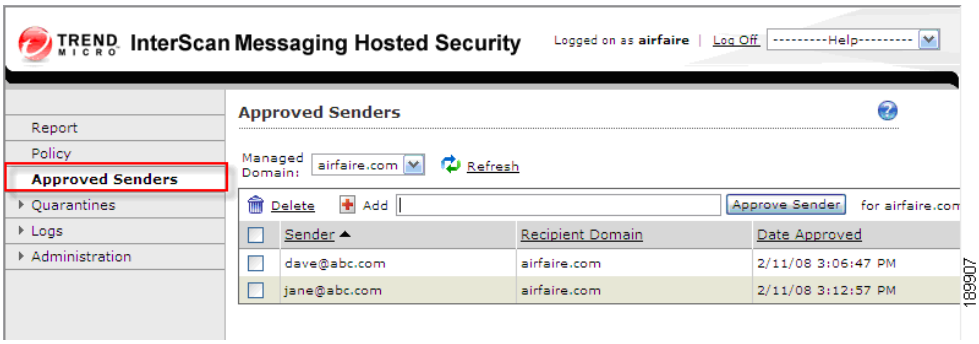
Pour gérer les expéditeurs approuvés, suivez les étapes suivantes :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Approved Senders** dans le menu de navigation.

La page Approved Senders apparaît.



ÉTAPE 3 Pour afficher les expéditeurs approuvés d'un domaine géré différent, procédez au tâches suivantes :

a. Dans la liste Managed Domain, sélectionnez un domaine particulier que vous gérez ou sélectionnez l'option **All Domains** pour afficher les expéditeurs approuvés de tous les domaines.

b. Cliquez sur **Refresh** pour afficher les expéditeurs approuvés du domaine sélectionné.

ÉTAPE 4 Pour ajouter un expéditeur, effectuez les tâches suivantes :

a. Dans la liste Managed Domain, choisissez d'approuver cet expéditeur pour un domaine particulier ou pour tous les domaines ; dans ce dernier cas, sélectionnez l'option **All Domains**.

b. Cliquez dans la zone **Add**, puis saisissez une adresse électronique (au format *utilisateur@domaine.com*) ou saisissez un domaine (par exemple *domaine.com*).

c. Cliquez sur **Approve Sender** pour ajouter l'expéditeur à la liste.

ÉTAPE 5 Pour modifier une entrée, effectuez les actions suivantes :

a. Cliquez sur l'entrée.

b. Modifiez le texte.

c. Cliquez sur **OK**.

ÉTAPE 6 Pour supprimer une entrée, effectuez les actions suivantes :

a. Cochez la case de l'entrée.

b. Cliquez sur **Delete**.

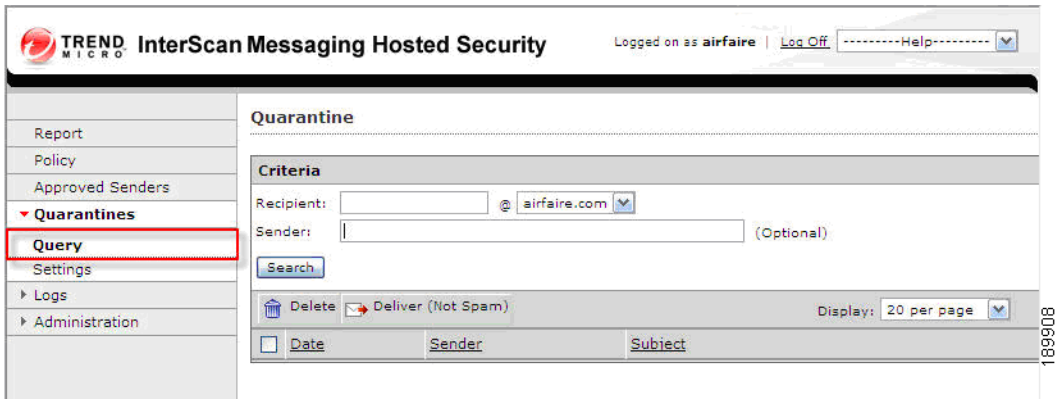
Gestion des messages mis en quarantaine

Vous pouvez rechercher les messages mis en quarantaine d'un destinataire, d'un expéditeur ou d'un domaine spécifique, à l'aide de critères de recherche. Ensuite, choisissez l'action à effectuer : supprimer les messages ou les libérer de la quarantaine.

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Quarantines** dans le menu de navigation, puis sur **Query**.



ÉTAPE 3 Saisissez des critères de recherche.

- **Recipient (obligatoire)** : saisissez le nom d'utilisateur de messagerie du destinataire. Par exemple, si l'adresse complète est *utilisateur@domaine.com*, vous devez saisir *utilisateur*.
- **Domain (non étiqueté)** : choisissez le domaine dans la liste déroulante.
- **Sender (facultatif)** : saisissez l'adresse complète ou le domaine de l'expéditeur.
- **Display** : sélectionnez le nombre de messages à afficher par page. Pour un affichage plus rapide, choisissez un nombre de messages plus petit sur chaque page. Des boutons vous permettent de vous déplacer d'une page à l'autre.

ÉTAPE 4 Cliquez sur **Search**.

Les résultats apparaissent sous forme de tableau. Les informations comprennent la date, le nom de l'expéditeur et l'objet du message. Vous pouvez modifier l'ordre de tri en cliquant sur un en-tête de colonne. Les résultats seront triés dans l'ordre croissant en fonction de l'en-tête sélectionné.

ÉTAPE 5 Pour supprimer des messages, effectuez les actions suivantes :

a. Pour chaque message à supprimer, cochez la case correspondante dans la première colonne.
—Ou— Sélectionnez tous les messages de la page en cochant la case située dans l'en-tête de la première colonne.

b. Cliquez sur le bouton **Delete** situé au-dessus du tableau. Tous les messages sélectionnés seront supprimés.

c. Répétez ces actions pour toutes les autres pages, le cas échéant.

ÉTAPE 6 Pour libérer un élément de la quarantaine, effectuez les actions suivantes :

a. Pour chaque message à libérer, cochez la case correspondante dans la première colonne.
—Ou— Sélectionnez tous les messages de la page en cochant la case située dans l'en-tête de la première colonne.

b. Cliquez sur le bouton **Deliver (Not Spam)** au-dessus du tableau.

> **REMARQUE** Lorsqu'un message est libéré de la quarantaine, IMHS traite la demande mais n'applique pas les critères relatifs au courrier indésirable. Le message est ensuite envoyé. Sachez cependant qu'un message peut être bloqué par le serveur de réception de messagerie, en fonction des politiques de sécurité appliquées. IMHS n'a aucun contrôle sur ces politiques. Dans un tel cas, le message ne sera pas remis dans la boîte de réception du destinataire.

c. Répétez ces actions pour toutes les autres pages, le cas échéant.

Configuration du message récapitulatif concernant la quarantaine

Configurez IMHS de sorte qu'il envoie un message récapitulatif à chaque destinataire dont des messages ont été mis en quarantaine. Vous pouvez choisir la fréquence, le jour de la semaine et l'heure d'envoi de ce message. Vous pouvez également définir le contenu du message. Le message récapitulatif peut répertorier jusqu'à 100 messages mis en quarantaine, et fournit au destinataire un lien permettant d'avoir accès aux messages.

Un message récapitulatif est envoyé uniquement si la fonction est activée.

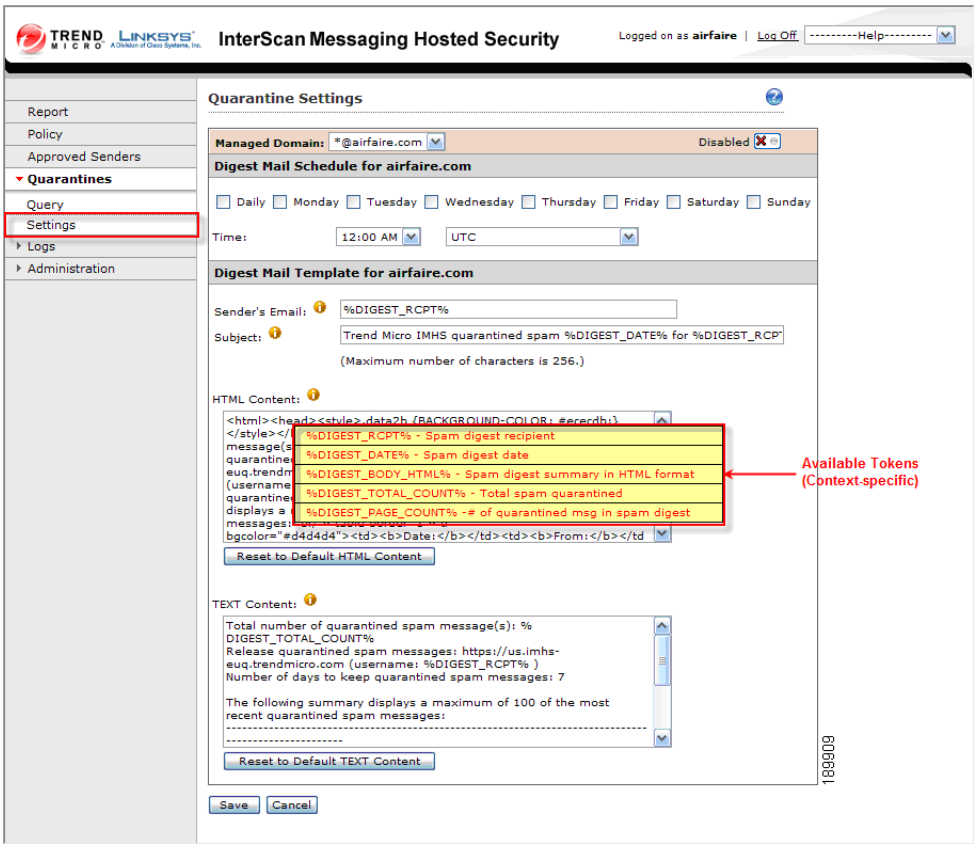
Pour configurer le message récapitulatif :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Quarantines** dans le menu de navigation, puis sur **Settings**.

La fenêtre Quarantine Settings apparaît.



REMARQUE Tel qu'illustré en jaune, vous pouvez cliquer avec le bouton droit de la souris sur n'importe quel champ de la zone Digest Mail Template pour afficher les jetons disponibles. Les jetons sont des codes servant à insérer des informations telles que l'adresse électronique du destinataire, la date du message récapitulatif et d'autres informations. La procédure pas à pas ci-dessous fournit davantage d'informations.

ÉTAPE 3 Pour activer cette fonctionnalité, cliquez sur l'icône **Disabled** située dans le coin supérieur droit de la page. L'étiquette du bouton se change en **Enabled**. Pour désactiver la fonctionnalité, cliquez à nouveau sur le bouton (par défaut, cette fonction est désactivée).

ÉTAPE 4 Dans la liste déroulante **Managed Domain**, sélectionnez le domaine pour lequel le message récapitulatif va être créé.

REMARQUE Le domaine utilisé dans l'adresse électronique de l'expéditeur doit être identique à celui auquel le message va être livré.

ÉTAPE 5 Sélectionnez la fréquence d'envoi du message récapitulatif en cochant l'option **Daily** ou les cases des jours de la semaine souhaités.

REMARQUE Les messages mis en quarantaine sont conservés pendant sept jours.

ÉTAPE 6 Sélectionnez des valeurs dans les champs **Time** et **Time Zone** pour définir quand le message récapitulatif doit être envoyé.

ÉTAPE 7 Saisissez les informations suivantes pour configurer le message qui va être envoyé :

REMARQUE Pour saisir un jeton dans un champ, cliquez d'abord sur le champ pour placer le curseur au point d'insertion. Puis cliquez avec le bouton droit à cet endroit pour afficher la liste des codes pouvant être utilisés. Pour insérer un code, cliquez dessus dans la liste.

- **Sender's Email** : saisissez l'adresse électronique à afficher dans l'en-tête comme expéditeur du message.

  REMARQUE L'entrée par défaut est le code `%DIGEST_RCPT%`, qui insère automatiquement l'adresse du destinataire dans la ligne « De » du message.

- **Subject** : saisissez le texte qui apparaît dans la ligne Objet du message récapitulatif.

  REMARQUE L'entrée par défaut est *Trend Micro IMHS quarantined spam*, avec le code `%DIGEST_DATE%` pour insérer la date du message et le code `%DIGEST_RCPT%` pour insérer automatiquement l'adresse du destinataire dans la ligne « De » du message.

- **HTML Content** : saisissez le corps du message HTML, pour les utilisateurs qui peuvent recevoir des messages au format HTML.

  REMARQUE Le contenu par défaut comprend des balises de mise en forme, que vous pouvez modifier si vous avez des connaissances en HTML. Le contenu de ce message est identique au contenu par défaut de la zone TEXT Content. Le message comprend le nombre total de messages mis en quarantaine à l'aide du code `%DIGEST_TOTAL_COUNT%`. Il contient aussi un lien qui permet à l'utilisateur de se connecter à la page de connexion IMHS Web EUQ. Une fois connecté avec le nom d'utilisateur et le mot de passe affectés, l'utilisateur peut consulter les messages et spécifier quels messages il souhaite libérer de la quarantaine.

- **TEXT Content** : saisissez le message au format texte brut, sans balises de mise en forme HTML, pour les utilisateurs qui ne peuvent pas recevoir de messages au format HTML.

ÉTAPE 8 Cliquez sur **Save**, pour enregistrer vos modifications.

Utilisation des journaux de suivi de la messagerie

Utilisez la section Logs > Mail Tracking pour rechercher et consulter les journaux de suivi de la messagerie, en fonction d'une date, d'une période, d'un expéditeur ou d'un destinataire spécifique. Les informations de suivi de la messagerie sont uniquement disponibles pour les cinq jours précédents.

La fonctionnalité de suivi de la messagerie vous permet de rechercher dans le système tout message, à l'aide des informations d'identification du destinataire et de l'expéditeur. Cette fonctionnalité affiche l'état du message et l'action prise le concernant, par exemple :

- Bloqué ou retardé par le système à l'aide d'un service de réputation
- Accepté pour le traitement et supprimé avec un virus
- Accepté, traité et livré
- Non résolu

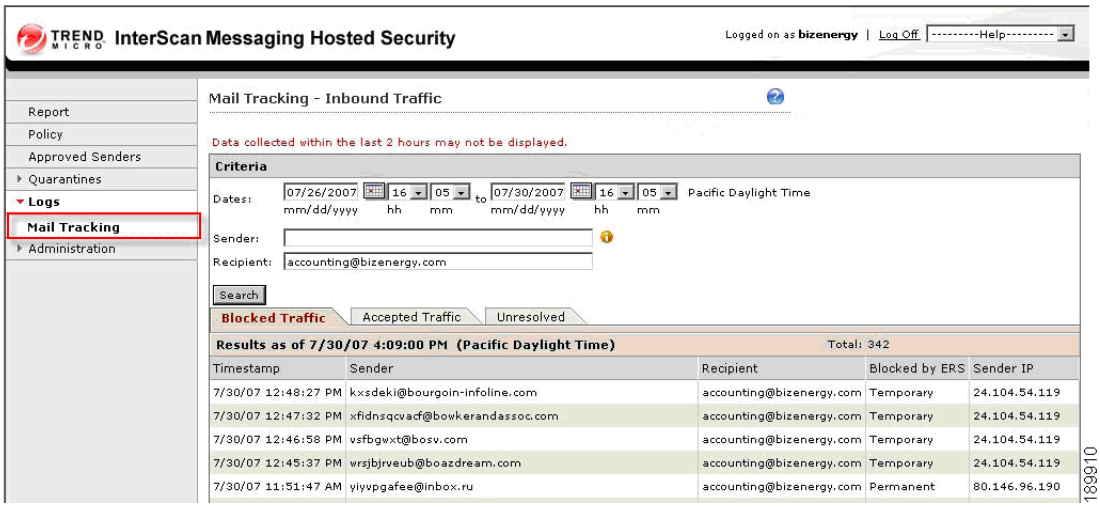
Pour afficher les journaux de suivi de la messagerie :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Mail Tracking** dans le menu de navigation.

La page Mail Tracking - Inbound Traffic apparaît.



ÉTAPE 3 Saisissez les critères des journaux que vous voulez consulter :

- **Dates** : passez de la gauche vers la droite pour sélectionner un début et une fin de période. Cliquez sur le bouton du calendrier pour choisir une date. Utilisez la liste déroulante **hh** pour choisir une heure (de 0 à 23) et la liste déroulante **mm** pour définir les minutes (de 0 à 59). Le fuseau horaire affiché dépend des paramètres régionaux de votre ordinateur.
- **Recipient** : saisissez le nom d'utilisateur de messagerie du destinataire. Par exemple, si l'adresse complète est *utilisateur@domaine.com*, vous devez saisir *utilisateur*.
- **Sender (facultatif)** : saisissez l'adresse complète ou le domaine de l'expéditeur.

ÉTAPE 4 Cliquez sur **Search**.

Les résultats apparaissent.

ÉTAPE 5 Cliquez sur un onglet pour choisir le type de messages à afficher : **Blocked Traffic**, **Accepted Traffic** ou **Unresolved**.

Tâches d'administration de la console IMHS

Cette section couvre les tâches suivantes :

- **Gestion des mots de passe, page 74**
- **Importation de répertoires d'utilisateurs, page 77**
- **Co-marquage pour l'affichage d'un logo d'entreprise sur le portail Web, page 79**

Gestion des mots de passe

Les administrateurs peuvent modifier les mots de passe administrateurs et les mots de passe des utilisateurs finaux.

Tous les mots de passe IMHS doivent comporter entre 8 et 32 caractères. Cisco recommande fortement d'utiliser des mots de passe qui satisfont aux critères suivants :

- Inclure différents types de caractères (une combinaison de lettres, chiffres et autres caractères).
- Ne pas utiliser de formats facilement identifiables (comme votre date d'anniversaire, numéro de permis de conduire ou numéro d'employé).

Reportez-vous aux rubriques suivantes :

- **Gestion du mot de passe administrateur, page 75**
- **Modification du mot de passe d'un utilisateur, page 76**

Gestion du mot de passe administrateur

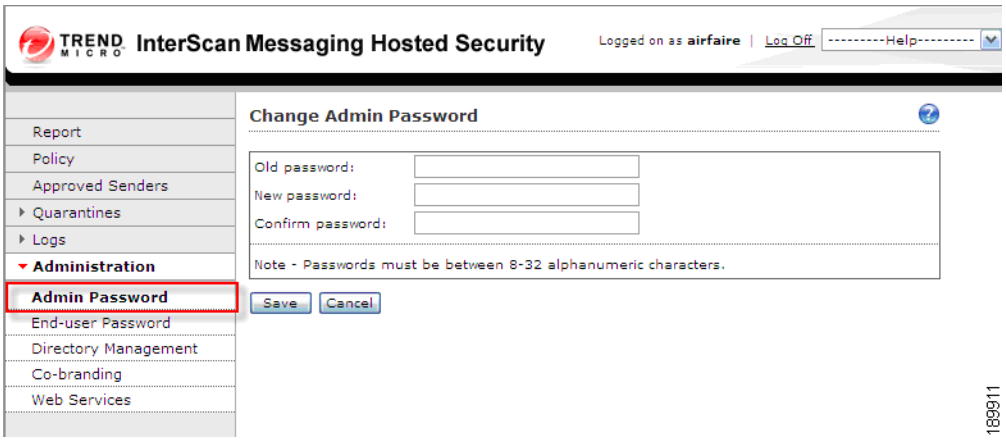
Pour modifier le mot de passe de l'administrateur, suivez ces étapes :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Administration** dans le menu de navigation, puis sur **Admin Password**.

La page Change Admin Password apparaît.



ÉTAPE 3 Saisissez les informations suivantes :

- **Old Password** : saisissez votre mot de passe actuel.
- **New password** : saisissez un mot de passe comprenant entre 8 et 32 caractères.
- **Confirm password** : saisissez de nouveau le nouveau mot de passe.

ÉTAPE 4 Cliquez sur **Save**.

Modification du mot de passe d'un utilisateur

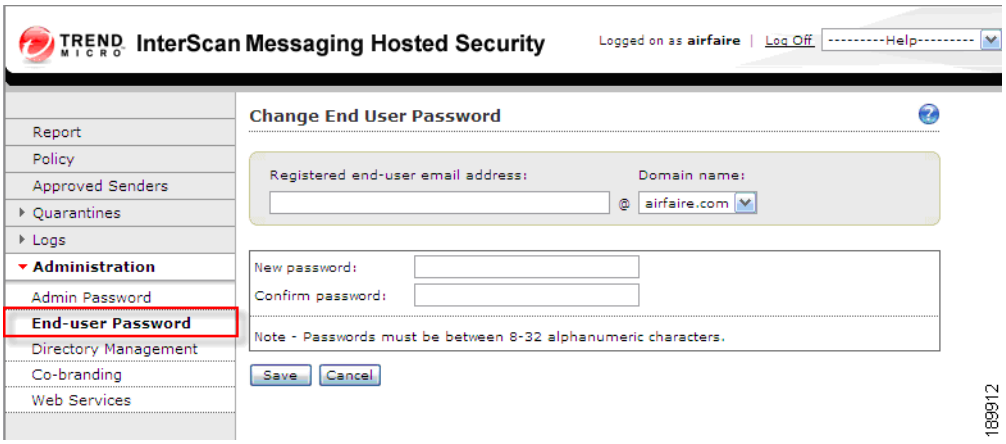
Pour redéfinir le mot de passe d'un utilisateur, suivez ces étapes :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Administration** dans le menu de navigation, puis sur **End-user Password**.

La page Change End User Password apparaît.



ÉTAPE 3 Saisissez les informations suivantes :

- **Registered end-user's email address** : saisissez la première partie de l'adresse électronique. Par exemple, si l'adresse est *utilisateur@domaine.com*, saisissez *utilisateur*.
- **New password** : saisissez un mot de passe comprenant entre 8 et 32 caractères.
- **Confirm password** : saisissez de nouveau le nouveau mot de passe.

REMARQUE L'utilisateur final doit être informé du nouveau mot de passe afin de se connecter. Le système envoie à l'utilisateur final un message avec un lien d'activation.

Importation de répertoires d'utilisateurs

L'importation de répertoires d'utilisateurs dans IMHS peut aider à prévenir les attaques par courrier indésirable qui consistent à envoyer des messages vers des adresses non valides de votre domaine. Par exemple, dans une attaque de répertoire Directory Harvest Attack (DHA), un expéditeur de courrier indésirable envoie des messages à tous les noms d'utilisateur possibles sur un domaine. Lorsque le serveur renvoie des notifications de non-remise pour les adresses non valides, les expéditeurs de courrier indésirable peuvent déduire quelles adresses électroniques sont valides et les utiliser pour de futures attaques.

L'importation de répertoires utilisateur permet à IMHS de connaître les adresses électroniques et les domaines légitimes de votre organisation. IMHS ne transmettra pas de messages à des adresses non valides.

Il est possible d'importer des fichiers de répertoire aux formats suivants :

- LDAP Data Interchange Format (LDIF: .ldf).
- Comma-separated Values (CSV: .csv).

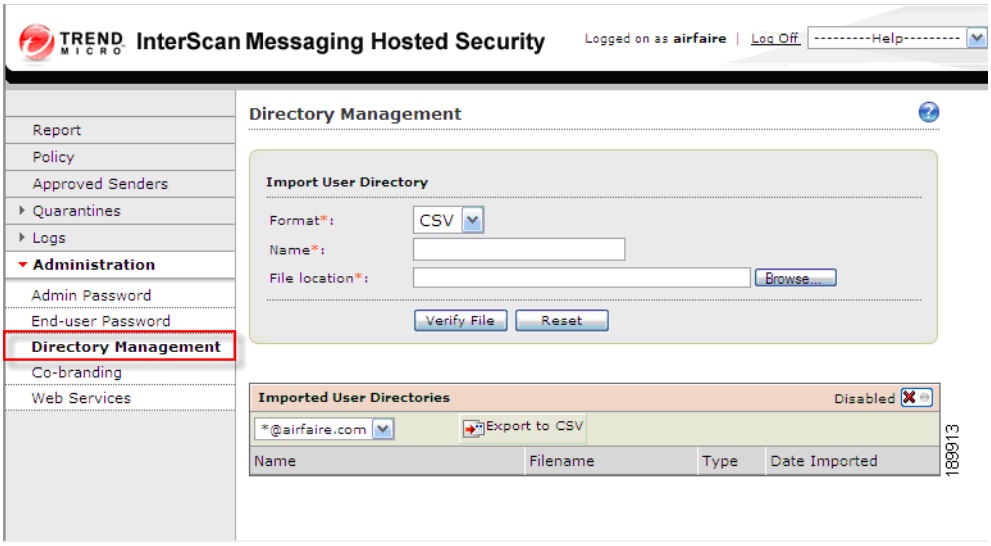
Pour importer un fichier de répertoire utilisateur, suivez ces étapes :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

> **REMARQUE** Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Administration** dans le menu de navigation, puis sur **Directory Management**.

La page Directory Management apparaît.



Cette page comporte deux sections :

- **Import User Directory** : permet de sélectionner un nouveau fichier de répertoire utilisateur à importer.
- **Imported User Directories** : présente les fichiers de répertoire utilisateur actuellement utilisés par IMHS. IMHS remplace un seul domaine de messagerie utilisateur à la fois. Les utilisateurs peuvent être une combinaison de plusieurs répertoires.

ÉTAPE 3 Dans la section **Import User Directory**, saisissez les informations suivantes sur le répertoire à importer :

- **Format** : sélectionnez le format: **LDIF** ou **CSV**.
- **Name :** saisissez un nom descriptif pour le fichier.
- **File location** : cliquez sur **Browse** et choisissez le fichier sur votre ordinateur.

ÉTAPE 4 Cliquez sur **Verify File**.

Une fois la barre de progression complétée, une page récapitulative apparaît et les informations suivantes s'affichent :

- **Summary** : récapitulatif des informations saisies.
- **Domains and Number of Current Users to Replace Current Users** : les domaines spécifiés lors de l'abonnement au service IMHS.

- **Invalid domains** : domaines compris dans votre répertoire, mais non utilisés de manière officielle dans votre service IMHS. IMHS ne peut pas fournir de service pour ces domaines et les adresses de messagerie qui leur correspondent.

ÉTAPE 5 Cliquez sur **Import**.

REMARQUE Ce sont les meilleures pratiques pour l'exportation et l'importation dans IMHS, ainsi que pour l'administration et la vérification des répertoires utilisateurs. Pour plus de détails sur ces pratiques, consultez le guide *Trend Micro InterScan Messaging Hosted Security 1 Getting Started Guide*, pages 3-23 à 3-26.)

Co-marquage pour l'affichage d'un logo d'entreprise sur le portail Web

IMHS permet aux utilisateurs d'afficher un logo d'entreprise à divers endroits du portail Web. Si cette fonctionnalité est activée, le logo sélectionné apparaît aux endroits suivants :

- La barre des bannières de la page de connexion IMHS
- Le volet de navigation de gauche de l'interface graphique IMHS après la connexion
- La barre des bannières de la page de connexion IMHS Web EUQ
- Le volet de navigation de gauche de l'interface graphique IMHS Web EUQ après la connexion

REMARQUE Les revendeurs peuvent définir différents logos pour différents domaines ou autoriser les administrateurs du système à définir le logo de leur domaine, de manière distincte du logo du revendeur. Le logo sélectionné pour un domaine s'affiche également dans la barre des bannières et dans le volet de navigation IMHS Web EUQ associés au domaine.

Les utilisateurs de niveau revendeur peuvent définir différents domaines avec le même logo ou autoriser les administrateurs du domaine à définir le logo de leur domaine. Les revendeurs peuvent aussi choisir de laisser cette fonctionnalité désactivée.

Vérifiez que le fichier image du logo satisfait aux conditions suivantes :

- Hauteur de l'image : 45 pixels
- Largeur de l'image : 45-150 pixels
- Format du fichier : .gif, .jpg ou .png

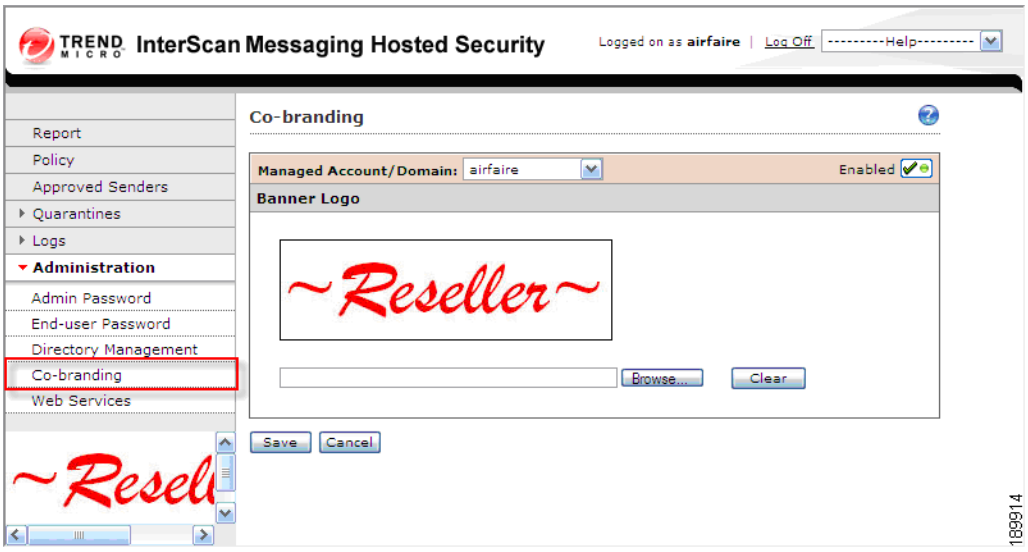
Pour afficher votre logo, suivez ces étapes :

ÉTAPE 1 Lancez le portail Web IMHS et connectez-vous.

REMARQUE Pour obtenir plus d'informations, reportez-vous à la section **Lancement du portail Web pour la protection de la messagerie, page 56**.

ÉTAPE 2 Cliquez sur **Administration** dans le menu de navigation, puis sur **Co-branding**.

La page Co-branding apparaît.



ÉTAPE 3 Pour activer cette fonctionnalité, cliquez sur l'icône **Disabled** située dans le coin droit de la page. L'étiquette de l'icône est maintenant Enabled. Si vous souhaitez ultérieurement désactiver cette fonctionnalité, cliquez sur l'icône **Enabled**. Par défaut, cette fonction est désactivée.

ÉTAPE 4 Dans la liste déroulante **Managed Account/Domain**, sélectionnez le compte ou le domaine qui va afficher le logo.

ÉTAPE 5 Cliquez sur **Browse** et choisissez le fichier du logo sur votre ordinateur.

ÉTAPE 6 Cliquez sur **Save**.

A

Pour en savoir plus

Cisco propose une vaste gamme de ressources pour vous aider à tirer pleinement parti du Cisco ProtectLink Web/Gateway.

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