YOGGIE

GATEKEEPER PICO™

MINI-ORDINATEUR DE SÉCURITÉ

Guide de l'Utilisateur

www.yoggie.com

Notification légale

NOTIFICATION RELATIVE À LA SÉCURITÉ : POUR ÉVITER LES DANGERS, GARDEZ LE PRODUIT ET SON EMBALLAGE HORS D'ATTEINTE DES BÉBÉS ET DES ENFANTS. LE PRODUIT N'EST PAS DESTINÉ AUX BÉBÉS NI AUX ENFANTS.

Q1 2008

YPUM001.3.6

Déclaration de conformité aux règlements de la FCC

DÉCLARATION DE CONFORMITÉ AUX RÈGLEMENTS DE LA FCC (Federal Communications Commision – USA) RELATIFS AUX ORDINATEURS ET PÉRIPHÉRIQUES DE LA CLASSE B

Nous, Yoggie Security Systems Ltd. B.P. 156 de Beit Halevy Israël, 42870 déclarons sous notre seule responsabilité que les produits :

Gatekeeper Pico™ et **Gatekeeper Pico Pro™**

auxquels cette déclaration se rapporte :

Sont conformes à la Part 15 des règlements de la FCC. L'utilisation est soumise aux deux conditions ci-dessous : (1) ces dispositifs ne peuvent pas causer d'interférences nuisibles, et (2) ces dispositifs doivent être capables d'accepter toute interférence reçue, y compris des interférences qui pourraient causer l'utilisation indésirable.

Des changements ou modifications à cet équipement qui n'ont pas été expressément approuvés par la partie responsable de la conformité (Yoggie Security Systems Ltd.) pourraient annuler l'autorité de l'utilisateur d'utiliser l'équipement.

NOTE : Cet équipement a été testé et avéré comme conforme aux limites d'un appareil numérique de Classe B, conformément à la partie 15 des règlements de la FCC. Ces limites ont été prévues afin d'assurer une protection raisonnable contre des interférences nuisibles dans une installation résidentielle. Cet équipement génère, utilise et peut irradier de l'énergie de fréquence radio et, s'il n'est pas installé et utilisé conformément aux instructions, il peut causer des interférences nuisibles aux communications radio. Toutefois, il n'y a pas de garantie que des interférences ne se produiront pas dans une installation donnée. Si cet équipement cause des interférences nuisibles à la réception radio ou de télévision, ce qui peut être déterminé en mettant l'équipement en marche ou à l'arrêt, l'utilisateur est encouragé d'essayer de corriger les interférences par l'une ou plusieurs des mesures ci-dessous :

- Réorienter ou déplacer l'antenne réceptrice.
- Augmenter la séparation entre l'équipement et le récepteur.
- Connecter l'équipement à une prise de courant d'un autre circuit que celui auquel le récepteur est connecté.
- Consulter l'agent ou le représentant ou un technicien radio/TV chevronné pour qu'il vous aide

Table des matières

NOTIFICATION LEGALE II
DECLARATION DE CONFORMITE AUX REGLEMENTS DE LA FCC III
TABLE DES MATIERES IV
QUELQUES MOTS SUR LE GUIDE DE L'UTILISATEUR 6
INTRODUCTION 7
CARACTERISTIQUES DU GATEKEEPER PICO 8
MODES D'UTILISATION 8
Mode administré (Corporate) 8
Mode autonome (Standalone) 8
DRIVER ET LOGICIEL DU GATEKEEPER PICO 9
CONTENU DE L'EMBALLAGE 10
EXIGENCES DU SYSTEME 11
FAITES CONNAISSANCE AVEC VOTRE GATEKEEPER PICO 12
MISE EN MARCHE 13
CONNEXION DU GATEKEEPER PICO 13
INSTALLATION ET ENREGISTREMENT DU DRIVER 13
CONSOLE DE GESTION DE YOGGIE 15
L'ACCES A LA CONSOLE DE GESTION VIA L'ICONE DU GATEKEEPER PICO 15
ACCESSION MANUELLE A LA CONSOLE DE GESTION 17
CHANGEMENT DE LANGUE D'INTERFACE 18
CHANGEMENT DE VOTRE MOT DE PASSE 18
CHANGEMENT DE VOTRE PROFIL D'UTILISATEUR 19
CHANGEMENT DE MODE 19
MODIFICATION DES REGLAGES DE CONFIDENTIALITE 20
REGLAGE DU FUSEAU HORAIRE 20
SURVEILLANCE DE L'ACTIVITE SECURITAIRE 21
Visualisation du statut de la sécurité 21
Visualisation et impression de rapports 24
Visualisation du Journal de sécurité 26
Visualisation du Journal du système 27
Visualisation du journal de RPV 27
CONFIGURATION DES REGLAGES DE RESEAU DU GATEKEEPER PICO 30
CONFIGURATION DU RPV (DISPONIBLE DANS LE GATEKEEPER PICO PRO) 33
REGLAGES DE LA PROTECTION CONTRE LES POURRIELS 36
REGLAGES AVANCES DE SECURITE 39
Filtrage Web / Contrôle parental du contenu 39
Firewall 41
Politique relative à la taille 45
Composants 46

SDI/SPI 47
SUPPORT 49
GENERATION D'UN FICHIER DE SUPPORT TECHNIQUE 49
OPTIONS DE REMISE A ZERO 49
DIAGNOSTICS 50
RESTRICTION DE L'ACCES A INTERNET GRACE AU GATEKEEPER PICO 53
DESACTIVATION DES RESTRICTIONS D'UTILISATION DU GATEKEEPER PICO 53
CHANGEMENT DU MOT DE PASSE DES RESTRICTIONS D'UTILISATION DU GATEKEEPER 53
DESINSTALLATION DU GATEKEEPER PICO 55
SPECIFICATIONS TECHNIQUES 56

Quelques mots sur le Guide de l'utilisateur

Ce Guide de l'utilisateur donne des instructions d'installation et d'utilisation pour les versions suivantes du Gatekeeper Pico™ :

- Gatekeeper Pico™
- Gatekeeper Pico Pro™

Introduction

Le Gatekeeper Pico est un appareil de sécurité miniature USB, il protège votre PC ou votre ordinateur portatif contre des intrusions hostiles, y compris des virus, chevaux de Troie, logiciels espions, vers et autres attaques via l'Internet, en les empêchant d'arriver à votre ordinateur. Il vous donne la liberté de connecter votre ordinateur à l'Internet où que ce soit, et il vous permet de jouir du plus haut niveau de protection — le niveau entreprise, de solutions de sécurité basées sur du matériel - utilisées par les organisations dont la sécurité est rigoureusement gardée.

Afin d'assurer une solution sécuritaire complète contre les menaces connues et inconnues, le Gatekeeper Pico combine les meilleurs produits logiciels de classe entreprise avec des développements exclusifs pour lesquels des demandes de brevets ont été déposées. Ces solutions comprennent :

- Adaptive Security Politcy™
- Multi-Layer Security Agent™
- Layer-8 Security Engine™
- Catégorisation et filtrage des URL
- Anti-pourriel
- Anti-hammeçonnage
- Anti-logiciels espions
- Anti-virus
- Des protocoles d'E-mail (POP3, SMTP)
- Des protocoles de Web transparents (HTTP; FTP)
- Détection /Prévention d'Intrusion
- Client à Réseau Privé Virtuel (disponible dans le Gatekeeper Pico Pro)
- Firewall dynamique

Avant qu'une donnée quelconque soit acceptée, puis traitée par le système d'exploitation de l'ordinateur, un driver de bas niveau la redirige vers le Gatekeeper Pico où une vérification sécuritaire complète est exécutée. Les tentatives d'effraction de brèche de sécurité sont identifiées puis déjouées, seulement ensuite les données sures et sécurisées sont retournées à l'ordinateur.

Gatekeeper Pico comprend une Console de Gestion basée sur le Web, elle donne des informations sur le statut, des journaux relatifs à la sécurité ainsi que des rapports, elle peut être utilisée pour personnaliser les connexions réseaux ainsi que les paramètres de sécurité.

Caractéristiques du Gatekeeper Pico

Le Gatekeeper Pico offre les caractéristiques suivantes :

- Extrêmement petit – de la taille d'une clé USB standard
- Dispositif sécuritaire basé sur du matériel, à système d'exploitation Hardened Linux
- Séparation physique entre l'ordinateur portatif et le monde extérieur
- Le Linux kernel du système réside dans une section de mémoire morte
- Plug and forget, et facilement porté
- Mises à jour automatiques
- Logiciel de sécurité tout-en-un au niveau entreprise
- Logiciel sécuritaire exclusif
- Surveillance en temps réel et rapports complets
- Management à distance (version Gatekeeper Pico Pro)

Modes d'utilisation

Mode administré (Corporate)

Dans ce mode, qui est disponible seulement dans le Gatekeeper Pico Pro, l'ensemble Gatekeeper est connecté à un Yoggie Management Server. Le Yoggie Management Server permet le contrôle et la mise en application des usages définis par le responsable du service informatique pour les utilisateurs nomades Installé dans la salle de serveurs du service de Technologie de l'Information, le Yoggie Management Server™ gère la flotte des ensembles Gatekeeper Pico nomades de la manière suivante :

- Il définit et met en place les politiques de sécurité de l'entreprise
- Il délivre les mises à jour de la suite logicielle de sécurité ainsi que toutes modifications quant à l'usage de l'internet
- Il obtient des journaux et événements locaux pour que la visibilité soit complète

Mode autonome (Standalone)

Dans ce mode, le Gatekeeper n'est pas connecté à un Yoggie Management Server, il fonctionne indépendamment. Dans ce cas, la politique de sécurité est définie par les paramètres de l'utilisateur du Gatekeeper, alors que les mises à jour sécuritaires sont directement téléchargées de manière transparente à partir de Yoggie Security Systems.

Driver et logiciel du Gatekeeper Pico

Le driver et le logiciel de Gatekeeper Pico sont compris dans le CD fourni du Gatekeeper Pico. Ceux-ci sont installés la première fois que l'ensemble Gatekeeper Pico est connecté à l'ordinateur portatif, comme décrit dans la section Mise en marche.

Le driver et le logiciel fournissent les dispositifs et avantages suivants :

- **Redirection** — la capacité de connecter un ordinateur portatif à un réseau (Internet ou autre) en utilisant une connexion Wi-Fi (sans fils), un modem analogique, un modem cellulaire ou toute autre interface de réseau, tout le trafic est redirigé vers l'ensemble Gatekeeper. Le Gatekeeper ne permet qu'à un trafic sûr et sécurisé d'atteindre votre ordinateur.

- **Conditions de connexion à internet**— la capacité de se connecter à un réseau est désactivée lorsque le Gatekeeper Pico n'est pas connecté à l'ordinateur portatif. Lorsque le Gatekeeper est physiquement déconnecté de l'ordinateur portatif pendant l'utilisation, toutes les connexions du réseau sont automatiquement et immédiatement coupées.

- **L'icône du Gatekeeper Pico** — elle est située dans la zone de notification de Windows (plateau d'icônes). Un clic droit sur l'icône donne :

- L'accès rapide à la Console de Gestion du Gatekeeper Pico.

- La capacité de désactiver temporairement la protection (voir la section Désactivation des restrictions du Yoggie Gatekeeper).

- **Indication du statut de Protection** — l'icône du Gatekeeper Pico est verte lorsque la protection est activée, et rouge lorsqu'elle est désactivée et violette lorsque la protection est hors service.

- **Bulles de notification** — Des bulles de l'icône contiennent des informations sur le statut et sur des événements du Gatekeeper. Des infobulles de notification du statut peuvent aussi être visualisées en plaçant le curseur de la souris sur l'icône.

- **Désactivation de la protection** — (mot de passe exigé) en cas d'urgence, par exemple, lorsqu'un ensemble Gatekeeper Pico a été perdu ou endommagé, le réseau peut être accédé en désactivant les restrictions Gatekeeper Pico (voir la section Désactivation des restrictions d'utilisation du Gatekeeper Pico).

Contenu de l'emballage

- Gatekeeper Pico ou Gatekeeper Pico Pro
- CD du Gatekeeper Pico
- Guide de départ rapide

Exigences du système

Port USB et PC sous Windows XP ou Vista

Faites connaissance avec votre Gatekeeper Pico

- **Alimentation** – s'illumine lorsque le Gatekeeper Pico est alimenté.
- **Événements sécuritaires** – clignote lorsqu'un événement sécuritaire se produit.
- **Mise à jour** – clignote lorsque des mises à jour sont en cours de téléchargement.

Ne pas retirer le Gatekeeper Pico pendant des mises à jour.

Lorsque le Gatekeeper Pico s'amorce, l'indicateur de sécurité et celui de mise à jour scintillent jusqu'à ce que la séquence soit terminée.

Mise en marche

La mise en marche consiste en la connexion, la configuration initiale, puis l'enregistrement du Gatekeeper Pico.

Connexion du Gatekeeper Pico

➔ **Pour connecter le Gatekeeper Pico :**

1. Retirez le capuchon.
2. Insérer le Gatekeeper Pico dans un port USB disponible, les performances sont améliorées lorsque le Gatekeeper Pico est connecté à un port USB 2.0.

   Les indicateurs LED du Gatekeeper Pico commencent à clignoter, indiquant la séquence d'amorçage.

Il se peut que Windows détecte automatiquement Gatekeeper Pico comme étant un nouveau dispositif matériel et demande d'installer un driver. Cliquez sur **Annuler** pour quitter l'assistant d'installation du driver.

Installation et enregistrement du driver

Il est recommandé de désactiver toutes les suites de Firewall ou de protection Internet basées sur un logiciel .

1. Insérez le CD du Gatekeeper Pico.

   Un écran de menus apparaît.
2. Cliquez sur **Installer le logiciel et le driver de Yoggie** (Install Yoggie software and driver)**,** puis suivre les instructions de l'écran.

   Après l'installation du driver, votre navigateur Web s'ouvre et vous êtes automatiquement invité à indiquer un nom d'utilisateur et un mot de passe afin de commencer le processus d'enregistrement.
3. Entrez les informations d'ouverture de session par défaut (sensibles à la casse) :

   Utilisateur : admin
   Mot de passe : yoggie

   L'écran de choix de la langue d'interface apparaît.
4. Choisissez votre langue préférée.

   L'écran de contrat de licence d'utilisateur final (EULA) apparaît.
5. Veuillez lire le contrat de licence d'utilisateur final, puis cliquez sur **J'accepte** pour continuer.

L'écran d'enregistrement apparaît.

6. Faites une des actions suivantes :

   - Lorsque votre ordinateur portatif sera connecté au Yoggie Management Server (YMS), sélectionnez l'option de configuration **Mode d'entreprise** (Corporate mode).
   - Si votre ordinateur portatif ne fonctionnera pas avec le Yoggie Management Server™, sélectionnez l'option de configuration **Mode autonome** (Standalone Mode).

7. Entrez les informations suivantes :

   - Votre nom
   - Votre adresse e-mail
   - Une clé de licence valide, placée sur la vignette CD (Mode autonome seulement)
   - Les réglages pour le Yoggie Management Server de votre entreprise (IP/mot de passe) (seulement dans le Mode d'entreprise)

   Cliquez sur **Suivant** (Next).

8. L'écran Confidentialité apparaît. Configurez vos réglages désirés pour la confidentialité (partagez les informations sécuritaires avec Gatekeeper Pico pour améliorer la sécurité).

   Cliquez sur **Suivant** (Next).

9. Définissez votre nouveau mot de passe pour accéder à la Console de Gestion, et à votre fuseau horaire.

   Pour terminer l'enregistrement, cliquez sur **Terminer**.

L'icône du Gatekeeper Pico apparaît dans la zone de notification de Windows, et maintenant Gatekeeper Pico protège votre ordinateur portatif.

Faites passer un test au Gatekeeper Pico

Téléchargez le fichier de démo de virus d'EICAR à partir de :
http://www.eicar.org/anti_virus_test_file.htm

Gatekeeper Pico télécharge toute mise à jour exigée. Pendant la première utilisation, ce processus peut prendre jusqu'à quinze minutes, et vous ne pourrez pas utiliser le Gatekeeper Pico pendant cette période. Vous pouvez visualiser l'avancement de la mise à jour via la **Console de Gestion de Yoggie,** basée sur le Web.

Console de Gestion de Yoggie

La Console de Gestion de Yoggie (Console de Gestion) donne accès aux dispositifs de management du Gatekeeper Pico via votre navigateur Web. Vous pouvez surveiller l'activité sécuritaire en visualisant le statut actuel de la sécurité, visualisant et imprimant les rapports et journaux de sécurité, visualisant et configurant la sécurité, visualisant les réglages du système et de l'utilisateur, visualisant et imprimant les journaux des événements non-sécuritaires du système, et bien plus.

La Console de Gestion peut être accédée selon les méthodes suivantes :

- **L'icône du Gatekeeper Pico** — lorsque le driver/logiciel de Gatekeeper Pico est installé (voir la section Mise en marche.
- **Navigateur Web** — si pour une raison quelconque l'icône du Gatekeeper Pico n'est pas disponible vous pouvez accéder manuellement à la Console de Gestion au moyen d'un navigateur Web standard.

L'accès à la Console de Gestion via l'icône du Gatekeeper Pico

La Console de Gestion du Gatekeeper peut être accédée via l'icône du Gatekeeper Pico.

➔ **Pour accéder à la Console de Gestion via l'icône du Gatekeeper Pico :**

1. Dans la zone de notification de Windows, Cliquez avec le bouton droit sur l'icône du Gatekeeper Pico.
2. Sélectionnez **Ouvrir la Console de Gestion** dans le menu affiché en mode fenêtre.

Pour ouvrir la Console de Gestion, vous pouvez aussi double-cliquer sur l'icône du Gatekeeper Pico.

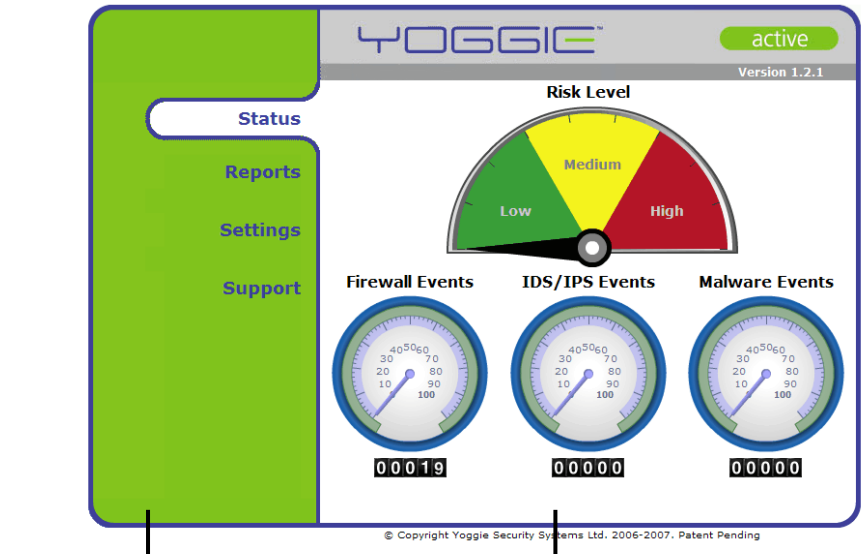
La boîte de dialogue **d'Ouverture de session (Login)** s'ouvre.

3. Entrez les informations suivantes :
   - **Nom d'utilisateur** (User name) — admin

- **Mot de passe** (Password) — entrez votre mot de passe de Gatekeeper Pico (le mot de passe par défaut est yoggie).

4. Cliquez sur **OK**.

La Console de Gestion s'ouvre, comme représenté ci-dessous.



Carreau de navigation Carreau d'affichage

Accession manuelle à la Console de Gestion

Si pour une raison quelconque l'icône du Gatekeeper Pico n'est pas disponible vous pouvez accéder manuellement à la Console de Gestion à l'aide d'un navigateur Web standard.

La Console de Gestion peut être manuellement accédée en entrant l'URL de la Console de Gestion du Gatekeeper Pico dans le champ adresse de votre Web.

➔ **Pour accéder manuellement à la Console de Gestion :**

1. Ouvrez un navigateur Web et entrez l' URL suivante de la Console de Gestion du Gatekeeper Pico dans le champ d'adresse du navigateur : `https://yoggie.yoggie.com:8443`

   La boîte de dialogue d' **Ouverture de session (Login)** s'ouvre.

2. Entrez les informations suivantes :
   - **Nom d'utilisateur** (User name)— admin
   - **Mot de passe** (Password) — entrez votre mot de passe au Gatekeeper Pico (le mot de passe par défaut est yoggie).
3. Cliquez sur **OK**. La Console de Gestion s'ouvre.

Changement de langue d'interface

À tout moment, vous pouvez changer la langue d'interface de l'utilisateur (étiquettes et dialogues) dans votre Console de Gestion du Gatekeeper Pico.

➔ **Pour changer la langue d'interface de votre Console de Gestion :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** (Security) apparaît dans le carreau d' **Afffichage**.

2. Cliquez sur l'onglet **Système (**System).

   La page **Détails du Yoggie** apparaît dans le carreau d' **Affichage**.

3. Cliquez sur **Langue** (Language**)**.

   La page **Réglages de la langue** apparaît.

4. Dans la liste choisissez la langue que vous désirez utiliser.

5. Cliquez sur **Appliquer** (Apply).

   La langue d'interface sélectionnée sera utilisée, et la page principale **Détails du Yoggie** apparaît.

Changement de votre mot de passe

À tout moment, vous pouvez changer votre mot de passe vers la Console de Gestion du Gatekeeper Pico.

➔ **Pour changer votre mot de passe vers la Console de Gestion du Gatekeeper Pico :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** (Security) apparaît dans le carreau d' **Affichage**.

2. Cliquez sur l'onglet **Système**.

   La page **Détails du Yoggie** apparaît dans le carreau **Affichage**.

3. Cliquez sur **Changer le Mot de passe** (Change Password).

   La page **Réglages du Mot de passe** apparaît.

4. Entrez les informations suivantes :

   - **Mot de passe actuel** (Current Password) — entrez votre mot de passe actuel
   - **Nouveau mot de passe** (New Password) — entrez le nouveau mot de passe
   - **Confirmation du mot de passe** (Confirm Password) — entrez encore une fois le nouveau mot de passe

5. Cliquez sur **Appliquer** (Apply).

Votre mot de passe est changé et la page principale **Détails du Yoggie** apparaît.

Changement de votre profil d'utilisateur

Les détails relatifs à l'utilisateur de Gatekeeper Pico consistent en votre nom d'utilisateur et votre adresse E-mail. Ceux-ci peuvent être changés à tout moment.

➔ **Pour changer vos détails d'utilisateur de Gatekeeper Pico :**

1. Cliquez sur **Réglages** dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur l'onglet **Système** (System).

   La page **Détails de Yoggie** apparaît dans le carreau **Affichage**.

3. Sous **Détails de Yoggie** (Yoggie Details), Cliquez sur **Modifier** (Modify).
4. Entrez votre nouveau nom d'utilisateur dans le champ **Nom** (Name), comme exigé.
5. Entrez votre nouvelle adresse e-mail dans le champ **Adresse E-mail** (E-mail address), comme exigé.
6. Cliquez sur **Appliquer** (Apply).

   Vos détails d'utilisateur sont changés et la page **Détails de Yoggie** apparaît.

Changement de mode

Le Gatekeeper Pico peut être utilisé comme un Pico autonome (Mode autonome) ou comme une partie d'une flotte de dispositifs Gatekeeper gérée par un Yoggie Management Server (YMS). Le mode est établi pendant l'enregistrement, mais il peut être modifié à tout moment.

➔ **Pour changer le mode de votre Gatekeeper Pico :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur l'onglet **Système** (System).

   La page **Détails de Yoggie** apparaît dans le carreau d' **Affichage**.

3. Sous **Détails de Yoggie** (Yoggie Details) , Cliquez sur **Modifier** (Modify).
4. Choisissez le mode que vous désirez :

   - Mode autonome — entrez le numéro de la licence fournie dans le champ **Licence**.
   - Mode d'entreprise — entrez l'adresse IP du Yoggie Management Server dans le champ **Adresse du Serveur** (Server Address) et le mot de passe dans le champ **Mot de passe** (Password).

5. Cliquez sur **Appliquer** (Apply).

Votre mode est changé et la page **Détails de Yoggie** apparaît.

Modification des réglages de confidentialité

Gatekeeper Pico collecte seulement des informations liées à la sécurité afin d'améliorer la qualité des produits et celle du service. Il est très recommandé que vous utilisiez les réglages par défaut de la confidentialité. Yoggie ne partagera jamais quelque information privée que ce soit avec un tiers, et ne fera aucune autre utilisation de cette information.

➔ **Pour modifier les réglages de la confidentialité :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de Navigation de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur l'onglet **Système (System)**.

   La page **Détails de Yoggie** apparaît dans le carreau d' **Affichage**.

3. Cliquez sur **Confidentialité** (Privacy).

   La page **Réglages de confidentialité** apparaît.

4. Choisissez si vous voulez enregistrer votre nom et votre adresse d'e-mail avec Yoggie. Choisissez votre réglage de confidentialité dans la liste déroulante. Vous pouvez choisir une des options suivantes :

   - **Partager les journaux de sécurité avec Yoggie** – partager tous les événements sécuritaires collectés par les journaux du Gatekeeper Pico avec Yoggie Security Systems.
   - **Cacher un domaine spécifique et les informations URL** – ne pas partager des événements sécuritaires qui contiennent la source et la destination de pourriels ou d'URL de destination. Partager tous les autres événements sécuritaires collectés par les journaux du Gatekeeper Pico avec Yoggie Security Systems.
   - **Ne partager aucun événement sécuritaire** – ne partager aucun événement sécuritaire collecté par les journaux du Gatekeeper Pico avec Yoggie Security Systems.

5. Cliquez sur **Appliquer** (Apply).

   La page **Détails de Yoggie** apparaît.

Réglage du fuseau horaire

La date et l'heure actuelles sont affichées dans la page principale **Réglages** de la Console de Gestion. Ces informations sont mises à jour via le serveur de Yoggie selon le fuseau horaire défini dans la Console de Gestion. Pour changer l'heure, définissez un nouveau fuseau horaire — La date et l'heure sont instantanément mises à jour et affichées.

➔ **Pour définir le fuseau horaire :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur l'onglet **Système** (System)**.**

   La page **Détails de Yoggie** apparaît dans le carreau d' **Affichage**.

3. Sous **Fuseau horaire** (Time Zone), cliquez sur **Modifier** (Modify).

   La page **Réglages du fuseau horaire** apparaît.

4. Choisissez votre emplacement dans la liste déroulante de fuseaux horaires.

5. Cliquez sur **Appliquer** (Apply).

   Le fuseau horaire sélectionné est affiché, et la date et l'heure courantes sont mises à jour. La page **Yoggie Détails** apparaît.

Surveillance de l'activité sécuritaire

La Console de Gestion donne plusieurs options de surveillance de l'activité sécuritaire. Vous pouvez visualiser votre statut actuel de la sécurité, des graphiques sur les activité sécuritaire (y compris des graphiques en 3D), des journaux de sécurité et du système, puis visualiser et imprimer des rapports sur les activités sécuritaires.

Visualisation du statut de la sécurité

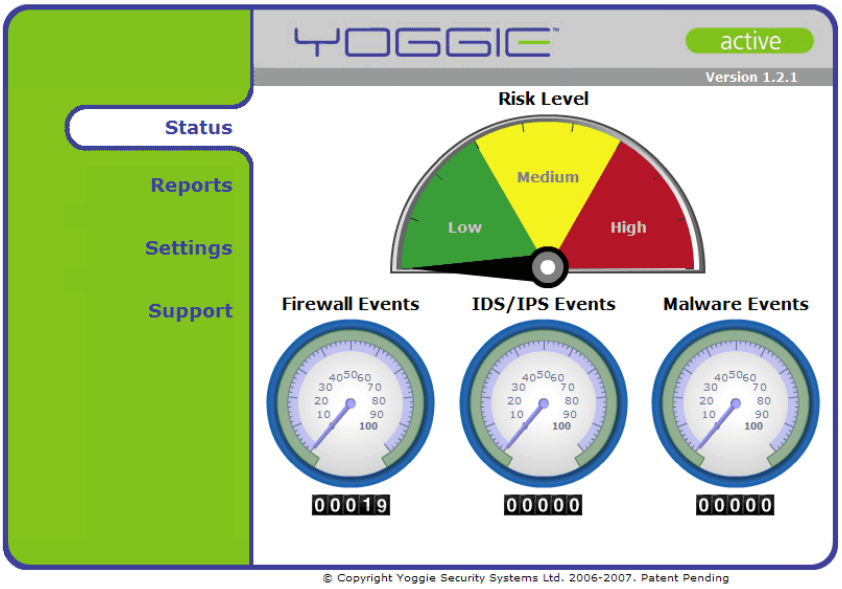
La page Statut de la Console de Gestion vous permet de visualiser votre niveau actuel de risque (une notation basée sur l'activité courante) et des événements sécuritaires. La page comprend des indicateurs et compteurs d'événements qui indiquent le nombre de tentatives de brèche de sécurité déjouées par votre Gatekeeper Pico au cours des 15 dernières minutes pendant lesquelles le Pico était connecté et fonctionnait.

La page Statut ne montre pas le niveau de sécurité du Gatekeeper Pico, mais l'intensité des tentatives de sécurité brèche. Le Gatekeeper Pico protège votre ordinateur portatif à tous les niveaux de risques.

➔ **Pour visualiser le statut de la sécurité :**

- Cliquez sur **Statut** (Status) dans le carreau de **Navigation** de la Console de Gestion.

La page **Statut** apparaît dans le carreau d' **Affichage**, comme représenté ci-dessous.



La page **Statut** affiche les indications suivantes, qui vous permettent de surveiller l'activité sécuritaire :

- **Niveau de risque** (Risk Level) — affiche votre niveau courant de risque de sécurité, il est basé sur l'analyse du Gatekeeper Pico de tous les événements sécuritaires du firewall, du SDI/SPI, et de logiciels malveillants.
- **Événements du Firewall** (Firewall Events) — affiche le nombre d'attaques tentées contre le firewall qui ont eu lieu au cours des 15 dernières minutes.
- **Événements SDI/SPI** (IDS /IPS Events) — affiche le nombre de tentatives de brèches de sécurité détectées puis défaites par le Système de Détection d'Intrusion Système / Système de Protection contre les Intrusions (SDI/SPI) au cours des 15 dernières minutes.
- **Événements de Logiciels malveillants** (Malware Events) — affiche le nombre de virus, logiciels espions, contenus actifs, et autres tentatives d'exécution similaires qui ont eu lieu au cours des 15 dernières minutes.

Les indicateurs numériques (compteurs d'événements) sous chaque indicateur d'événement affichent le total de chaque type de tentative de brèche de sécurité. Le nombre affiché est le nombre de tentatives depuis la dernière remise à zéro. Pour avoir plus d'informations sur la remise à zéro des compteurs d'événements, voir la section *Remise à zéro des compteurs d'événements* .

Remise à zéro des compteurs d'événements

Les indicateurs numériques (compteurs d'événements) sous chaque indicateur d'événements dans la page **Statut** montrent un recueil continuel de données pour chaque type d'événement sécuritaire. Ces indicateurs peuvent être remis à zéro.

➔ **Pour remettre à zéro les compteurs d'événements :**

1. Cliquez sur **Soutien** (Support) dans le carreau de **Navigation** de la Console de Gestion.
2. Cliquez sur l'onglet **Outils de soutien** (Support Tools).
3. Cliquez sur **Options de remise à zéro** (Reset Options).
4. Cochez **Remettre à zéro les compteurs** (Reset Counters)
5. Dans la page de confirmation affichée, cliquez sur **Appliquer** (Apply).

   Les compteurs sont remis à zéro.

Visualisation et impression de rapports

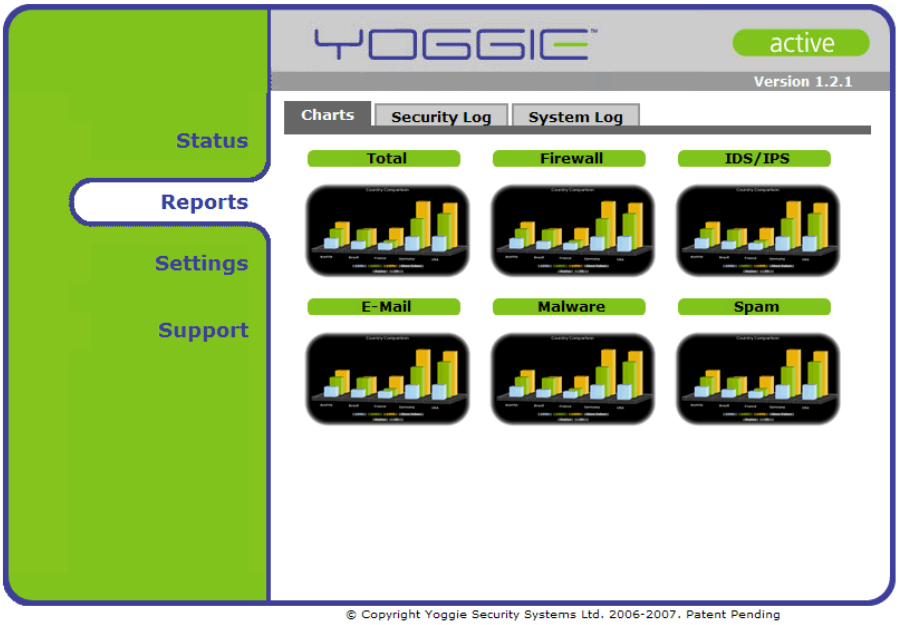
Les graphiques de sécurité fournissent des rapports sur les événements sécuritaires selon les types sous forme de graphiques. Ces graphiques reflètent des informations rassemblées pendant les dernières 24 heures de fonctionnement.

Vous pouvez cliquer sur un graphique pour le visualiser sous forme de graphique en 3D, et ensuite cliquer dessus, puis le faire glisser pour changer son orientation. Vous pouvez aussi naviguer entre les graphiques, les visualiser en 2D, réinsérer des animations, et les imprimer.

➔ **Pour visualiser des rapports :**

1. Cliquez sur **Rapports** (Reports) dans le carreau de **Navigation** de la Console de Gestion.

   La page principale de graphiques de l'onglet **Graphiques** apparaît dans le carreau d' **Affichage**, comme représentée ci-dessous.



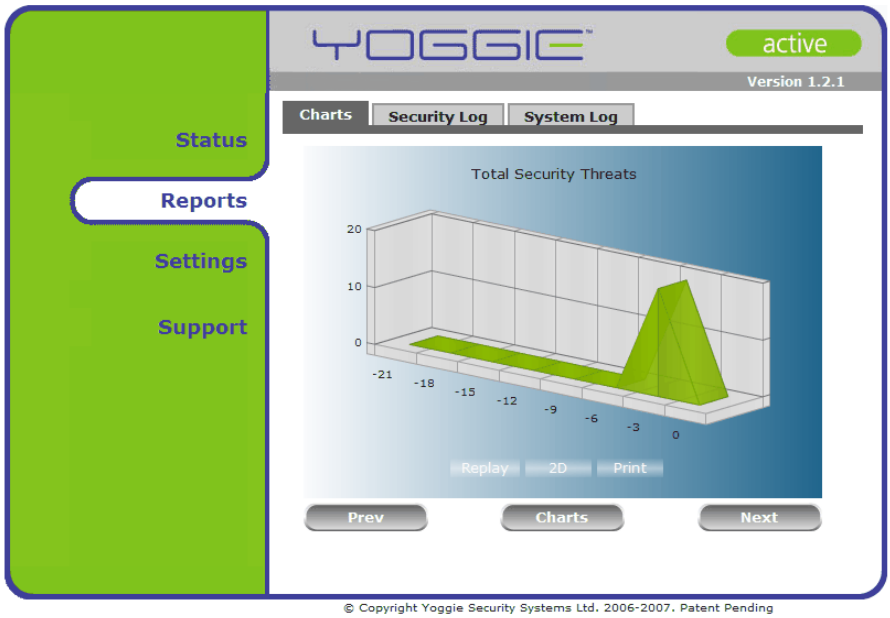
L'onglet **Graphiques** affiche les graphiques suivants :

Tous les graphiques affichent des informations rassemblées pendant les dernières 24 heures de fonctionnement.

- **Total** — affiche le nombre total d'événements de brèches de sécurité.
- **Firewall** — affiche le total des attaques tentées contre le firewall.
- **SDI/SPI** (IDS/IPS)— affiche le nombre total de brèches de sécurité tentées détectées puis défaites par le SDI/SPI.
- **E-Mail** — affiche le total de menaces d'hammeçonnage, de pourriel, et d'autres courriels.

- **Logiciels malveillants** (Malware) — affiche le total de virus, logiciels espions, contenus actifs, et d'autres tentatives similaires.
- **Pourriel** (Spam) — affiche le score de la distribution de pourriels (le nombre de messages e-mail qui sont probablement des pourriels).

2. Dans l'onglet **Graphiques** (Charts) , cliquez sur un graphique pour l'afficher en 3D, comme présenté dans l'exemple ci-dessous.



Vous pouvez changer l'orientation d'un graphique en 3D, cliquez dessus puis faites-le glisser.

3. Dans l'affichage en 3D, cliquez sur :

- **Réinsertion** (Replay) — ré exécute une animation
- **2D** — affiche le graphique en 2D
- **Imprimer** (Print) — imprime le graphique en 3D
- **Précédent** (Prev) — affiche le graphique précédent en 3D
- **Suivant** (Next)— affiche le graphique suivant en 3D
- **Graphiques** (Charts) — revient à la page principale graphique

Visualisation du Journal de sécurité

Le Journal de sécurité du Gatekeeper Pico affiche des informations sur des événements sécuritaires. Vous pouvez visualiser le journal initial et les détails relatifs à chaque événement.

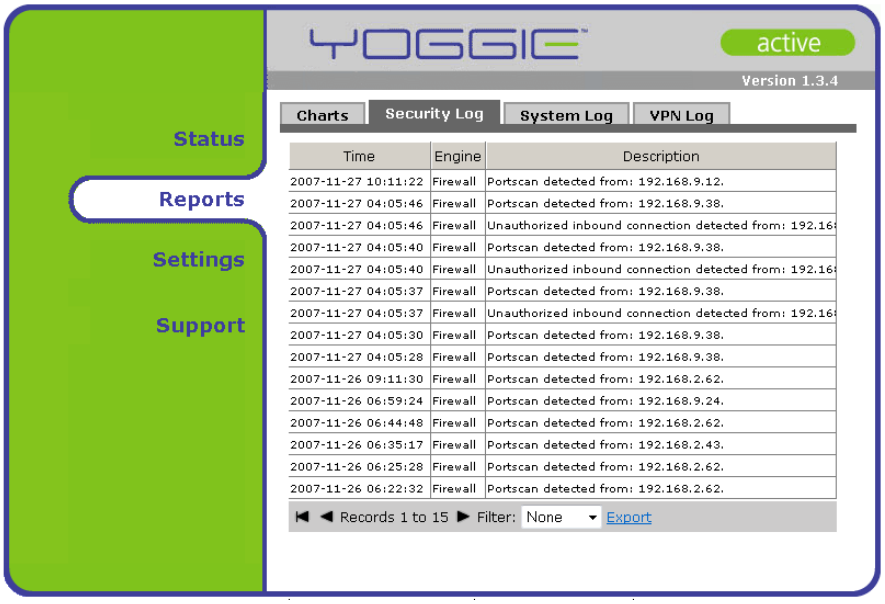
➔ **Pour visualiser le Journal de sécurité :**

1. Cliquez sur **Rapports** (Reports) dans le carreau de **Navigation** de la Console de Gestion.

   La page principale graphique de l'onglet **Graphiques** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur l'onglet **Journal de sécurité** (Security log).

   Le Journal de sécurité est affiché, comme représenté ci-dessous.



3. Pour affficher un sommaire des détails d'un événement, cliquez sur cet événement.
4. Pour naviguer vers des pages suivantes/précédentes du Journal de sécurité, cliquez sur le bouton flèche droite/gauche, selon le besoin.
5. Pour exporter le Journal de sécurité, cliquez sur **Export**.

   Un dialogue de sauvegarde de fichier apparaît.

6. Sauvegardez sur votre PC le fichier compressé du journal de sécurité.

Visualisation du Journal du système

Le journal du système affiche tous les événements importants du système qui n'ont pas trait à la sécurité.

➔ **Pour visualiser le Journal du système :**

1. Cliquez sur **Rapports** (Reports) dans le carreau de **Navigation** de la Console de Gestion.

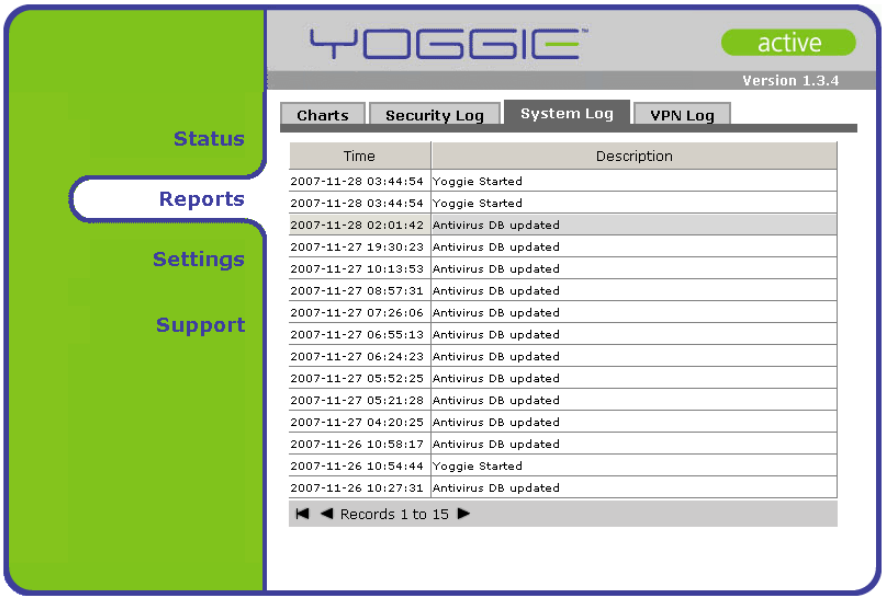
   La page principale de graphique de l'onglet **Graphiques** apparaît dans le carreau d'**Affichage**.

2. Cliquez sur l'onglet du **Journal du système** (System log).

   Le journal du système est affiché.

3. Cliquez sur un événement pour afficher les détails de l'événement.

4. Pour naviguer vers des pages suivantes/précédentes du Journal du système, cliquez sur le bouton flèche droite/gauche selon le besoin.



.

Visualisation du journal de RPV

Le Journal de RPV affiche les événements liés au RPV.

➔ **Pour visualiser le journal du RPV:**

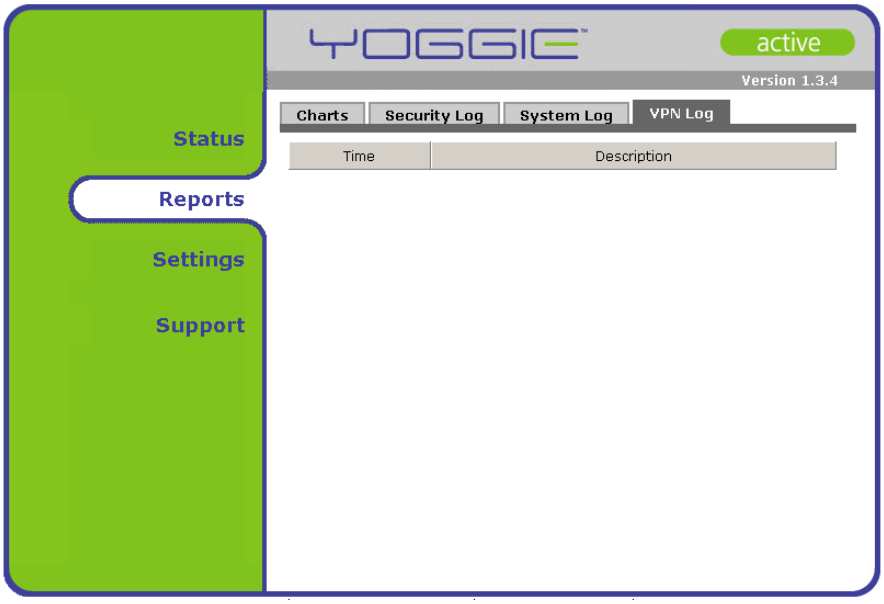
1. Cliquez sur **Rapports** (Reports) dans le carreau de **Navigation** de la Console de Gestion.

La page principale de graphiques de l'onglet **Graphiques** apparaît dans le carreau d' **Afffichage**.

2. Cliquez sur l'onglet **Journal de RPV** (VPN Log).

   Le Journal de RPV est affiché.

3. Pour afficher un sommaire des détails d'un événement, positionnez le curseur de votre souris sur cet événement.
4. Pour afficher les détails d'un événement, cliquez sur cet événement.
5. Pour naviguer vers des pages suivantes/précédentes du Journal du RPV, cliquez sur le bouton flèche droite/gauche selon le besoin.



Configuration de la Sécurité

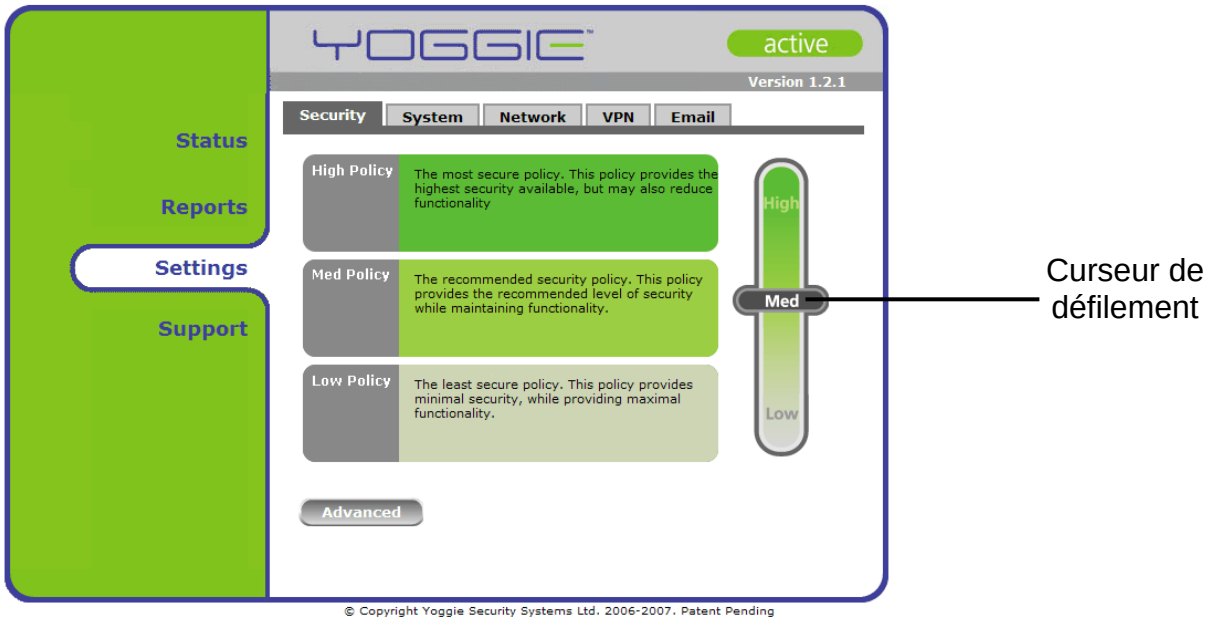
La configuration de la politique sécuritaire du Gatekeeper Pico est simple et intuitive. Il y a trois niveaux de sécurité :

- **Politique stricte** (High policy) — c'est la politique la plus sécurisée ; Elle fournit la meilleure sécurité, mais risque de réduire la fonctionnalité.
- **Politique moyenne** (Med policy) — c'est la politique recommandée ; Elle donne le niveau de sécurité recommandé, tout en maintenant la fonctionnalité.
- **Politique tolérante** (Low policy) —c'est la politique la moins sécurisée ; Cette politique donne la sécurité minimale, tout en assurant la fonctionnalité maximale.

➔ **Pour définir la politique sécuritaire :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**, comme représenté ci-dessous.



2. Pour changer de politique sécuritaire, cliquez sur le curseur de défilement, puis le faire glisser.
3. Cliquez sur **Appliquer** (Apply)**.**

   La politique sécuritaire est établie.

Configuration des réglages de réseau du Gatekeeper Pico

Les réglages de votre réseau actuel sont affichés sous l'onglet **Réseau** (network) dans le menu **Réglages** (Settings). Si normalement vous vous connectez à l'Internet via un Serveur de proximité, ce serveur doit être défini dans la Console de Gestion de Yoggie.

➔ **Pour configurer les réglages du réseau interne :**

1. Dans le carreau de Navigation de la Console de Gestion cliquez sur **Réglages** (Settings).

   La page principale des **Réglages** apparaît.

2. Cliquez sur l'onglet **Réseau** (Network).

   La page **Réglages du réseau** apparaît dans la zone d'affichage.

3. Cliquez sur **Modifier** (Modify).

   La page **Réglages du réseau interne** apparaît dans la zone d'affichage.

4. Dans le champ **Adresse IP** (Addess IP), entrez la nouvelle adresse IP du dispositif.

5. Dans le champ **Masque de sous réseau (Subnet Mask)**, entrez le nouveau masque du sous réseau du dispositif.

   Cliquez sur **Appliquer** (Apply).

   Les réglages du Réseau interne sont configurés.

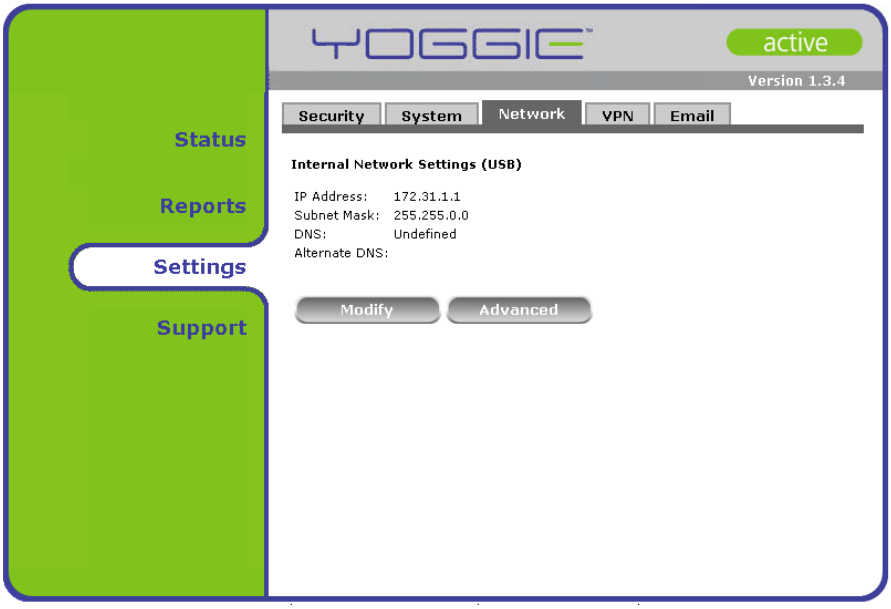
➔ **Pour configurer les Réglages de proximité :**

1. Cliquez sur **Réglages** dans le carreau de Navigation de la Console de Gestion.

   La page principale **Réglages** apparaît.

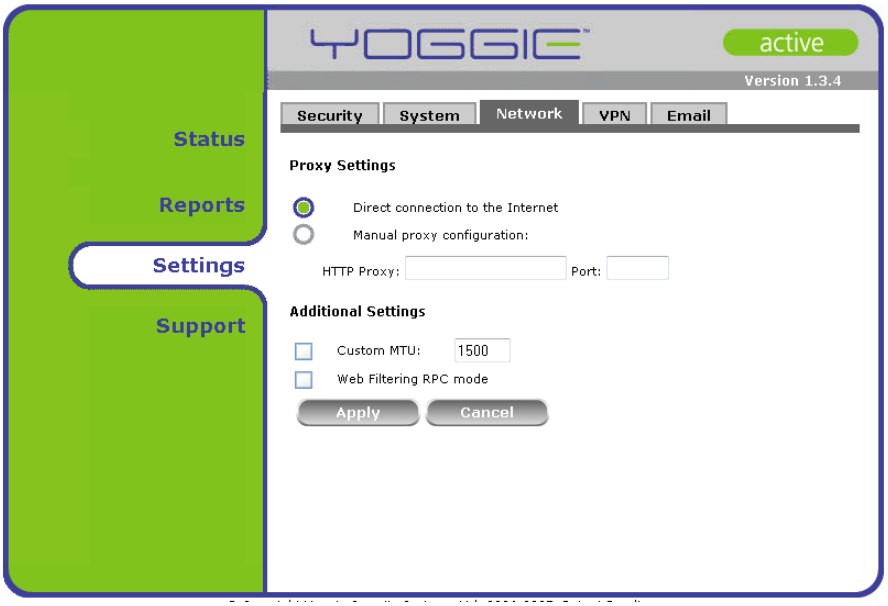
2. Cliquez sur l'onglet **Réseau** (Network).

   La page **Réglages du réseau** apparaît dans la zone d'affichage.



3. Cliquez sur **Avancé** (Advanced)**.**

   La page **Réglages de Proximité** apparaît.



4. Choisissez **Configuration manuelle du serveur de proximité** (manual proxy configuration).
5. Dans le champ **Protocole HTTP** (HTTP Proxy), entrez l'adresse web du Serveur de proximité.

6. Dans le champ **Port**, entrez le numéro du port auquel le Serveur de proximité assure le service.

   Cliquez sur **Appliquer** (Apply).

   Les réglages du serveur de proximité sont configurés.

Configurez des réglages supplémentaires si nécessaire

➔ **Pour configurer les réglages de l'Unité Maximale de Transfert – UMT** (Maximum Transmission Unit - MTU) **:**

1. Choisissez **Adaptation sur mesure de l'Unité maximale de transfert** (Custom MTU)
2. Entrez le nouvel UMT (par défaut 1 500 bytes).

   Cliquez sur **Appliquer** (Apply).

Certains Firewalls limitent l'accès au port UDP 9020 qui est nécessaire au moteur de filtrage Web. Pour surmonter ce problème nous permettons au filtrage Web de fonctionner sur le port HTTP bien connu qui est toujours ouvert sur le Firewall. Ce mode d'utilisation est dénommé mode Appel de Procédure Distant- APC (Remote Procedure Call - RPC).

➔ **Pour configurer les réglages d' Appel de Procédure Distant (APC) :**

1. Choisissez le mode de Filtrage Web d'APC

   Cliquez sur **Appliquer** (Apply).

   Les réglages supplémentaires de proximité sont configurés.

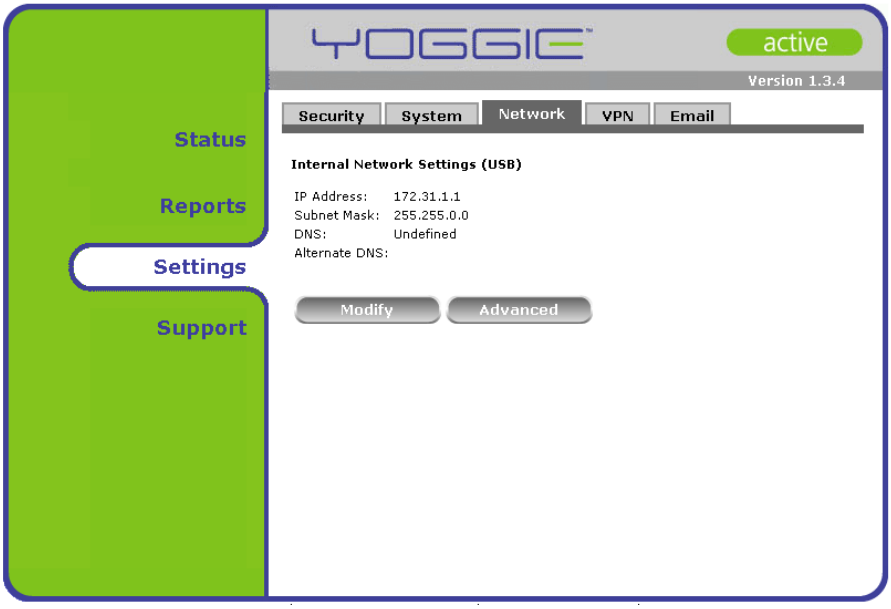
➔ **Pour configurer les réglages de proximité :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Réglages** apparaît.

2. Cliquez sur l'onglet **Réseau** (Network).

   La page **Réglages de réseau** apparaît dans la zone d'affichage.



Configuration du RPV (Disponible dans le Gatekeeper Pico Pro)

Le Gatekeeper Pico Pro comprend un Client RPV destiné à connecter à un serveur distant de RPV. Vous pouvez activer ou désactiver le Client RPV à tout moment.

➔ **Pour activer /désactiver la connexion RPV :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Réglages** apparaît.

2. Pour désactiver la connexion RPV, dans le carreau **RPV,** cliquez sur **Connexion RPV désactivée** (VPN Connection disabled) ; ou pour activer la connexion RPV. cliquez sur **Connexion RPV activée** (VPN Connection enabled).
   Dans le champ **Type de RPV** (VPN Type), choisissez un des types de RPV suivants : Générique (genéric), Cisco, CheckPoint.

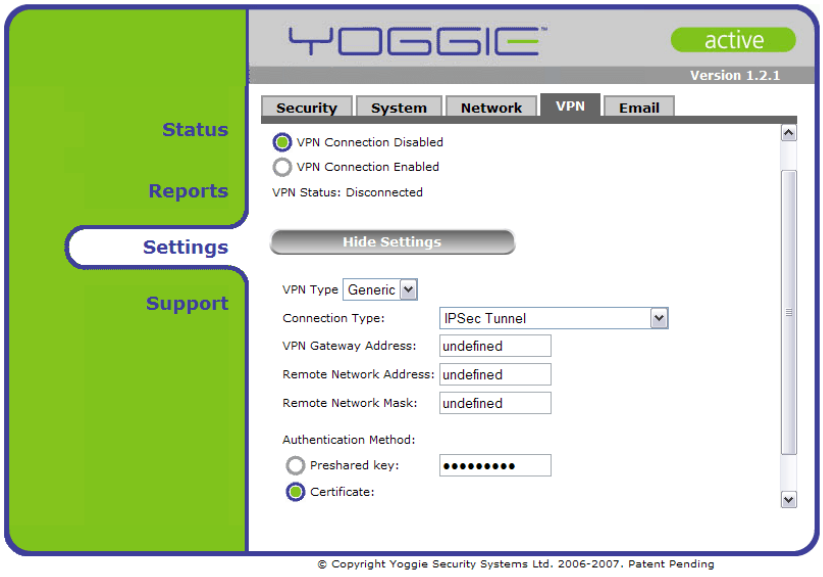
➔ **Pour configurer la connexion générique de RPV :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Réglages** apparaît.

2. Dans le carreau **RPV,** cliquez sur **Visualiser les réglages** (View Settings)**.**

   L'écran Réglages de RPV apparaît.



3 Dans le champ **Type de connexion** (Connection type), choisissez un des types de connexion suivants : IPSec Tunnel, IPSec Tunnel Single Host, IPSec L2TP Transport (Windows).

4. Dans le champ **Adresse de Passerelle RPV** (VPN Gateway address) entrez l'adresse IP du serveur RPV à accès distant.

5. Dans le champ **Adresse du réseau distant** (Remote Network address) entrez l'adresse du réseau distant.

6. Dans le champ **Masque du réseau distant** (Remote Network Mask) entrez le masque du sous-réseau distant.

En dessous de **Méthode d'Authentification** (Authentication Method) faites une des actions ci-dessous :

- Si la méthode d'authentification entre le client et le serveur est par une clé pré répartie, choisissez **Clé pré répartie (**Preshared key), puis entrez la clé.

- Si l'authentification entre le client et le serveur se fait par un certificat, choisissez **Certificat** (Certificate), puis cliquez sur **Naviguer** (Browse) pour charger le fichier du certificat.

Les réglages de RPV par défaut se servent de l'algorithme DES pour le chiffrement et SHA1 pour le prétraitement du message pour l'authentification. L'utilisateur peut définir manuellement les méthodes de chiffrement et d'authentification.

7. Pour permettre la configuration manuelle des méthodes de chiffrement et d'authentification choisissez **Utiliser des réglages manuels** (Use Manual Settings).

8. Choisissez la **Méthode de chiffrement** et la **Méthode d'authentification** désirées dans les menus déroulants.
9. Cliquez sur **Appliquer** (Apply).

➔ **Pour configurer la Connexion RPV de CheckPoint :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Réglages** apparaît.

2. Dans le carreau **RPV** cliquez sur **Visualiser les réglages** (View Settings)**.**

   L'écran Réglages de RPV apparaît.

3. Dans le champ **Adresse de Passerelle RPV** (VPN Gateway address) entrez l'adresse IP du serveur RPV à accès distant.
4. Dans le champ **Adresse du réseau distant** (Remote Network address) entrez l'adresse du réseau distant
5. Dans le champ **Masque du réseau distant** (Remote Network Mask) entrez le masque du sous-réseau distant.
6. Entrez le **Nom d'Utilisateur** et le **Mot de passe de l'Utilisateur.**
7. Dans le champ **Certificat** (Certificate), choisissez le fichier du certificat en utilisant le bouton **Navigation** (Browse).
8. Cliquez sur **Appliquer** (Apply).

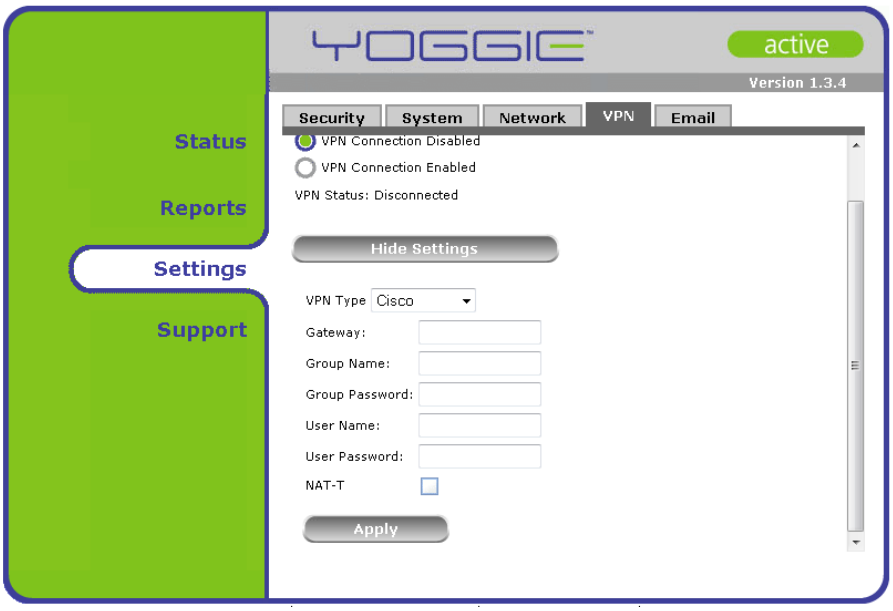
➔ **Pour configurer la connexion RPV de Cisco :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de Navigation de la Console de Gestion.

La page principale **Réglages** apparaît.

2. Dans le carreau **RPV** cliquez sur **Visualiser les réglages** (View Settings)**.**

   L'écran Réglages de RPV apparaît.



3. Dans le champ **Passerelle** (**Gateway)** entrez l'adresse IP du serveur éloigné de RPV.
4. Dans le champ **Nom du groupe** (Group name) entrez le Nom du groupe.
5. Dans le champ **Mot de passe du groupe** entrez le Mot de passe du groupe.
6. Entrez le **Nom de l'utilisateur** et le **Mot de passe de l'utilisateur**.
7. Choisissez la boîte à cocher **NAT-T**. NAT-T permet aux paquets IPsec (ESP) de passer via NAT.
8. Cliquez sur **Appliquer** (Apply).

Réglages de la protection contre les pourriels

Le pourriel est un courriel qui n'a pas été sollicité, souvent de nature commerciale, il a été envoyé indistinctement à des listes multiples de publipostage, à des individus, ou à des forums. L'hameçonnage comprend des escroqueries d'Internet conçus pour tromper les destinataires et les amener à révéler leur carte de crédit, mots de passe, numéros de Sécurité Sociale, et d'autres informations personnelles à des individus qui ont l'intention d'utiliser ces informations à des fins frauduleuses.

Le Gatekeeper Pico et le Gatekeeper Pico Pro assurent la protection contre les pourriels et l'hameçonnage en intégrant le puissant moteur *MailShell*™. Chaque courriel, entrant ou sortant, est examiné par le Gatekeeper Pico afin d'identifier et neutraliser toute menace à la sécurité de la même manière que toutes les données du réseau sont examinées. Ces menaces comprennent les virus, logiciels espions, et les contenus actifs. Ces courriels sont étiquetés par Yoggie™, et une des mentions suivantes est insérée dans la ligne du sujet :

- [Pourriel] (Spam)
- [Probablement Pourriel] (Probably Spam)
- [Hammeçonnage] (Phishing)

Le Gatekeeper Pico génère aussi des fichiers à deux en-têtes relatifs aux pourriels, qui peuvent être trouvés dans la source du message, ils comprendront les informations suivantes :

- **X-Yoggie-SpamScore** – le score exact de pourriels, de 0 à 100. 100 signifie que le courriel est entièrement du pourriel, 0 signifie que le courriel n'est absolument pas du pourriel.
- **X-Yoggie-SpamLevel** – Indique pourriel, probablement du pourriel, hammeçonnage, ou vide si ce n'est pas un pourriel.

Dans le programme d'e-mail de l'utilisateur, des règles peuvent être créées pour traiter ces courriels étiquetés. Par exemple, le programme d'e-mail peut automatiquement supprimer tous les courriels étiquetés par Yoggie comme étant des pourriels.

En sélectionnant ou désélectionnant la case à cocher **Lignes de sujet de l'étiquette relatives à la suspicion que les courriels sont des pourriels** (Tags subject subject lines of suspicious spam emails) **;** Vous pouvez définir si le Gatekeeper Pico ajoute ou n'ajoute pas ces étiquettes

➔ **Pour configurer les réglages de protection contre les pourriels :**

1. Cliquez sur **Réglages** dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans **l**e carreau d' Affichage.

2. Cliquez sur l'onglet **E-mail** (Email).

   L'écran **Réglages d'E-mail** apparaît.

3. Choisissez la boîte à cocher si vous désirez que le Gatekeeper Pico étiquette les lignes de sujet de courriels suspectés d'être des pourriels. Ces courriels comprendront des étiquettes dans leur ligne de sujet.
4. Cliquez sur **Appliquer**.

Vous pouvez configurer votre propre définition de pourriel en créant des **Règles sur mesure pour les courriels** (Custom Email Rules).

➔ **Pour ajouter une Règle sur mesure pour les courriels :**

1. Cliquez sur le bouton **+** (plus).
2. Entrez un **Nom de règle**.
3. Définissez la condition de règle, en vous servant du menu déroulant et de la **Boîte à formes** (Pattern)
4. Choisissez l'**Action** du menu déroulant. Choisissez **Permettre** (Allow) ou **Étiqueter avec** (Tag with), puis entrez l'étiquette de votre choix dans la boîte de droite.
5. Activez la règle en sélectionnant la boîte adéquate de la colonne **Active**.
6. Cliquez sur **Appliquer** (Apply).

La nouvelle règle sur mesure a été créée et activée.

➔ **Pour modifier une règle sur mesure pour les courriels :**

1. Double cliquez sur la règle que vous désirez modifier.
2. Éditez les champs adéquats.
3. Cliquez sur **Appliquer** (Apply)**.**

La règle sélectionnée a été modifiée.

➔ **Pour supprimer une règle sur mesure pour les courriels :**

1. Cliquez sur la règle que vous désirez supprimer.
2. Cliquez sur le bouton **-** (moins).
3. Cliquez sur **Appliquer** (Apply)**.**

La règle sélectionnée a été supprimée.

Réglages avancés de sécurité

Les réglages avancés de sécurité suivants peuvent être configurés via l'écran **Réglages avancés de sécurité** :

- **Filtrage Web /Contrôle parental du contenu (**Web Filtering / Parental Content Control) — Le Gatekeeper Pico peut bloquer des contenus de Web indésirables. Dans cette option de configuration avancée vous pouvez spécifier les catégories de contenus indésirables à bloquer.
- **Firewall** — Le Gatekeeper Pico peut bloquer les trafics indésirables sortant en utilisant des listes de numéros de ports, une liste blanche ou une liste noire.
- **Politique relative à la taille des fichiers** — Gatekeeper Pico peut examiner les fichiers de moins que 10 MB. Vous pouvez spécifier au Gatekeeper Pico de bloquer les fichiers de plus de 10 MB ou d'examiner jusqu'à la taille limite.
- **Protocoles** – Yoggie Pico utilise des scanneurs de couche d'application (anti-virus, anti-logiciels espions, anti-pourriel, anti-hammeçonnage, filtrage Web, etc.) sur différents protocoles de communication entrante. Dans cette option de configuration avancée vous pouvez activer ou désactiver le scannage au niveau de l'application de certains protocoles.
- **SDI/SPI –** Yoggie Pico dispose de la protection par SDI/SPI. Dans cette option de configuration avancée vous pouvez spécifier les politiques de sécurité pour chaque activité.

Filtrage Web / Contrôle parental du contenu

Le Gatekeeper Pico peut bloquer des contenus de Web indésirables. Dans cette option de configuration avancée vous pouvez spécifier les catégories de contenus indésirables à bloquer. Vous pouvez configurer votre propre définition de filtrage Web en créant des **Règles Web sur mesure** (Custom Web rules).

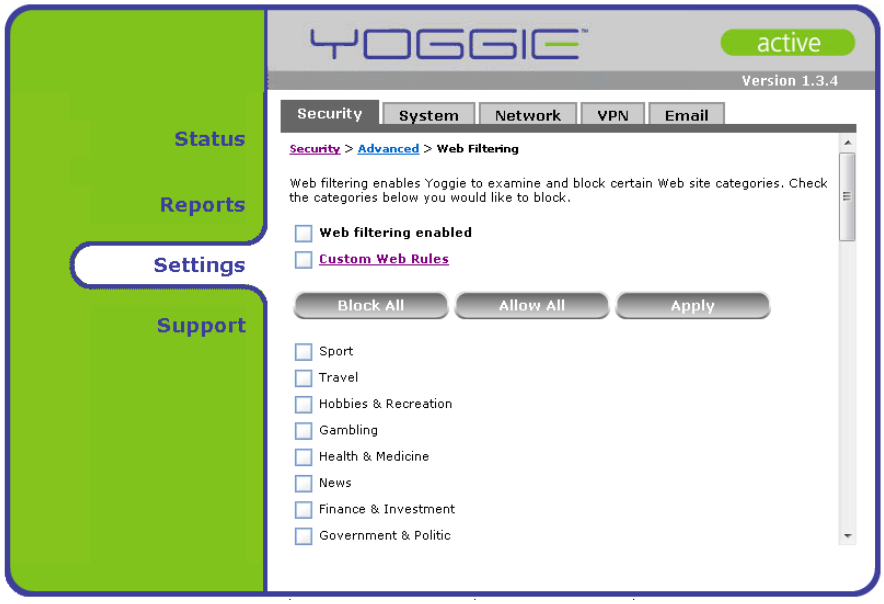
➔ **Pour configurer les catégories de filtrage Web :**

1. Cliquez sur **Réglages** dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur **Avancé** (Advanced)**.**
3. Cliquez sur **Filtrage Web** (Web filtering).

   L'écran de Filtrage Web apparaît.



4. Pour activer vos règles de filtrage Web sur mesure, choisissez la case à cocher **Filtrage Web activé** (Web Filtering enabled)**.**
5. Choisissez la case à cocher de la catégorie que vous désirez filtrer. Pour choisir toutes les catégories, cliquez sur **Bloquer tout** (Block All). Pour supprimer toutes les catégories, cliquez sur **Permettre tout** (Allow All).

➔ **Pour ajouter une règle de Web sur mesure :**

1. Cliquez sur le lien **Règles Web sur mesure** (Custom Web rules)

   La fenêtre **Règles Web sur mesure** apparaît.
2. Ajoutez une règle Web sur mesure en cliquant sur le bouton **+** (plus).
3. Entrez un **Nom de règle.**
4. Définissez la condition de la règle en utilisant le menu déroulant, puis entrez la forme.
5. Choisissez l'Action dans le menu déroulant.
6. Pour activer vos règles de filtrage Web sur mesure, choisissez la case à cocher **Règles Web sur mesure** (Custom Web rules).
7. Pour sauvegarder vos réglages, cliquez sur **Appliquer** (Apply).

➔ **Pour modifier une règle de Web sur mesure :**

1. Double cliquez sur la règle que vous désirez modifier.
2. Editez les champs pertinents.
3. Cliquez sur **Appliquer** (Apply).

   La règle choisie a été modifiée.

➔ **Pour supprimer une règle de Web sur mesure :**

1. Cliquez sur la règle que vous désirez supprimer.
2. Cliquez sur le bouton **-** (moins).
3. Cliquez sur **Appliquer** (Apply).

   La règle choisie a été supprimée.

   Le Gatekeeper Pico filtrera le contenu du Web selon les réglages spécifiés.

Firewall

Gatekeeper Pico peut bloquer un trafic sortant non désiré. Dans cette option avancée de configuration vous pouvez spécifier le trafic indésirable que vous aimeriez bloquer en utilisant la liste de numéros de ports. Vous pouvez optionnellement utiliser une *liste noire* (logiciels malveillants) pour lister les ports sur lesquels le trafic sortant doit être bloqué, ou une *liste blanche* pour spécifier que **tout** trafic sortant doit être bloqué **sauf** via les ports non cochés de la liste.

La politique sécuritaire par défaut prédéfinie spécifie que :

- Toutes les connexions entrantes sont bloquées, et
- Toutes les connexions sortantes sont permises, à l'exception de la liste noire prédéfinie.

Pour modifier la politique, vous pouvez :

- Ajouter des règles manuelles de politique pour le trafic entrant et le trafic sortant, et/ou
- Pour le trafic sortant, modifier la liste noire, ou spécifier la liste blanche (liste de ports acceptables) à utiliser.

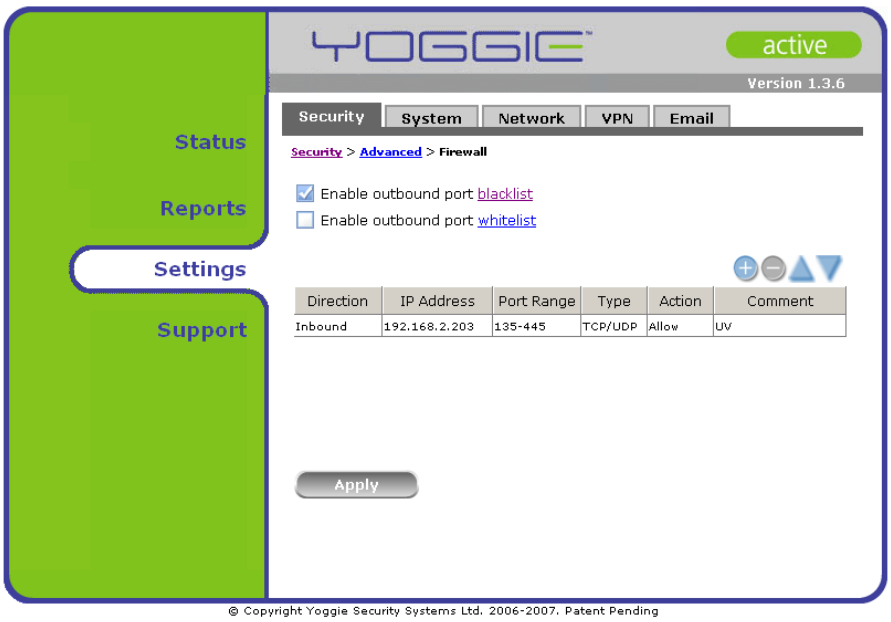
La convention suivante de priorité est appliquée :

- Les règles définies manuellement annulent (c'est à dire qu'elles ont la priorité sur) les spécifications de coches de la liste noire/liste blanche, qu'elle soit prédéfinies ou sur mesure.
- Lorsqu'il y a deux règles ou plus, une règle située plus haut dans la liste a la priorité sur celles se trouvant plus bas.
- Si la liste blanche et la liste noire sont toutes deux cochées, la liste blanche annule toute spécification dans la liste noire.

➔ **Pour activer /désactiver le blocage basé sur la liste noire/liste blanche :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.



2. Cliquez sur **Avancé (**Advanced).
3. Cliquez sur **Firewall**.
4. Pour désactiver le blocage du port de sortie (c'est à dire, pour permettre que tout le trafic sauf ce qui est spécifié par les règles de la partie inférieure de l'écran) décochez la première case à cocher, liste noire (Enable outbound blacklist) ; ou pour bloquer le port de sortie basé sur la liste noire, avant d'appliquer toute règle, cochez de nouveau cette case.

   Cochez la seconde case à cocher, liste blanche (Enable outbound whitelist) pour bloquer le trafic sortant basé sur la liste blanche (c'est à dire, pour permettre les ports cochés dans la liste blanche et bloquer **tous les autres**) ; ou pour ignorer la liste blanche décocher cette case.
5. Voir les procédures ci-dessous pour modifier la liste noire et la liste blanche.
6. Cliquez sur **Appliquer** (Apply).

   La politique sécuritaire est établie. (Veuillez noter que les réglages de la liste noire seront ignorés si une liste blanche est utilisée.)

➔ **Pour modifier la liste noire :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.
2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **Firewall**.

4. Cliquez sur le lien de la liste noire.

   Le dialogue de la liste noire s'ouvre.

5. Cochez tous les ports qui doivent être bloqués (c'est à dire, ceux compris dans la liste noire) et décocher tous les ports à autoriser.
6. Cliquez sur **Appliquer**.

   La politique sécuritaire est établie. (Pour activer /désactiver le blocage basé sur la liste noire, voir la procédure ci-dessus). Veuillez noter que les réglages de la liste noire seront ignorés si une liste blanche est utilisée.

➔ **Pour modifier la liste blanche :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **Firewall**.
4. Cliquez sur le lien de la liste blanche.

   Le dialogue **Liste blanche** s'ouvre.

5. Cochez tous les ports à autoriser (c'est à dire, ceux compris dans la liste blanche) et décocher tous les ports à bloquer.
6. Cliquez sur **Appliquer** (Apply).

   La politique sécuritaire est établie. (Pour activer /désactiver le blocage basé sur la liste blanche, voir la procédure ci-dessus)

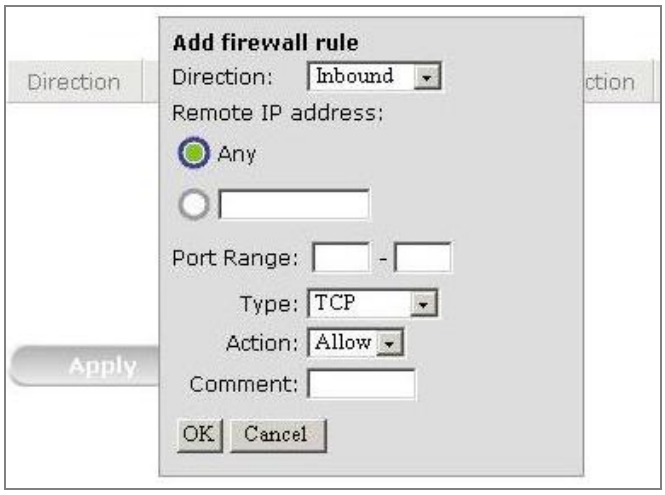
➔ **Pour créer et établir une séquence de règles de Firewall :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.

2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **Firewall**.
4. Appuyez sur le bouton rond **+** du côté droit du carreau.

   Le dialogue **Ajouter une règle de firewall** apparaît.



5. Spécifier les composants suivants de la règle :

   - **Direction :** trafic entrant (Inbound) ou sortant (Outbound).
   - **Adresse IP distante** (Remote IP address) **:** Pour le trafic entrant, spécifier la source ; ou, pour le trafic sortant, spécifier la destination : **Toute** (Any) destination, ou une adresse IP spécifique (par exemple, 192.168.2.2).
   - **Plage des ports :** Plage des numéros de ports (1 au minimum et 65 535 au maximum).
     Pour un port unique, utilisez le même numéro de port dans les deux cases. Ne laissez aucun des deux champs en blanc.
   - **Type :** UDP, TCP, ou les deux.
   - **Action :** Permettre ou bloquer le trafic.
   - **Commentaire** (Comment) **:** champ textuel libre pour votre usage personnel. Ce texte apparaît dans une colonne de la table de sommaire de l'onglet **Sécurité**.

6. Appuyez sur **OK**.

   La règle est ajoutée à la liste.

7. Répéter les opérations ci-dessus pour toutes les règles que vous désirez définir. Par exemple, vous pouvez créer plusieurs règles de blocage, et ensuite en ajouter une à la fin qui bloquera tous les autres trafics.

8. Pour recréer la séquence de la liste de règles :

   - Choisissez une règle puis utilisez les boutons à flèche triangulaire haut/bas pour déplacer cette règle vers le haut ou vers le bas dans la liste. (Rappelez-vous que les règles plus élevées dans la liste ont la priorité sur celles qui sont en dessous d'elles.)
   - Répéter pour toute autre règle que vous voulez repositionner.

9. Appuyez sur **Appliquer** (Apply) pour sauvegarder et appliquer les modifications.

➔ **Pour supprimer une règle de Firewall :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.
2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **Firewall**.
4. Choisissez la règle que vous désirez supprimer.
5. Appuyez sur le bouton rond **- (moins)** du côté droit du carreau.

   Après la confirmation de l'action, la règle est supprimée.

Politique relative à la taille

Le Gatekeeper Pico peut examiner des fichiers de moins que 10 MB. Vous pouvez spécifier au Gatekeeper Pico de bloquer des fichiers de plus que 10 MB ou d'examiner les fichiers jusqu'à la taille limite.

➔ **Pour configurer la politique relative à la taille :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.
2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **Politique relative à la taille** (Size Policy).

   L'écran de Politique relative à la taille apparaît.

4. Choisissez la boîte à cocher si vous désirez que le Gatekeeper Pico bloque tous les fichiers plus grands que 10 MB téléchargés du Web (HTTP). Ne pas sélectionner cette option signifie que ces fichiers passeront, mais que 10 MB de leur taille seront examinés.
5. Cliquez sur **Appliquer** (Apply).

   Gatekeeper Pico bloquera ou permettra les grands fichiers du Web selon les réglages spécifiés

Composants

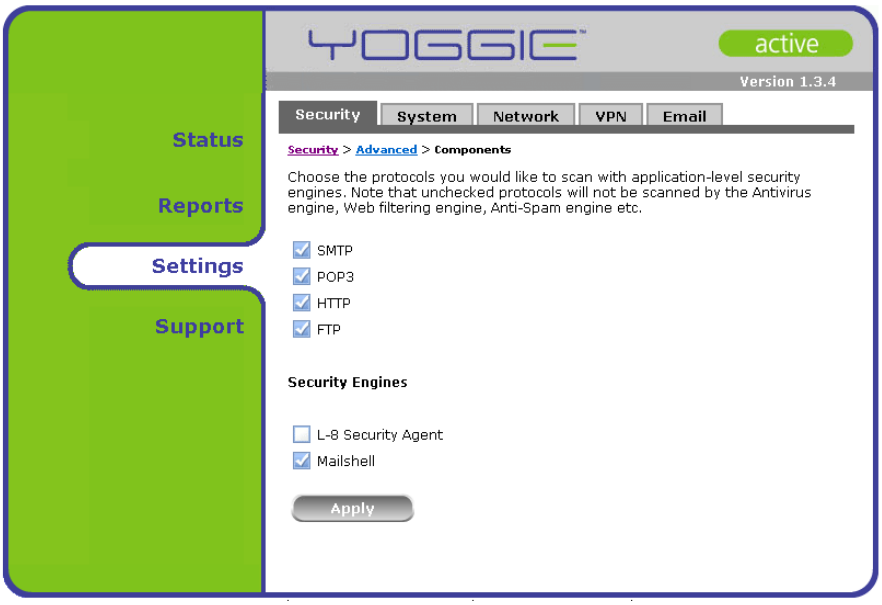
Le Gatekeeper Pico utilise des scanneurs et des moteurs de couche d'application (anti-virus, anti-logiciels espions, anti-pourriel, anti-hammeçonnage, filtrage Web, etc.) sur différents protocoles de communication entrante. Dans cette option avancée de configuration vous pouvez activer ou désactiver le scannage des niveaux des applications de certains protocoles et activer ou désactiver des moteurs des niveaux des applications.

➔ **Pour configurer l'examen du protocole :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans **l**e carreau d' **Affichage**.
2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **Composants** (Components).

   L'écran **Composants** apparaît.



4. Choisissez la boîte à cocher du protocole que vous désirez que Gatekeeper Pico examine. Ne pas sélectionner ces options signifie que le protocole ne sera pas examiné.
5. Choisissez la boîte à cocher du Moteur de Sécurité (Security Engines) que vous désirez que le Gatekeeper Pico utilise. Choisissez Mailshell si vous désirez activer les vérifications que les courriels ne sont pas des pourriels. Choisissez L-8 Security Agent™ de Yoggie (pour lequel une demande de brevet a été déposée) si vous désirez activer la protection de la couche 8.
6. Cliquez sur **Appliquer** (Apply).

   Gatekeeper Pico examinera les protocoles selon les réglages spécifiés.

SDI/SPI

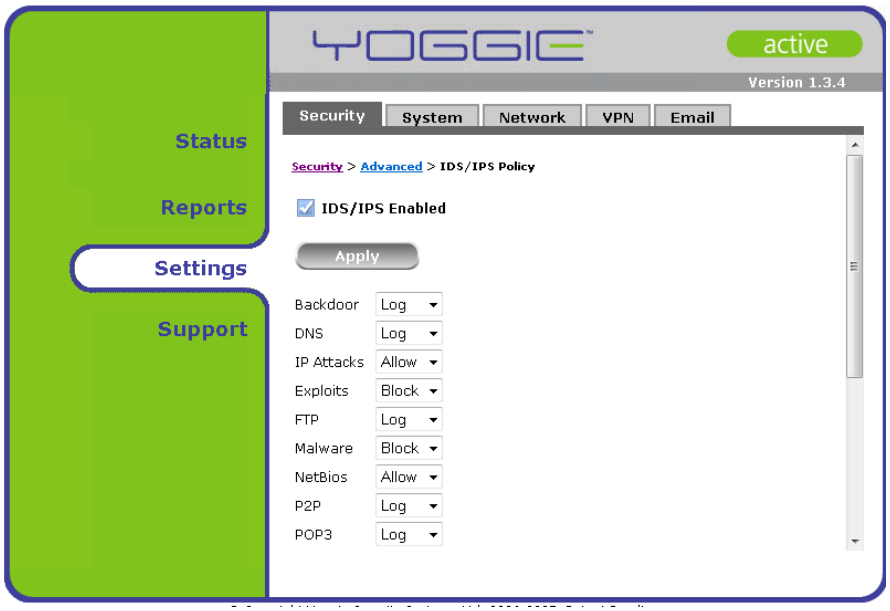
Gatekeeper Pico dispose de la protection SDI/SPI. Dans cette option de configuration avancée vous pouvez spécifier la politique de sécurité pour chaque activité.

➔ **Pour configurer la protection par SDI/SPI :**

1. Cliquez sur **Réglages** (Settings) dans le carreau de **Navigation** de la Console de Gestion.

   L'onglet **Sécurité** apparaît dans le carreau d' **Affichage**.
2. Cliquez sur **Avancé** (Advanced).
3. Cliquez sur **SDI/SPI** (IDS/IPS).

   L'écran **Politique de SDI/SPI** apparaît.



4. Choisissez la boîte à cocher **SDI/SPI Activé** (IDS/IPS enabled)**.**
5. Pour chaque activité/menace, choisissez dans le menu déroulant un des réglages suivants :

   - **Permettre** (Allow) – Le Gatekeeper Pico permettra cette activité et ne l'enregistrera pas dans un journal.
   - **Enregistrement** (Log) – Le Gatekeeper Pico permettra cette activité, et l'enregistrera dans un journal.
   - **Bloquer** (Block) – Le Gatekeeper Pico bloquera l'activité et l'enregistrera dans un journal.

6. Cliquez sur **Appliquer** (Apply).

Le Gatekeeper Pico exécutera la protection par IPS/IDS selon les réglages spécifiés.

Support

Dans de rares cas, vous pouvez avoir besoin de générer un fichier de support, de réamorcer, ou d'arrêter le système Gatekeeper Pico, comme décrit dans cette section.

Génération d'un fichier de support technique

Vous pouvez générer et sauvegarder un fichier de soutien qui contient tous les journaux du Gatekeeper Pico, les donnée de configuration, et d'autres informations pertinentes. Ensuite, ce fichier pourra être envoyé à un expert de soutien du Gatekeeper Pico pour qu'il l'analyse.

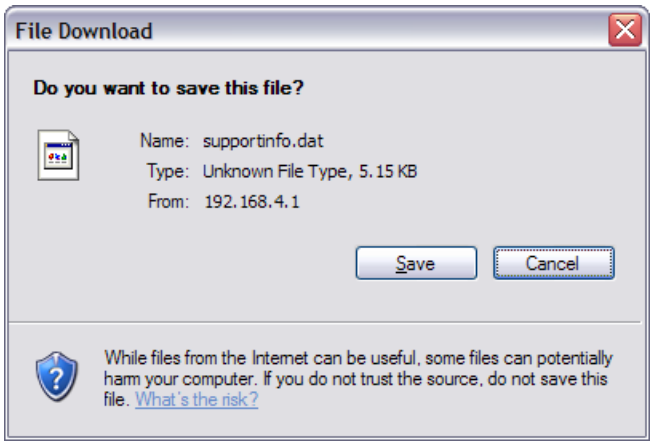
➔ **Pour générer un fichier de soutien :**

1. Cliquez sur **Soutien** (Support) dans le carreau de **Navigation** de la Console de Gestion.

   La page principale **Soutien** apparaît.

2. Dans l'onglet **Outils de soutien** (Support Tools), cliquez sur le bouton **Fichier de soutien** (Support File).

   Le fichier de soutien est généré, puis la boîte de dialogue **Chargement du fichier** (File Download) s'ouvre.



3. Notez le nom du fichier, puis cliquez sur **Sauvegarder** (Save).
4. Naviguez, puis choisissez l'emplacement vers lequel vous voulez sauvegarder le fichier de soutien.
5. Cliquez sur **Sauvegarder** (Save).

Options de remise à zéro

Pour dépanner, vous pouvez avoir besoin de remettre à zéro des journaux, des compteurs.

➔ **Pour remettre à zéro des compteurs du dispositif :**

1. Cliquez sur **Soutien** (Support) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Soutien** apparaît.

2. Dans l'onglet **Outils de soutien** (Support tools), Cliquez sur le bouton **Options de remise à zéro** (Reset Options)**.**

3. Choisissez le journal ou compteur que vous désirez supprimer.

Diagnostics

Vous pouvez assurer que votre Gatekeeper Pico protège votre ordinateur portatif en exécutant un contrôle diagnostic. Il se peut qu'il vous soit demandé d'exécuter le test de diagnostic suivant pendant une session de soutien :

- **Diagnostics généraux** (General Diagnostics) – exécutent des tests de diagnostic sur des applications sécuritaires du Yoggie Pico.
- **Diagnostics de Réseau** (Network Diagnostics) – exécute un test du Contrôleur de connexion et de trace.
- **Test de Virus** (Virus Test) – Une partie de ce test consiste à charger un fichier viral échantillon mais inoffensif, le Gatekeeper Pico le bloque et l'empêche d'atteindre votre ordinateur portatif.

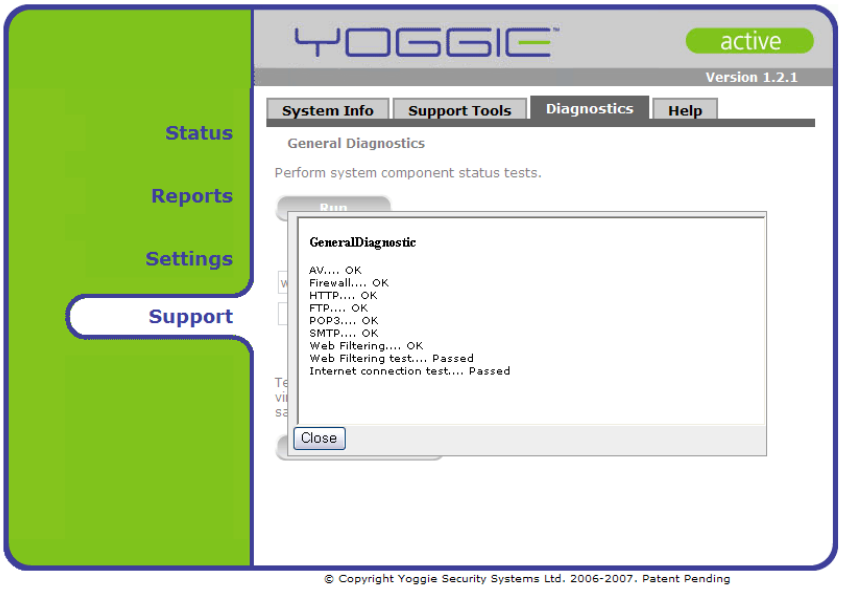
➔ **Pour exécuter les diagnostics généraux :**

1. Cliquez sur **Soutien** (Support) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Soutien** apparaît.

2. Dans l'onglet **Diagnostics**, sous **Diagnostics Généraux** (General Diagnostics) Cliquez sur le bouton **Exécuter** (Run).

   Le dialogue diagnostics généraux s'ouvre avec les résultats des divers tests.



➔ **Pour exécuter un diagnostic du réseau:**

1. Cliquez sur **Soutien** (Support) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Soutien** apparaît.

2. Dans l'onglet **Diagnostic**, sous **Diagnostics du réseau** (Network Diagnostics) entrez l'adresse IP ou le nom de l'ordinateur dans le champ suivant du bouton **Contrôleur de connexion** (Ping).

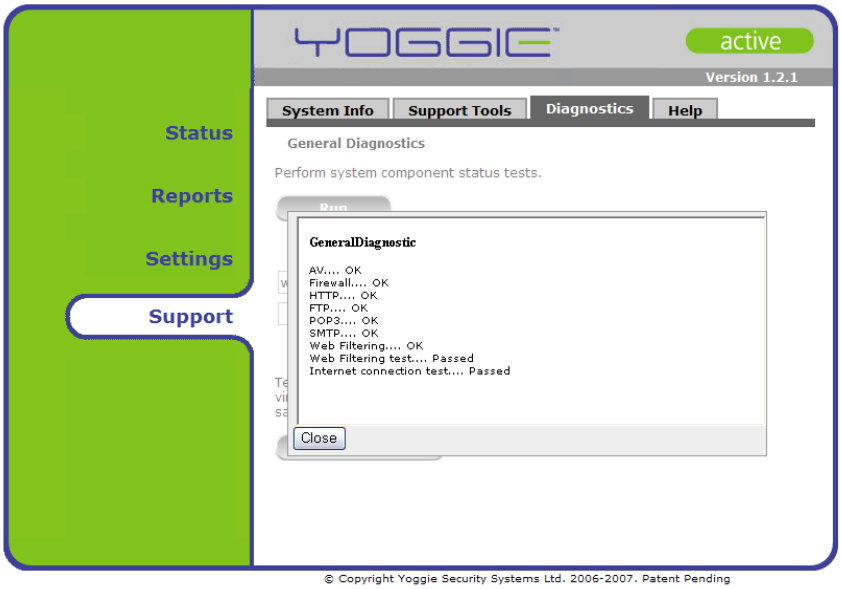
3. Cliquez sur **Contrôleur de connexion** (Ping).

   Le dialogue de statistique du Contrôleur de connexion s'ouvre.

4. Pour exécuter une trace, entrez l'adresse IP ou le nom de l'ordinateur dans le champ suivant au bouton **Trace**.

5. Cliquez sur **Trace**.

   Le dialogue diagnostics généraux s'ouvre avec les résultats des divers tests.



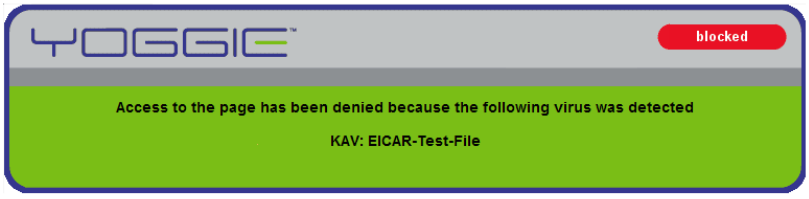
➔ **Pour passer le fichier de test de virus :**

1. Cliquez sur **Soutien** (Support) dans le carreau de Navigation de la Console de Gestion.

   La page principale **Soutien** apparaît.

2. Dans l'onglet **Diagnostics**, Cliquez sur le bouton **Test**.

   Le fichier est téléchargé, puis bloqué par le Gatekeeper Pico et le message suivant apparaît :



L'accès à cette page a été refusé parce que le virus suivant a été détecté Kav:EICAR-Test-File.

Restriction de l’accès à internet grâce au gatekeeper pico

Une des caractéristiques du Gatekeeper est de ne permettre l’accès à internet que lorsque celui-ci est inséré est connecté à votre ordinateur, quel que soit votre mode de connexion.

Dans certain cas (si le Gatekeeper Pico a été endommagé ou perdu) vous pouvez souhaiter accéder à internet sans utiliser votre gatekeeper, dans ce cas vous devez désactiver le Gatekeeper Pico. Dès que le Gatekeeper Pico est désactivé, vous pouvez continuer à travailler avec une connexion de réseau. Toutefois, ceci doit être fait avec précaution vu que toute la protection assurée par le Gatekeeper Pico est désactivée.

Désactivation des restrictions d'utilisation du Gatekeeper Pico

➔ **Pour désactiver la protection par le Gatekeeper Pico :**

1. Cliquez avec le bouton droit sur l'icône du Gatekeeper Pico dans la zone de notification.
2. Choisissez **Désactiver la protection** (Disable protection) dans le menu déroulant affiché.

   La boîte de dialogue **Désactiver la protection** s'ouvre.
3. Entrez le mot de passe de désactivation de la protection dans le champ **Mot de passe** (Password).

Le mot de passe par défaut de désactivation de la protection est `yoggie`. Si vous êtes un utilisateur de l'entreprise, contactez l'administrateur de votre système pour obtenir le mot de passe. Le mot de passe que vous recevrez sera temporaire.

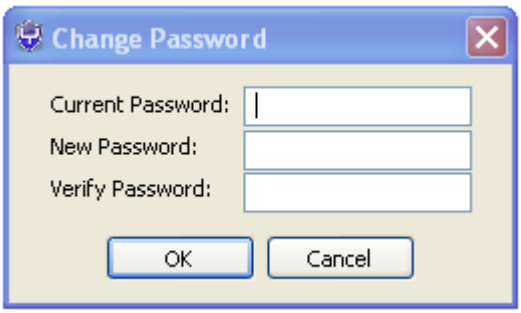
Changement du mot de passe des restrictions d'utilisation du Gatekeeper

À tout moment vous pouvez changer le mot de passe de l'imposition (le mot de passe utilisé pour désactiver l'imposition).

➔ **Pour changer le mot de passe de l'imposition :**

1. Cliquez avec le bouton droit sur l'icône du Gatekeeper Pico dans la zone de notification.
2. Choisissez **Changer le mot de passe (**Changer Password) dans le menu affiché en mode fenêtre.

La boîte de dialogue **Changer le mot de passe** s'ouvre.



3. Entrez le mot de passe actuel de désactivation dans le champ **Mot de passe actuel** (Current Password).
4. Entrez le nouveau mot de passe dans le champ **Nouveau mot de passe** (New Password).
5. Entrez le nouveau mot de passe encore une fois dans le champ **Vérifier le mot de passe** (Verify Password).
6. Cliquez sur **OK**.

Le nouveau mot de passe est établi.

Désinstallation du Gatekeeper Pico

Le Gatekeeper Pico peut être désinstallé à tout moment.

➔ **Pour désinstaller le Gatekeeper Pico :**

1. À partir du menu **Démarrage** (Start), choisissez **Programmes (Programs)** >**Yoggie**> **Désinstaller Yoggie** (Uninstall Yoggie).

   L'assistant **Désinstallation** s'ouvre.

2. Entrez le mot de passe de **Désinstallation** dans le champ **Mot de passe** (Password).

Le mot de passe par défaut de désinstallation est yoggie. Si vous êtes un utilisateur de l'entreprise, contactez l'administrateur de votre système pour obtenir le mot de passe.

Spécifications techniques

Composants	
UCT	Intel XScale PXA270 à 520MHz
Mémoire NAND Flash	128 MB
Mémoire NOR Flash	8 MB
Mémoire SDRAM	128 MB
Interface	
USB	USB 2.0
Indicateurs à LED	Alimentation, Événement sécuritaire, Mise à jour
Conditions environnementales	
Dimensions	Longueur : 63 mm [2,48 pouce]; largeur : 23 mm [0,91 pouce]; Épaisseur : 12 mm / 16 mm [0,47 pouce / 0,63 pouce] (Capuchon enlevé / avec le capuchon)
Poids	18 grammes/0,6 oz
Puissance	2 W Max
Conformité environnementale	FCC Classe B; CE; Rohs
Température environnementale de fonctionnement.	0° à 40° C (32° à 104° F)
Température de stockage.	-20° à 70° C (4° à 185° F)
Fonctionnement - Humidité	10 à 80% sans condensation
Stockage - Humidité	5 à 90% sans condensation