



# Manuel de l'utilisateur

## **Avertissements juridiques**

Aucune partie de ce document ne peut être reproduit, stocké dans un système de recherche documentaire ou transmis, sous quelque forme et par quelque moyen, électronique ou mécanique, par photocopie ou enregistrement, ou autre, que ce soit sans l'accord préalable du propriétaire des droits réservés.

Copyright © 2008 Race River Corporation Pty Ltd.

Tous droits réservés.

# Table des matières

1	Introduction.....	3
1.1	Bienvenue dans Integard Edition Familiale .....	3
1.2	Configuration requise .....	3
1.3	Installation du logiciel Integard .....	3
2	Caractéristiques Integard.....	4
3	Administration.....	5
3.1	Écran d'état.....	6
3.2	Paramètres utilisateur .....	7
3.3	Paramètres système .....	12
3.4	Restrictions d'applications.....	15
3.5	Mots-clés .....	17
3.6	Informations personnelles .....	18
3.7	Sites autorisés .....	19
3.8	Sites bloqués .....	19
3.9	Génération de compte-rendu .....	20
4	Informations complémentaires.....	21
4.1	Mises à jour automatiques de données.....	21
4.2	Utilisation d'Integard avec un pare-feu et un logiciel antivirus .....	21
4.3	Notifications par e-mail.....	21
4.4	Contournement d'Integard .....	22
4.5	Précautions générales .....	22
5	Dépannage.....	23
5.1	Integard bloque trop.....	23
5.2	Integard ne bloque pas les pages qu'il devrait. ....	23
5.3	Logiciel antivirus et pare-feux personnels .....	24
6	Désinstallation d'Integard.....	25

# 1 Introduction

## 1.1 Bienvenue dans Integard Edition Familiale

Une fois installé sur votre PC, Integard bloque, filtre et consigne les opérations de navigation sur internet, vous permettant ainsi d'empêcher à vos enfants d'accéder à des images à caractère sexuel ou à du contenu pour adultes.

Grâce à l'interface d'administration Integard (« Gestionnaire Integard »), vous pouvez personnaliser le niveau d'accès et de filtrage pour chaque utilisateur de l'ordinateur.

## 1.2 Configuration requise

Système d'exploitation	Microsoft Windows XP, 2000, ME, 98SE
Navigateur Internet	Internet Explorer 5, 6 et 7, Opera 8, 9 ou Firefox
Mémoire vive	64 Mo de RAM minimum
Espace disque	10 Mo minimum sur le disque dur
CPU	Pentium II ou supérieur

## 1.3 Installation du logiciel Integard

Rapide et facile à installer, Integard commence le filtrage sans aucun besoin de configuration supplémentaire.

Le profil utilisateur Integard « par défaut » est automatiquement créé avec le niveau de filtrage défini durant l'installation.

Veillez consulter le Manuel de démarrage rapide pour obtenir le détail de la procédure d'installation.

## 2 Caractéristiques Integard

Le tableau suivant résume les caractéristiques du logiciel Integard.



Caractéristique	Description
<b>Filtrage de contenu</b>	Integard bloque les pages internet dont le contenu est inapproprié pour des enfants. Integard est fourni avec une base de données complète de sites internet et de mots clés continuellement mis à jour.
<b>Surveillance « chat » / messagerie instantanée (IM)</b>	Contrôle et enregistre les conversations en ligne pour protéger les enfants des personnes malveillantes et de la « cyberintimidation ». Génère des e-mails d'alerte si des termes douteux ou inappropriés sont employés.
<b>Surf sur sites autorisés uniquement</b>	Limite l'accès aux sites spécifiés par les parents ou l'administrateur. Tout autre site peut être bloqué.
<b>Administration Web</b>	Configure Integard et contrôle l'utilisation du navigateur à partir d'un même PC ou sur le réseau entier.
<b>Mots clés et liste de sites choisis par l'utilisateur</b>	Définissez vos propres règles de blocage à l'aide de mots-clés, de phrases et d'adresses de sites internet.
<b>Protection des informations personnelles</b>	Empêche les informations personnelles contenues dans votre PC d'être envoyées vers l'extérieur.
<b>Écrasement instantané</b>	Écrase les blocages de pages internet et les limites de temps rapidement et facilement via le mot de passe administrateur.
<b>Recherche sécurisée</b>	Oblige les moteurs de recherche classiques à passer en mode sécurisé, ce qui limite les résultats des recherches. Cette fonction vient s'ajouter aux fonctions de blocage et de filtrage automatique du logiciel Integard, permettant ainsi d'obtenir un outil de protection puissant et convivial.
<b>Notifications par e-mail</b>	Vous pouvez décider de recevoir par e-mail un compte-rendu résumé des alertes internet ou chat du jour ainsi que des notifications immédiates.
<b>Paramétrage de limites de données</b>	Limite la quantité de données qu'un utilisateur peut consulter dans la journée. Idéal pour les familles ayant instauré un plan de restriction de l'utilisation d'Internet. Peut également calculer la quantité de données téléchargées vers le PC ou vers internet.
<b>Paramétrage des limites de temps</b>	Limite la durée d'utilisation d'internet pour les utilisateurs.

<b>Contrôle à distance</b>	Contrôle à distance l'utilisation d'internet à partir d'un autre ordinateur installé à la maison ou au travail.
<b>Blocage du partage de fichier P2P</b>	Peut bloquer les applications de partage de fichiers poste à poste (P2P).
<b>Prise en charge de liste blanche externe</b>	Intégré des sites internet recensés dans une liste blanche externe, comme <a href="http://www.openwhitelist.com">www.openwhitelist.com</a> par exemple.
<b>Mode furtif</b>	Integard peut garder un profil bas et faire passer les blocages de pages internet pour des erreurs de réseau.

### 3 Administration

La configuration d'Integard s'effectue via l'administrateur Integard.

Vous pouvez y accéder de l'une des manières suivantes.

1. Menu Démarrer -> Programmes -> Integard – Gestionnaire.
2. Cliquez avec le bouton droit sur l'icône  dans la zone de notification (en bas à droite de l'écran), puis choisissez Gestionnaire.
3. Double-cliquez avec le bouton gauche sur l'icône Integard  dans la zone de notification (en bas à droite de l'écran).
4. Ouvrez un navigateur et tapez <http://integard> ou <http://127.0.0.2> sur l'ordinateur sur lequel Integard est installé.
5. Vous pouvez également utiliser un autre ordinateur du même réseau local avec l'adresse IP du PC sur lequel Integard est installé. Exemple: <http://192.168.0.3:18881>

Lorsque la page de connexion Integard s'affiche à l'écran, entrez le mot de passe utilisé lors de l'installation.

Une fois connecté, vous pouvez accéder à différentes pages de configuration, comme indiqué ci-dessous.

Commande du menu	Description
<b>État d'Integard</b>	Aperçu rapide de l'état d'Integard.
<b>Paramètres utilisateur</b>	Permet de personnaliser les paramètres d'accès de chaque utilisateur à internet et de créer de nouveaux utilisateurs.
<b>Paramètres système</b>	Configuration système du logiciel Integard, telle que le mot de passe et l'adresse e-mail.

<b>Limites du programme</b>	Autorise ou restreint l'accès à internet ou l'exécution d'applications données.
<b>Mots-clés</b>	Permet de définir les mots-clés ou les phrases qui entraîneront le blocage d'une page.
<b>Infos personnelles</b>	Permet de spécifier les informations personnelles qui ne doivent pas être envoyées vers l'extérieur, à d'autres personnes ou sites, via internet.
<b>Sites autorisés</b>	Permet de définir une liste de sites autorisés au niveau système.
<b>Sites bloqués</b>	Permet de définir une liste de sites bloqués au niveau système.
<b>Génération de compte-rendu</b>	Permet de générer des comptes-rendus détaillés ou résumés de l'utilisation d'internet, par utilisateur.
<b>Déconnexion</b>	Déconnexion de l'administrateur Integard.

Les sections suivantes vous présentent en détail les différentes commandes introduites dans le tableau précédent.

### **3.1 Écran d'état**

L'écran d'état Integard présente, sur une page, des informations sur la version et l'état actuel du logiciel, les détails de l'abonnement, l'utilisateur actuellement connecté, l'heure système et l'heure Integard.

#### **3.1.1 Version**

Cette section affiche la version d'Integard et de la base de données de filtrage de sites internet en cours d'exécution et d'utilisation.

#### **3.1.2 État**

La section État indique si Integard est actuellement lancé ou non. Lorsqu'Integard est lancé, il contrôle, filtre et consigne toutes les connexions internet.

Lorsque le logiciel est désactivé, il autorise le transfert de toutes les données internet, sans restrictions. Dans cet état, il est également impossible de s'identifier.

Cette section affiche également l'heure système et l'heure Integard, et indique quelle heure est utilisée par le logiciel pour calculer les éventuelles limites de temps définies.

#### **3.1.3 Utilisateurs Integard**

Cette section affiche le nom de l'utilisateur Windows et de l'utilisateur Integard actuellement connecté au logiciel, ainsi que leurs droits d'utilisation pour la session en cours. Pour de plus amples informations et une présentation détaillée de l'utilisation d'internet, veuillez consulter la section « Génération de compte-rendu ».

#### **3.1.4 État de l'abonnement**

Cette section indique si vous utilisez la version d'évaluation (valable 14 jours) ou si votre abonnement est actif.

L'abonnement Integard fait référence au téléchargement des données de filtrage et

de sites internet ainsi que des mises à jour logicielles, lorsqu'elles sont disponibles.

A la fin de la période d'évaluation de 14 jours, le PC ne peut plus se connecter à internet tant que le logiciel Integard n'est pas activé via un numéro de série.

Vous pouvez vous abonner à Integard en ligne à l'adresse suivante :

<http://www.integard.com>.

Vous pouvez également désactiver ou désinstaller Integard en utilisant le mot de passe Administrateur.

## **3.2 Paramètres utilisateur**

Cet écran affiche sous forme de tableau tous les utilisateurs déjà créés, et vous donne la possibilité d'en créer de nouveaux. Lors de la création d'un nouvel utilisateur, les options sont les suivantes.

### **3.2.1 Paramètres généraux**

#### **Nom d'utilisateur**

Le nom d'utilisateur est utilisé pour permettre à différents utilisateurs de se connecter à Integard. Si plusieurs utilisateurs sont configurés, chacun d'entre eux doit se connecter à l'aide d'un mot de passe pour pouvoir accéder à internet.

#### **Nom complet**

Pour être plus explicite, le nom affiché sur divers écrans et comptes-rendus est le nom complet.

#### **Mot de passe**

Le mot de passe est obligatoire pour pouvoir utiliser internet, à moins que l'utilisateur ne soit désigné comme utilisateur « par défaut » dans les paramètres système.

### **3.2.2 Paramètres de filtrage**

#### **Configurations prédéfinies**

Les configurations prédéfinies sont un moyen rapide et facile de choisir un niveau de filtrage en fonction de l'âge de l'utilisateur.

Vous pouvez personnaliser le niveau de filtrage de manière plus complète, en utilisant l'option « Éditer utilisateur » accessible en cliquant sur le nom de l'utilisateur, dans les paramètres utilisateur.

<b>Valeur prédéfinie</b>	<b>Description</b>
Jeune enfant	Protection maximale pour les enfants de moins de 10 ans.

Jeune adolescent	Filtrage de sites internet de la même catégorie que pour un jeune enfant, mais légèrement moins restrictif. Adapté aux enfants entre 11 et 15 ans, selon le choix des parents ou du tuteur.
Adolescent plus âgé	Destiné aux adolescents de plus de 16 ans qui pourraient s'intéresser à des sujets habituellement réservés aux adultes. La navigation internet est moins restrictive mais les contenus explicites et extrêmes sont tout de même bloqués.
Adulte – Accès restreint	Cette option de configuration permet une liberté maximale de navigation tout en bloquant les sites internet à caractère extrêmement violent, grossier ou sexuel.
Adulte – Accès libre	Dans cette configuration, aucune page internet n'est filtrée.

### 3.2.3 Mode de filtrage

Mode de filtrage	Description
Analyse dynamique et sites autorisés	Tous les sites internet sont accessibles, dans la mesure où ils n'apparaissent pas dans une catégorie bloquée de la liste des « Catégories de sites internet » ci-dessous. Ce mode, qui peut avoir pour effet de bloquer une grande partie des pages internet, est généralement utilisé en conjonction avec une liste blanche ou une liste de sites autorisés définie par l'utilisateur.
Mode sites autorisés seulement	Tous les sites internet seront bloqués, à l'exception de ceux appartenant à une catégorie autorisée, ou figurant dans la « liste de sites autorisés » définie par l'utilisateur.
Blocage de tous les accès internet	L'utilisateur ne peut se connecter à internet.
Aucun filtrage	L'utilisateur n'est pas limité par la liste des catégories ou celle des sites bloqués. Tous les sites internet sont donc accessibles.

### 3.2.4 Sensibilité de filtrage

Chaque site internet visité est contrôlé par rapport à une base de données de sites connus ; si la catégorie à laquelle il appartient est bloquée, alors l'accès au site sera bloqué également. Si le site ne fait pas partie de la base de données, Integard analyse la page et détermine automatiquement sa catégorie. La sensibilité du moteur d'analyse peut être définie par niveaux.

Niveau de sensibilité	Description
Niveau 1	Blocage maximal
Niveau 2	Très élevé
Niveau 3	Élevé
Niveau 4	Moyen
Niveau 5	Faible
Niveau 6	Très faible
Niveau 7	Blocage minimal

### 3.2.5 Recherche d'image

La fonction Integard de « recherche d'image » oblige les moteurs de recherche classiques à passer en mode sécurisé, ce qui limite les résultats des recherches. Cette fonction ajoute au filtrage effectué par Integard une couche de protection

supplémentaire.

### **3.2.6 Filtre géographique**

Le « filtre géographique » permet un filtrage plus poussé des sites pour adultes difficilement détectables. Il bloque l'accès aux sites reliés à des serveurs de pays non anglophones. Si vous désirez débloquer un site bloqué, vous pouvez l'ajouter à la « liste des sites autorisés » ou désactiver cette fonction de filtrage supplémentaire.

### **3.2.7 Filtre HTTPS**

Le « filtre HTTPS » bloque toutes les connexions HTTPS/SSL. Ce filtre fournit une meilleure protection contre les serveurs mandataires (*proxy*) qui pourraient servir à contourner le logiciel Integard. Il bloque l'accès à la plupart des sites accessibles par connexion, comme les sites bancaires ou les messageries. Si ce filtre est trop restrictif, vous pouvez le désactiver.

### **3.2.8 Catégories de sites internet**

Dans cette section, vous sélectionnez les catégories de sites auxquelles l'utilisateur aura accès. Pour accélérer le processus de configuration, vous pouvez également sélectionner des configurations prédéfinies.

### **3.2.9 Options Chat/IM**

Applications Chat/IM Autorise ou bloque l'accès à toutes les applications de « chat » (aussi appelé « clavardage »).

Lorsque cette option est paramétrée sur « Autoriser », les applications de chat suivantes peuvent être utilisées : MSN Messenger, Yahoo Messenger, ICQ, AOL Instant Messenger, Myspace Messenger et IRC.

Si elle est paramétrée sur « Bloquer », tous les programmes de discussion en ligne mentionnés ci-dessous, plus d'autres, seront théoriquement bloqués.

### **3.2.10 Autres applications**

Dans cette section, tous les accès aux services de messagerie, de FTP et les forums peuvent être autorisés ou bloqués, et une fonction de connexion peut être activée. Les services de messagerie peuvent également être surveillés ; tout langage inapproprié, mot-clé ou information personnelle envoyée par e-mail générera une alerte par l'envoi d'un e-mail à la personne concernée, contenant le destinataire du message, la personne à l'origine du message, l'heure d'envoi et l'objet du message. Cette fonction n'est disponible que pour les clients de messagerie basés sur serveur POP3 et SMTP. Les fichiers journaux peuvent être consultés dans la section de génération de compte-rendu de l'administrateur Integard.

Remarque : Le filtrage des forums prend en charge principalement les forums basés sur protocole NNTP, comme Microsoft Outlook Express. Il ne permet aucun contrôle des forums internet.

### **3.2.11 Sites internet autorisés**

Cette fonctionnalité vous permet de définir les sites internet auxquels un utilisateur donné aura accès. Les sites répertoriés dans cette liste ne sont autorisés que pour cet utilisateur.

### **3.2.12 Sites bloqués**

Cette fonctionnalité vous permet de définir les sites internet auxquels un utilisateur donné ne pourra avoir accès. Les sites répertoriés dans cette liste ne sont bloqués que pour cet utilisateur.

### **3.2.13 Page de blocage personnalisée**

Cette fonctionnalité vous permet de choisir entre la page de blocage standard, la page de blocage standard personnalisée avec un message, ou une page internet personnelle.

### **3.2.14 Paramétrage des limites de temps et de données**

Limite de temps quotidien : La limite de temps quotidien vous permet d'allouer à chaque utilisateur un nombre de minutes maximum par jour pour l'accès internet.

Limite de données quotidien : La limite de données quotidiennes vous permet de définir pour chaque utilisateur un quota de données maximum. Tous les téléchargements sont pris en compte : du PC vers les serveurs et des serveurs vers le PC.

Lorsque les limites de données ou de temps sont atteintes, l'utilisateur ne peut plus accéder aux sites internet, envoyer/recevoir des e-mails ou discuter sur internet. Mais cela ne les empêche de continuer à utiliser leur ordinateur hors connexion.

### **3.2.15 Paramétrage des heures d'accès quotidiennes**

Dans cette section, vous pouvez configurer les heures de la journée pendant lesquelles un utilisateur peut accéder à internet.

## **3.3 Paramètres système**

### **3.3.1 Paramètres généraux**

#### **Adresse e-mail**

Integard peut envoyer à cette adresse des comptes-rendus journaliers et des alertes relatives aux sites internet bloqués ou aux discussions internet inappropriées. Cette adresse sert également à recevoir les informations de connexion en cas de mot de passe oublié. En raison des informations contenues dans ces e-mails, il est important de s'assurer que l'e-mail envoyé à l'adresse définie ne peut être lu par les utilisateurs non autorisés.

#### **Mode furtif**

Lorsque le mode furtif est activé, l'activité d'Integard devient invisible aux yeux de l'utilisateur. L'icône de la zone de notification (en bas à droite de l'écran) est supprimée et les pages bloquées affichent un message d'erreur, comme si le site internet était indisponible. L'utilisateur pense alors que le site auquel il essaye d'accéder est en maintenance, et non que son accès est bloqué.

#### **Désactivation du pare-feu**

Integard intègre un pare-feu qui empêche certains logiciels d'accéder à internet. Vous pouvez choisir d'ajouter un programme ou un port particulier à la liste des sites autorisés, mais vous pouvez également choisir de désactiver le pare-feu totalement. Lorsque le pare-feu est désactivé, Integard filtre et contrôle uniquement les ports de messagerie instantanée, d'internet et de messagerie électronique.

#### **Compter téléversements**

Integard est capable de limiter les accès internet en fonction de la quantité de données consommées par l'utilisateur en mégaoctets. Certains plans internet prennent comme base de limitation les téléchargements de serveur à PC uniquement. D'autres plans prennent en compte tous les types de téléchargement. Si seuls les téléchargements de serveur à PC sont pris en compte, il est inutile de cocher cette case. Si la limitation se base sur tous les types de téléchargement (PC à serveur internet – aussi appelé « téléversement » - et vice-versa), cette case devrait être cochée.

#### **Nom d'utilisateur Windows**

Lorsque cette case est cochée, Integard essaie de sélectionner le profil utilisateur dont le nom d'utilisateur correspond au nom de l'utilisateur actuellement connecté sous Windows. S'il est impossible d'effectuer cette correspondance, Integard choisit le nom d'utilisateur paramétré dans le champ « Utilisateur par défaut » ci-dessous.

#### **Création automatique d'utilisateur**

Cette fonctionnalité permet à un utilisateur Windows qui se connecte, et dont le nom d'utilisateur ne correspond à aucun nom d'utilisateur Integard, de se voir attribuer automatiquement un profil Integard à partir des paramètres par défaut définis dans le logiciel.

### **Utilisateur par défaut**

L'utilisateur par défaut est l'utilisateur qui est automatiquement identifié à au démarrage de l'ordinateur si le nom d'utilisateur Windows n'est pas sélectionné ou s'il n'y a aucune correspondance entre les noms d'utilisateur Windows et Integard. Pour vous connecter avec un autre utilisateur, il vous suffit de faire un clic droit sur l'icône Integard de la zone de notification, de choisir « Déconnexion utilisateur » dans le menu, puis de vous connecter avec un autre utilisateur.

### **Mot de passe administrateur**

Le mot de passe administrateur permet d'accéder aux pages d'administration Integard. Il est également utilisé pour écraser les blocages paramétrés et désactiver ou réinstaller Integard.

### **Confirmer mot de passe**

Le mot de passe doit être entré deux fois pour détecter les éventuelles fautes de frappe lors du changement du mot de passe administrateur.

## **3.3.2 Comptes-rendus et alertes automatiques**

### **Serveur SMTP**

Le serveur SMTP doit être spécifié pour pouvoir activer la notification automatique d'alertes et recevoir les comptes-rendus journaliers. Demandez à votre fournisseur d'accès internet ou regardez dans les paramètres de votre client de messagerie pour savoir quelle valeur de SMTP entrer.

### **Adresse expéditeur pour les notifications**

L'adresse de messagerie de l'expéditeur (« De ») pour les alertes et les comptes-rendus automatiques journaliers peut être configurée ici. Si ce champ n'est pas renseigné, Integard utilisera par défaut l'adresse de messagerie de l'administrateur configurée ci-dessus.

### **Nom d'utilisateur et mot de passe SMTP**

Certains serveurs SMTP nécessitent un nom d'utilisateur et un mot de passe pour pouvoir utiliser leurs services. Si c'est le cas, vous pouvez entrer les détails ici pour utiliser la fonction d'authentification du serveur SMTP. Si vous avez un doute, contactez votre fournisseur d'accès internet.

### **Envoi de comptes-rendus journaliers**

Permet d'activer la génération et l'envoi d'un compte-rendu journalier à l'adresse mentionnée plus haut. Le compte-rendu dresse la liste des accès internet pour chaque utilisateur sur les 7 derniers jours. (Nécessite le paramétrage du serveur SMTP)

### **Envoi d'e-mail après blocage de contenu de site internet**

Permet d'activer l'envoi automatique d'e-mail à chaque fois qu'un accès à un site internet est bloqué suite à un filtrage de contenu. Cette fonction ne permet pas d'envoyer d'e-mail de notification lorsque une action est bloquée en raison d'un dépassement de quota de temps ou de données. (Nécessite le paramétrage du serveur SMTP)

### **Envoi d'e-mail après détection d'informations personnelles**

Permet d'activer l'envoi automatique d'e-mail à chaque fois que l'envoi d'informations personnelles vers l'extérieur est bloqué. (Nécessite le paramétrage du serveur SMTP)

### **3.3.3 Serveur mandataire (proxy)**

#### **Utilisation d'un serveur mandataire**

Si votre connexion internet nécessite l'utilisation d'un serveur mandataire, cochez cette case et entrez les détails du serveur mandataire plus bas.

Remarque : N'activez et ne paramétrez l'utilisation d'un serveur mandataire que si vous êtes certain de l'exactitude de la configuration ; de mauvais paramètres pourraient empêcher toute tentative de connexion à internet.

#### **Serveur mandataire**

Nom ou adresse IP du serveur mandataire.

#### **Port du serveur mandataire**

Numéro de port du serveur mandataire (1 à 65535)

### **3.3.4 Liste blanche externe**

Cette fonctionnalité peut être utilisée pour charger une liste blanche à partir d'une source externe, comme [www.openwhitelist.com](http://www.openwhitelist.com) par exemple. Elle peut être utile si vous désirez limiter les accès internet à une liste blanche prédéfinie de sites autorisés.

### **3.3.5 Paramètres d'heure**

Cette fonction vous permet de synchroniser les fuseaux horaires Windows et Integard et donne la possibilité à Integard de passer outre l'horloge interne Windows et d'utiliser les serveurs Integard, en cochant la case « Heure internet ». Cette fonctionnalité permet d'éviter que l'heure Windows soit modifiée pour contourner les quotas de temps définis dans Integard. Elle permet également d'afficher les temps système et internet pour repérer les éventuelles différences entre les deux.

## 3.4 Restrictions d'applications

### 3.4.1 Règles d'applications

Sur cette page « Restrictions d'applications », vous pouvez autoriser ou interdire les accès internet pour certaines applications. Vous pouvez également empêcher l'exécution pure et simple d'une application.

Droits d'exécution.

Restriction	Description
<b>Restrictions normales</b>	En termes de filtrage, les restrictions normales sont identiques à celles qui seraient appliquées si elles n'apparaissaient pas du tout dans la liste. Elles permettent en revanche d'intégrer une application dans la liste, puis de la modifier ultérieurement sans avoir à l'ajouter à nouveau
<b>Aucun accès réseau</b>	Tous les accès internet pour l'application spécifiée sont bloqués.
<b>Exécution interdite</b>	Le programme spécifié n'est pas autorisé à être exécuté et sera immédiatement arrêté après son lancement.
<b>Aucune restriction</b>	Le programme spécifié peut se connecter au réseau sans aucun filtrage ou contrôle. À ce niveau de privilège, les applications ne sont pas concernées par les limites de données définies pour un utilisateur.
<b>Suppression de la liste</b>	Choisissez cette option et appliquez les modifications pour supprimer l'application de la liste.

Pour spécifier une application, vous pouvez utiliser le bouton « Parcourir » et parcourir l'arborescence pour choisir le programme exécutable ( fichiers avec extension .exe par exemple) ou simplement entrer le nom de l'exécutable, comme Notepad.exe. Il n'est pas nécessaire d'entrer le chemin complet.

La plupart des applications n'ont pas besoin d'apparaître dans cette liste. Celles qu'il est conseillé de spécifier sont les clients FTP ainsi que les serveurs et les téléphones VOIP, en raison de leurs exigences particulières de paramétrage réseau.

Remarque : L'activité réseau pour les applications définies ici sur « Aucune restriction » ne sera pas prise en compte dans le calcul des limites de données, et ne sera nullement surveillée ou filtrée.

### 3.4.2 Ports

La liste des ports peut être consultée au bas de la page de « Restrictions d'applications ».

Copyright © 2008 Race River Corporation Pty Ltd. Tous droits réservés.

Dans cette section, vous pouvez répertorier les ports TCP et UDP qu'Integard ne devrait pas bloquer.

Par exemple, si vous possédez un outil d'administration à distance qui requiert le fonctionnement du port TCP 4899, vous pouvez l'entrer ici, dans le champ « TCP ».

Remarque : L'activité réseau pour les ports répertoriés ici peut ne pas être prise en compte dans le calcul des limites de données.

### **3.4.3 Programmes récemment bloqués**

Ce tableau affiche une liste des programmes récemment bloqués et les ports sur lesquels ils ont été bloqués. Le tableau vous permet également d'autoriser les accès réseau pour le programme ou le port. Il vous suffit pour cela de cliquer sur le texte bleu correspondant dans le tableau. Ceci l'ajoutera automatiquement à la liste du dessus.

Il est déconseillé d'ajouter un navigateur internet dans cette liste, car cela aurait pour effet d'empêcher tout filtrage de contenu par Integard pour ce navigateur.

### 3.5 Mots-clés

La page des mots-clés vous permet de définir les mots et les phrases qui ne doivent pas apparaître sur une page internet visitée pour que celle-ci puisse être affichée.

Cette fonctionnalité est utile si l'on veut empêcher l'utilisateur d'accéder aux pages traitant d'un certain sujet.

Les mots-clés et les phrases doivent être entrés sur des lignes séparées.

**Exemple :**

ordinateur chats et chiens
-------------------------------

Dans cet exemple, si le mot-clé « ordinateur » apparaît dans une page internet, la page sera bloquée.

Il en sera de même pour les pages contenant le texte « chats et chiens ». En revanche, la phrase « chiens et chats » ne sera pas bloquée. Seule la phrase exacte est prise en compte.

Les mots-clés et les phrases sont insensibles à la casse. Ce qui signifie que « Ordinateur » et « ORDINATEUR » seront bloqués indifféremment.

### 3.6 Informations personnelles

Permet de définir les mots et les phrases que vous voulez empêcher d'être envoyées vers l'extérieur via internet. Par exemple, vous pouvez choisir de bloquer votre adresse, vos numéros de téléphone, ou même vos numéros de carte de crédit.

Contrairement à la liste des mots-clés, qui sert à bloquer le contenu *en provenance* d'internet, cette liste bloque le contenu *à destination* d'internet.

Si le logiciel Integard détecte que ces mots sont envoyés vers l'extérieur, dans un formulaire en ligne ou lors d'une discussion internet par exemple, il procédera à leur blocage et enverra un e-mail d'alerte à l'adresse de messagerie définie dans les paramètres système.

Vous pouvez définir les mots ou les phrases sur des lignes séparées.

**Exemple :**

34872312 Place du Capitole
-------------------------------

Dans cet exemple, si le mot-clé « 34872312 » ou la phrase « Place du Capitole » apparaît dans un formulaire ou dans une conversation à destination d'internet, il/elle sera bloqué(e).

Les mots-clés et les phrases sont insensibles à la casse. Ce qui signifie que « Place du Capitole » et « PLACE DU CAPITOLE » seront bloqués indifféremment.

### **3.7 Sites autorisés**

Permet de répertorier les noms de domaine et les URL des sites internet autorisés, indifféremment de leur catégorie et des mots ou des phrases qu'ils peuvent contenir.

Chaque entrée doit être placée sur une ligne à part. Il n'est pas nécessaire d'entrer http:// devant chaque adresse.

Si vous entrez un nom de domaine, le contenu du site entier sera accessible.

Si vous entrez un chemin vers une page spécifique, seul le contenu de cette page sera accessible. Toute autre page pourra être affichée ou non, en fonction des autres types de filtrage définis par Integard (contenu ou catégorie par exemple).

#### **Exemple :**

www.toysrus.fr kids.aol.fr fr.wikipedia.org/wiki/Cat
--

Il n'est pas non plus nécessaire de faire apparaître le préfixe « www. » ; il est même conseillé d'éviter de l'ajouter, car certains sites internet utilisent un préfixe différent.

### **3.8 Sites bloqués**

Permet de répertorier les noms de domaine et les URL des sites internet que vous désirez bloquer.

Il s'agit généralement de sites internet qui ne peuvent être bloqués automatiquement par Integard.

Les entrées doivent apparaître sur des lignes séparées. Il n'est pas nécessaire d'entrer http:// devant chaque adresse.

#### **Exemple :**

www.mauvaissite1.com mauvaissite1.net www.siteok.com/PageInterdite.htm
--

Il n'est pas non plus nécessaire de faire apparaître le préfixe « www. » ; il est même conseillé d'éviter de l'ajouter, car certains sites internet utilisent un préfixe différent.

### 3.9 Génération de compte-rendu

Integard permet de générer deux types de compte-rendu. Les comptes-rendus résumés et les comptes-rendus détaillés.

#### 3.9.1 Compte-rendu résumé

Le compte-rendu résumé récapitule toute l'activité internet de ces 7, 14 ou 30 jours.

Il affiche toutes les activités de connexion internet, de discussion en ligne ou de messagerie électronique, le temps de connexion total, les mégaoctets échangés et les pages bloquées.

Exemple :

Date	Jour de la semaine	Internet	Chat	E-mail	Données	Minutes	Blocages
25-2-2007	Dim	169	22	17	1,96 Mo	10	3
24-2-2007	Sam	510	33	107	22,94 Mo	43	1
23-2-2007	Ven	137	12	55	1,02 Mo	19	0
22-2-2007	Jeu	1018	53	50	6,97 Mo	59	1
21-2-2007	Mer	121	3	57	0,77 Mo	11	1
20-2-2007	Mar	1047	43	21	10,03 Mo	52	3
19-2-2007	Lun	259	12	19	1,36 Mo	11	6

Le compte-rendu journalier peut être envoyé par e-mail automatiquement à l'adresse e-mail configurée dans les paramètres système.

#### 3.9.2 Compte-rendu détaillé

Le compte-rendu détaillé présente la liste complète des opérations effectuées par un utilisateur.

## **4 Informations complémentaires**

### **4.1 Mises à jour automatiques de données**

Si vous utilisez la version d'évaluation limitée à 14 jours ou un abonnement Integard valide, vous pouvez recevoir automatiquement les mises à jour de la base de données Integard.

Integard contrôle les mises à jour disponibles et les télécharge automatiquement au démarrage de l'ordinateur, ou quotidiennement si l'ordinateur reste allumé en permanence.

La fonction de mise à jour automatique peuvent être désactivée ; il suffit pour cela de se connecter en tant à l'interface d'administration d'Integard, de choisir « Paramètres système » à partir du menu, d'ouvrir la section des mises à jour automatiques et de décocher la case « Mises à jour automatiques ».

### **4.2 Utilisation d'Integard avec un pare-feu et un logiciel antivirus**

Integard est compatible avec la plupart des antivirus et des pare-feux classiques. Dans certains cas, le pare-feu peut nécessiter une configuration particulière pour permettre à Integard d'accéder à internet.

Lorsque le pare-feu demande si Integard est autorisé à accéder à internet, répondez « oui », sinon toutes les connexions internet risquent d'être bloquées.

Ceci s'explique par le fait qu'Integard s'interface entre votre navigateur internet, vos applications de messagerie et de chat et internet afin de pouvoir en surveiller le contenu. Ainsi, pour le pare-feu, Integard tente d'accéder à internet à la place de ces applications.

### **4.3 Notifications par e-mail**

Integard peut envoyer des notifications par e-mail dans les situations suivantes :

- Page internet est bloquée
- Informations personnelles dans un formulaire en ligne
- Informations personnelles dans une discussion en ligne
- Messages « chat » bloqué car contenant des termes interdits
- Message « chat » douteux susceptible de provenir d'un adulte en train d'essayer d'enjôler un enfant à mauvaises fins.

Pour activer les notifications par e-mail, vous devez procéder comme suit :

- Entrer l'adresse e-mail dans « Paramètres système »
- Paramétrer le serveur SMTP dans Paramètres système | Comptes-rendus automatiques

- Cocher les cases requises pour activer les notifications par e-mail

Ensuite, dans "Options Chat/IM", activez ou désactivez les notifications par e-mail pour chaque utilisateur comme voulu.

#### **4.4 Contournement d'Integard**

Integard étant conçu pour limiter les accès à internet, les utilisateurs concernés peuvent essayer de passer outre.

Integard intègre de nombreux dispositifs de protection contre les modifications abusives et les tentatives de désactivation ou de désinstallation par des utilisateurs autres que l'administrateur.

Certaines précautions peuvent être prises, en tant qu'administrateur, pour rendre très compliquées les tentatives de contournement d'Integard.

#### **4.5 Précautions générales**

Pour optimiser les performances d'Integard, il est important de limiter les possibilités de contournement du système et d'accès aux contenus restreints.

Nous vous conseillons de procéder comme suit :

Créer un utilisateur distinct sur le système d'exploitation pour les enfants qui ne disposent pas de privilèges administrateur. (pour Windows NT, 2000 , XP ou Vista)

Modifier les paramètres BIOS du système pour empêcher un démarrage au CD : sur un système d'exploitation différent, qui ne serait soumis à aucune restriction, ou pour contourner les comptes administrateur. Vous pouvez également ajouter un mot de passe au BIOS pour empêcher la modification de la séquence de démarrage.

Vous assurer que l'adresse e-mail configurée dans Integard n'est accessible ni aux enfants, ni aux autres utilisateurs non autorisés.

Choisir un mot de passe administrateur inconnu et difficile à deviner.

## 5 Dépannage

### 5.1 *Integard bloque trop.*

Si Integard bloque trop, vous pouvez réduire la sensibilité de filtrage, en réduisant le niveau de filtrage pour les utilisateurs. Pour cela, connectez-vous en tant qu'administrateur via un navigateur internet, choisissez « Paramètres utilisateur », cliquez sur nom d'utilisateur et réglez la sensibilité dans « Paramètres de filtrage ».

Si vous désirez autoriser l'accès à certaines pages ou à certains sites, entrez-les dans la liste des « Sites autorisés ».

### 5.2 *Integard ne bloque pas les pages qu'il devrait.*

Si Integard ne bloque pas les pages qu'il devrait, vous pouvez :

- Accroître la sensibilité de filtrage en augmentant le niveau de filtrage pour les utilisateurs.
- Ajouter vos propres mots-clés et phrases de blocage.
- Ajouter les pages et les sites internet à la liste des sites bloqués.

Toutes ces opérations peuvent être effectuées via l'interface d'administration d'Integard. Pour savoir comment vous connecter et utiliser cette interface, consultez la section « Administration » de ce manuel.

Il se peut également que la page qui s'affiche ait été mise en cache par Internet Explorer. Lorsqu'une page est mise en cache, votre navigateur y accède via une copie enregistrée sur le disque dur, et non via internet. Ainsi, Integard ne peut la bloquer. Pour vous assurer que ce n'est pas le cas, il est recommandé d'effacer votre répertoire de fichiers internet temporaires. Avec Internet Explorer v6.0, il vous suffit de choisir « Options internet » à partir du menu « Outils » de votre navigateur, puis de cliquer sur « Supprimer les fichiers » dans la section « Fichiers Internet temporaires », onglet « Général ».

### **5.3 Logiciel antivirus et pare-feux personnels**

Integard a été testé avec différents antivirus et pare-feux. Comme le but d'Integard et de ces applications est d'accéder à certains paramètres réseau du système d'exploitation, ils ont tendance à interférer dans le bon fonctionnement de l'un ou de l'autre.

#### **Antivirus**

L'effet secondaire le plus courant lorsqu'on utilise Integard en parallèle d'un antivirus est que l'antivirus essaie de scanner les e-mails de la même manière qu'Integard, mais pour des raisons différentes. Comme les deux applications essaient de faire la même chose, il y a de grandes chances pour qu'elles interfèrent. Si Integard détecte un problème, il peut cesser d'analyser et de consigner les e-mails pour empêcher de bloquer totalement la boîte de messagerie au niveau des envois ou de la réception d'e-mails. Si l'envoi ou la réception d'e-mails ne fonctionne plus suite à l'installation d'Integard, vous pouvez essayer de désactiver l'analyse d'e-mails à partir de votre anti-virus, ou d'ouvrir les ports TCP 25 et 110 à partir de la page de configuration Integard de « Restrictions d'applications ».

#### **Pare-feux**

L'effet secondaire le plus courant lorsqu'on utilise Integard en parallèle d'un pare-feu est que le pare-feu doit être mis au courant qu'Integard est « autorisé » à accéder à internet. Cette information est essentielle car Integard accède à internet au nom de vos applications de navigation internet, de messagerie et de chat, et qu'il doit donc être autorisé à le faire. Cette autorisation peut se faire automatiquement ou nécessiter votre intervention suivant le pare-feu que vous utilisez.

## 6 Désinstallation d'Integard

Pour désinstaller Integard sous Windows 2000, Windows XP ou Windows Vista, vous devez posséder des droits Windows « administrateur ».

Vous devez également connaître le mot de passe administrateur Integard. Si vous ne le connaissez pas, il vous sera impossible de désinstaller Integard de l'ordinateur.

Vous pouvez lancer le programme de désinstallation d'Integard des deux manières suivantes :

- Menu Démarrer -> Programmes -> Integard – Désinstaller.
- ou
- Panneau de configuration -> Ajouter ou supprimer des programmes

Lorsque vous y êtes invité, entrez le mot de passe administrateur Integard pour permettre sa désinstallation.





