Aide de Websense Manager

Websense® Web Security
Websense Web Filter

v7

©1996–2008, Websense Inc.
Tous droits réservés.
10240 Sorrento Valley Rd., San Diego, CA 92121, États-Unis

Publié le 2008
Imprimé aux États-Unis et en Irlande

Les produits et/ou méthodes d'utilisation décrits dans ce document sont couverts par les numéros de brevet 5 983 270, 6 606 659, 6 947 985, 7 185 015, 7 194 464 et RE40 187 aux États-Unis, et par d'autres brevets en cours d'homologation.

Toute copie, photocopie, reproduction, traduction ou réduction en un format lisible sur une machine ou sur un support électronique quelconque, de tout ou partie de ce document sans le consentement préalable de Websense Inc. est interdite.

Websense Inc. s'est efforcé d'assurer l'exactitude des informations présentées dans ce guide. Toutefois, Websense Inc. ne garantit en aucune façon cette documentation et exclut toute garantie implicite de qualité marchande et d'adéquation à un usage particulier. Websense Inc. ne peut en aucun cas être tenu responsable des erreurs ou des dommages accessoires ou indirects liés à la fourniture, aux performances ou à l'utilisation de ce guide ou des exemples qu'il contient. Les informations contenues dans ce document pourront faire l'objet de modifications sans préavis.

Marques déposées

Websense est une marque déposée de Websense, Inc. aux États-Unis et dans d'autres pays. Websense possède de nombreuses autres marques non enregistrées aux États-Unis et dans d'autres pays. Toutes les autres marques sont la propriété de leurs propriétaires respectifs.

Microsoft, Windows, Windows NT, Windows Server et Active Directory sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Sun, Sun Java System et tous les logos et marques Sun Java System sont des marques ou des marques déposées de Sun Microsystems, Inc., aux États-Unis et/ou dans d'autres pays.

Mozilla et Firefox sont des marques déposées de Mozilla Foundation aux États-Unis et dans d'autres pays.

eDirectory and Novell Directory Services sont des marques déposées de Novell, Inc., aux États-Unis et dans d'autres pays.

Adobe, Acrobat et Acrobat Reader sont des marques ou des marques déposées d'Adobe Systems Incorporated aux États-Unis et/ou dans d'autres pays.

Pentium est une marque déposée d'Intel Corporation.

Red Hat est une marque déposée de Red Hat, Inc., aux États-Unis et dans d'autres pays. Linux est une marque de Linus Torvalds, aux États-Unis et dans d'autres pays.

Ce produit comprend un logiciel édité par Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000. The Apache Software Foundation. Tous droits réservés.

Les autres noms de produits mentionnés dans ce guide peuvent être des marques ou des marques déposées de leurs sociétés respectives et sont la propriété exclusive de leurs fabricants respectifs.

Contenu

1 Mise en route

Websense offre aux administrateurs réseau de tous les secteurs, du commerce à l'administration en passant par l'enseignement, la possibilité de contrôler ou de surveiller leur trafic réseau sur Internet.

- Réduisez le temps passé par vos employés à naviguer sur des sites Internet considérés comme répréhensibles, inappropriés ou non reliés au travail.
- Réduisez l'abus de vos ressources réseau et tout risque d'action juridique encouru pour accès inapproprié.
- Ajoutez une solide couche de sécurité à votre réseau, protégez-le contre les logiciels espion, les codes malveillants, le piratage et autres intrusions.

Cette page vous permet d'accéder aux informations suivantes :

Configuration de base de Websense	Implémentation du filtrage Internet
• *Utilisation de Websense Manager*, page 17	• *Filtrage des catégories et des protocoles*, page 38
• *Votre abonnement*, page 28	• *Ajout d'un client*, page 68
• *Base de données principale Websense*, page 32	• *Fonctionnement des stratégies*, page 75
• *Vérification de la configuration de Network Agent*, page 352	• *Attribution d'une stratégie aux clients*, page 79

Vous pouvez également apprendre à :

Évaluer votre configuration	Affiner les stratégies de filtrage
• *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22	• *Création d'une catégorie personnalisée*, page 178
• *Historique : 30 derniers jours*, page 25	• *Redéfinition du filtrage pour des sites spécifiques*, page 182
• *Rapports de présentation*, page 98	• *Restriction des utilisateurs à une liste définie de sites Internet*, page 168
• *Rapports d'investigation*, page 118	• *Filtrage par mots-clés*, page 180
• *Utilisation de la boîte à outils pour vérifier le comportement du filtrage*, page 197	• *Gestion du trafic en fonction du type de fichiers*, page 193
	• *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191

Présentation

Grâce à un travail combiné avec les périphériques d'intégration (y compris des serveurs proxy, des pare-feu, des routeurs et des dispositifs de mise en cache), Websense fournit le moteur et les outils de configuration qui permettent de développer, de surveiller et d'imposer des stratégies d'accès à Internet.

La suite de composants Websense (décrits à la section *Composants de Websense*, page 272) offre des capacités de filtrage Internet, d'identification des utilisateurs, de création d'alertes, de génération de rapports et de dépannage.

Une présentation des nouvelles fonctionnalités incluses dans cette version de Websense est disponible dans les Notes de publication, accessibles depuis le portail du support technique de Websense.

Après son installation, Websense applique la stratégie **Par défaut** pour surveiller l'utilisation d'Internet sans bloquer les requêtes. Cette stratégie gère l'accès Internet de tous les clients du réseau jusqu'à ce que vous définissiez vos propres stratégies et les attribuiez aux clients. Après la création de vos propres paramètres de filtrage personnalisés, la stratégie Par défaut continue à s'appliquer chaque fois qu'un client n'est pas géré par une autre stratégie. Pour plus d'informations, consultez *La stratégie Par défaut*, page 74.

Les processus de création des filtres, d'ajout de clients, de définition et d'application des stratégies à des clients sont décrits dans les sections suivantes :

- *Filtres d'utilisation Internet*, page 37
- *Clients*, page 59
- *Stratégies de filtrage Internet*, page 73

Un même outil de type navigateur (Websense Manager) fournit une interface graphique centrale aux fonctions générales de configuration, de gestion des stratégies et de génération de rapports de votre logiciel Websense. Pour plus d'informations, consultez *Utilisation de Websense Manager*, page 17.

Vous pouvez définir les niveaux d'accès à Websense Manager pour autoriser certains administrateurs à gérer uniquement un groupe spécifique de clients, ou permettre à des individus de générer des rapports sur leur propre utilisation d'Internet. Pour plus d'informations, consultez *Administration déléguée*, page 237.

Utilisation de Websense Manager

Rubriques connexes :

- *Connexion à Websense Manager*, page 18
- *Navigation dans Websense Manager*, page 20
- *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22
- *Historique : 30 derniers jours*, page 25

Websense Manager est l'interface de configuration centrale qui permet de personnaliser le comportement du filtrage, de surveiller l'utilisation d'Internet, de générer des rapports sur l'utilisation d'Internet et de gérer la configuration et les paramètres de Websense. Cet outil de type Web s'exécute sur 2 navigateurs pris en charge :

- Microsoft Internet Explorer 7
- Mozilla Firefox 2

Bien qu'il soit possible de lancer Websense Manager avec d'autres navigateurs, préférez ceux qui sont pris en charge afin de profiter de l'ensemble des fonctionnalités et de l'affichage approprié de l'application.

Pour lancer Websense Manager, procédez de l'une des manières suivantes :

- Sur les ordinateurs Windows :
  - Sélectionnez **Démarrer > Tous les programmes > Websense**, puis **Websense Manager**.
  - Double-cliquez sur l'icône Websense Manager placée sur votre Bureau.
- Ouvrez un navigateur pris en charge sur un ordinateur de votre réseau et entrez :

  ```
  https://<adresse IP>:9443/mng
  ```

  Remplacez *<adresse IP>* par l'adresse IP de votre ordinateur Websense Manager.

Si vous ne parvenez pas à vous connecter à Websense Manager sur le port par défaut, consultez le fichier **tomcat.log** sur l'ordinateur Websense Manager (situé par défaut dans le répertoire **C:\Program Files\Websense\tomcat\logs** ou **/opt/Websense/tomcat/logs/**) pour vérifier le port.

Si vous utilisez le port approprié et que vous ne parvenez toujours pas à vous connecter à Websense Manager depuis un ordinateur distant, assurez-vous que votre pare-feu autorise les communications sur ce port.

Une connexion SSL est utilisée pour la communication sécurisée de type navigateur avec Websense Manager. Cette connexion utilise un certificat de sécurité publié par Websense, Inc. Les navigateurs pris en charge ne reconnaissant pas Websense, Inc. comme une autorité de certification connue, une erreur de certificat s'affiche au premier démarrage de Websense Manager à partir d'un nouveau navigateur. Pour éviter cette erreur, vous pouvez installer ou accepter définitivement le certificat dans le navigateur. Vous trouverez les instructions nécessaires dans la Base de connaissances de Websense.

Dès que le certificat de sécurité a été accepté, la page de connexion de Websense Manager s'affiche dans la fenêtre du navigateur (voir *Connexion à Websense Manager*).

Connexion à Websense Manager

Rubriques connexes :

- *Utilisation de Websense Manager*
- *Navigation dans Websense Manager*, page 20
- *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22
- *Historique : 30 derniers jours*, page 25

Après l'installation, le premier utilisateur qui se connecte à Websense Manager dispose de droits d'accès administratifs complets. Le nom d'utilisateur est **WebsenseAdministrator** et n'est pas modifiable. Le mot de passe du compte WebsenseAdministrator est configuré pendant l'installation.

Pour vous connecter, démarrez Websense Manager (voir *Utilisation de Websense Manager*). Sur la page de connexion :

1. Sélectionnez un serveur **Policy Server** à gérer.

   Si votre environnement ne comprend qu'un seul serveur Policy Server, ce dernier est sélectionné par défaut.
2. Sélectionnez un **Type de compte** :
   - Pour vous connecter avec un compte utilisateur Websense, tel que WebsenseAdministrator, cliquez sur **Compte Websense** (par défaut).
   - Pour vous connecter avec vos identifiants de connexion réseau, cliquez sur **Compte réseau**.
3. Entrez un **Nom d'utilisateur** et un **Mot de passe**, puis cliquez sur **Se connecter**.

Vous êtes connecté(e) à Websense Manager.

- S'il s'agit de votre première connexion à Websense Manager, vous avez la possibilité de visionner un didacticiel Démarrage rapide. Si vous découvrez Websense, ou cette version de Websense, ce didacticiel est vivement conseillé.
- Si vous utilisez l'Administration déléguée et que vous avez créé des rôles administratifs, vous pouvez être invité(e) à sélectionner un rôle à gérer. Pour plus d'informations, consultez *Administration déléguée*, page 237.

Une session Websense Manager prend fin après 30 minutes d'inactivité dans l'interface utilisateur (clic d'une page vers une autre, saisie d'informations, mise en cache de modifications ou enregistrement de modifications). Un message d'avertissement s'affiche 5 minutes avant la fin de la session.

- Si la page comprend des modifications non mises en cache ou des modifications en cours de mise en cache, ces modifications sont perdues lorsque la session se termine. N'oubliez pas de cliquer sur **OK** pour mettre en cache et sur **Enregistrer tout** pour enregistrer et implémenter les modifications éventuelles.

- Si Websense Manager est ouvert dans plusieurs onglets de la même fenêtre de navigateur, toutes les instances partagent la même session. Si la session arrive à expiration dans un onglet, il en est de même pour tous les autres onglets.
- Si Websense Manager est ouvert dans plusieurs fenêtres de navigateur sur le même ordinateur, les instances partagent la même session **si** :
  - Vous utilisez Microsoft Internet Explorer et le raccourci clavier Ctrl-N pour ouvrir une nouvelle instance de Websense Manager.
  - Vous utilisez Mozilla Firefox.

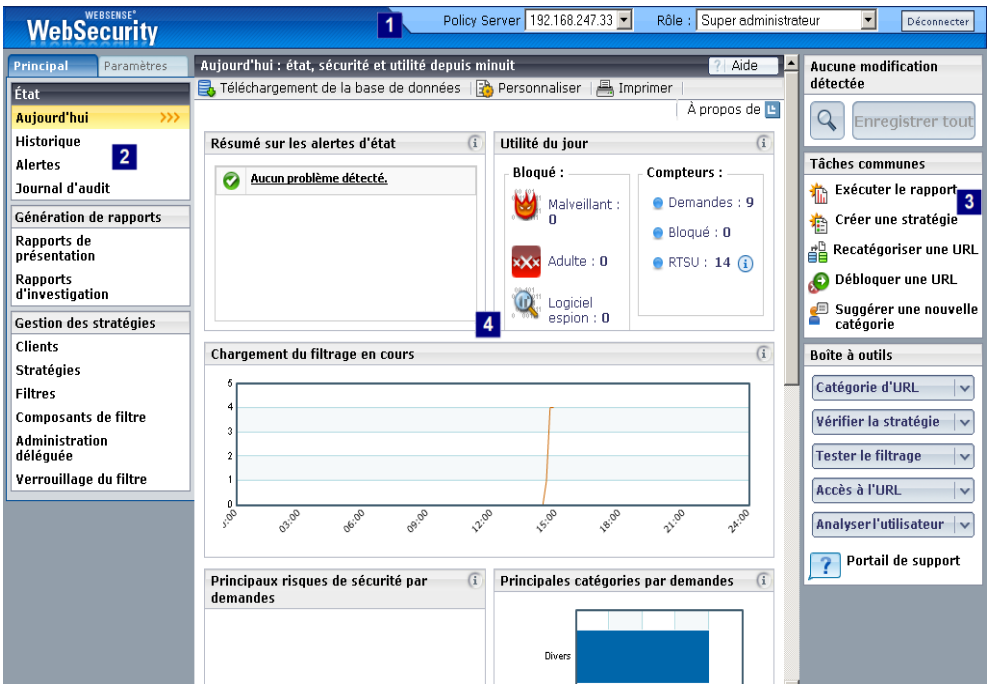
  Si la session arrive à expiration dans une fenêtre, il en est de même pour toutes les autres fenêtres.
- Si vous ouvrez plusieurs fenêtres Internet Explorer indépendamment les unes des autres et que vous les utilisez pour vous connecter en tant qu'administrateurs Websense Manager différents, les fenêtres ne partagent **pas** la même session. Lorsqu'une fenêtre arrive à expiration, les autres ne sont pas affectées.

Si vous fermez le navigateur sans vous déconnecter de Websense Manager, ou si l'ordinateur distant à partir duquel vous accédez à Websense Manager s'éteint de manière inattendue, il est possible que votre compte soit temporairement verrouillé. Websense détecte alors ce problème en 2 minutes environ et met fin à la session interrompue, ce qui vous permet de vous reconnecter.

Navigation dans Websense Manager

L'interface Websense Manager peut être divisée en 4 zones principales :

1. Bannière Websense
2. Panneau de navigation gauche
3. Panneau de raccourcis droit
4. Panneau de contenu



La **Bannière Websense** indique :

- Le serveur **Policy Server** sur lequel vous êtes connecté(e) (voir *Fonctionnement de Policy Server*, page 277)
- Votre **Rôle** administratif actuel (voir *Présentation des rôles d'administration*, page 238)
- Un bouton **Déconnecter**, que vous pouvez utiliser pour mettre fin à votre session administrative

Le contenu affiché dans Websense Manager dépend des droits accordés à l'utilisateur connecté. Par exemple, un utilisateur qui ne dispose que des droits de génération de rapports ne voit pas les paramètres de configuration des serveurs ni les outils d'administration des stratégies. Pour plus d'informations, consultez *Administration déléguée*, page 237.

Cette section décrit les options disponibles avec le compte WebsenseAdministrator et les autres utilisateurs disposant de droits Super administrateur.

Le **panneau de navigation gauche** comprend deux onglets : **Principal** et **Paramètres**. L'onglet **Principal** permet d'accéder aux fonctions d'état, de génération de rapports et de

gestion des stratégies. L'onglet **Paramètres** vous permet de gérer votre compte Websense et d'exécuter des tâches d'administration globales dans le système.

Le **panneau de raccourcis droit** contient des liens permettant d'accéder aux outils et aux tâches administratives courantes. Il vous permet également de revoir et d'enregistrer les modifications éventuellement apportées dans Websense Manager.

- La partie supérieure du panneau de navigation indique si des modifications mises en cache sont en attente d'enregistrement. Lorsque vous travaillez dans Websense Manager, la barre Modifications signale la présence éventuelle de **Modifications en attente**.

  Dans la plupart des cas, lorsque vous exécutez une tâche dans Websense Manager et que vous cliquez sur **OK**, vos modifications sont mises en cache. (Il vous faut parfois cliquer sur OK sur une page secondaire et sur une page principale pour mettre les modifications en cache.)

  Lorsque les modifications ont été mises en cache, cliquez sur **Enregistrer tout** pour enregistrer et implémenter les modifications. Pour afficher les modifications mises en cache avant leur enregistrement (voir *Revue, enregistrement et annulation des modifications*, page 21), cliquez sur le bouton **Afficher les modifications en attente**. Il s'agit du plus petit bouton placé à gauche de Enregistrer tout.
- La section **Tâches communes** fournit des raccourcis vers les tâches administratives les plus utilisées. Cliquez sur un élément de la liste pour ouvrir directement la page dans laquelle s'exécute la tâche.
- La section **Boîte à outils** contient des outils de recherche rapide qui vous permettent de vérifier votre configuration du filtrage. Pour plus d'informations, consultez *Utilisation de la boîte à outils pour vérifier le comportement du filtrage*, page 197.

Revue, enregistrement et annulation des modifications

Lorsque vous exécutez une tâche dans Websense Manager et que vous cliquez sur **OK**, vos modifications sont mises en cache. Pour revoir les modifications mises en cache, utilisez la page **Afficher les modifications en attente**.

Important

Évitez de double-cliquer ou de triple-cliquer sur le bouton OK. Plusieurs clics rapides sur le même bouton peuvent provoquer des problèmes d'affichage dans Mozilla Firefox, problèmes qui ne peuvent être résolus qu'en fermant et en rouvrant le navigateur.

Les modifications apportées à une seule zone de fonctionnalités sont généralement regroupées sous une seule entrée dans la liste du cache. Par exemple, si vous ajoutez 6 clients et que vous en supprimez 2, la liste du cache indique uniquement que des modifications ont été apportées aux Clients. À l'inverse, les modifications apportées à une seule page Paramètres peuvent se traduire par plusieurs entrées dans la liste du

cache. Cela se produit lorsqu'une seule page Paramètres est utilisée pour configurer plusieurs fonctions de Websense.

- Pour enregistrer toutes les modifications mises en cache, cliquez sur **Enregistrer toutes les modifications**.
- Pour abandonner toutes les modifications mises en cache, cliquez sur **Annuler toutes les modifications**.

Après avoir choisi Enregistrer tout ou Annuler tout, la barre Modifications située dans le panneau de raccourcis droit est actualisée en conséquence, et vous revenez à la dernière page sélectionnée. Les fonctions Enregistrer tout ou Annuler tout ne peuvent pas être annulées.

Servez-vous du Journal d'audit pour revoir les détails des modifications apportées dans Websense Manager. Pour plus d'informations, consultez *Affichage et exportation du journal d'audit*, page 284.

Aujourd'hui : état, sécurité et utilité depuis minuit

Rubriques connexes :

- *Navigation dans Websense Manager*, page 20
- *Historique : 30 derniers jours*, page 25
- *Personnalisation de la page Aujourd'hui*, page 24
- *Alertes*, page 287

La page **État > Aujourd'hui : état, sécurité et utilité depuis minuit** s'affiche en premier lorsque vous vous connectez à Websense Manager. Elle présente l'état actuel de votre logiciel de filtrage et offre une représentation graphique de l'activité de filtrage Internet sur 24 heures, à partir de 00:01, sur la base de l'heure de l'ordinateur de la Base de données d'activité.

En haut de la page, 2 sections récapitulatives présentent rapidement l'état en cours :

- Le **Résumé sur les alertes d'état** présente l'état de votre logiciel Websense. Si une erreur ou un avertissement s'affiche dans le résumé, cliquez sur le message d'alerte pour ouvrir la page Alertes, qui vous présente des informations plus détaillées (voir *Vérification de l'état du système en cours*, page 294).

  Les informations du Résumé sur les alertes d'état sont mises à jour toutes les 30 secondes.
- Sous **Utilité du jour**, examinez les exemples de protection de votre réseau par le filtrage Websense pendant la journée, de même que le nombre total de requêtes Internet traitées et d'autres totaux d'activité importants.

Sous les informations de résumé, jusqu'à 4 graphiques fournissent des informations sur les activités de filtrage. Ces graphiques sont disponibles aux Super administrateurs

et aux administrateurs délégués autorisés à afficher des rapports dans la page Aujourd'hui. Voir *Modification des rôles*, page 257.

Les informations de ces graphiques sont mises à jour toutes les 2 minutes. Il vous faudra peut-être faire défiler la fenêtre pour voir tous les graphiques.

Nom du graphique	Description
Chargement du filtrage en cours	Examinez le nombre de trafics Internet filtrés traités dans la Base de données d'activité, présentés par intervalles de 10 minutes.
Principaux risques de sécurité par demandes	Identifiez les catégories de Risque pour la sécurité ayant reçu le plus de requêtes dans la journée, et regardez si les stratégies de filtrage protègent correctement votre réseau.
Principales catégories par demandes	Visualisez les catégories les plus consultées dans la journée. Découvrez des précisions sur les problèmes potentiels de sécurité, de bande passante ou de productivité.
Application des stratégies par classe de risque	Découvrez combien de requêtes ont été autorisées et bloquées dans la journée pour chaque classe de risques (voir *Classes de risque*, page 41). Déterminez si les stratégies actuelles sont efficaces ou si des modifications sont nécessaires.
Principaux protocoles par bande passante	Identifiez les protocoles ayant utilisé le plus de bande passante sur votre réseau dans la journée. Servez-vous de ces informations pour évaluer les besoins en bande passante et la nécessité éventuelle d'une modification de stratégie.
Ordinateurs demandant des sites avec des risques de sécurité	Découvrez quels ordinateurs ont accédé à des sites présentant un risque pour la sécurité dans la journée. Vous pouvez éventuellement vous assurer ensuite que ces ordinateurs ne sont pas infectés par des virus ou des logiciels espion.
Principaux utilisateurs bloqués	Identifiez les utilisateurs ayant demandé le plus de sites bloqués dans la journée, en obtenant un aperçu du respect des règles d'utilisation Internet de l'organisation.
Principaux sites non catégorisés	Découvrez quels sites, non catégorisés par la base de données principale Websense, ont été les plus consultés aujourd'hui. Ouvrez la page **Tâches communes > Recatégoriser l'URL** pour attribuer un site à une catégorie de filtrage.

Cliquez sur l'un des graphiques à barres pour ouvrir un rapport d'investigation plus détaillé.

Trois boutons apparaissent sur la page :

- **Téléchargement de la base de données**, réservé aux Super administrateurs, ouvre une page qui permet de consulter l'état des téléchargements de la base de

données principale ou de démarrer un téléchargement (voir *Vérification de l'état du téléchargement de la base de données principale*, page 283).

- **Personnaliser**, réservé aux Super administrateurs, ouvre une page qui permet de choisir les graphiques devant s'afficher sur la page (voir *Personnalisation de la page Aujourd'hui*, page 24).
- **Imprimer**, disponible pour tous les administrateurs, ouvre une fenêtre secondaire présentant une version imprimable des graphiques affichés sur la page Aujourd'hui. Servez-vous des options du navigateur pour imprimer la page, qui omet toutes les options de navigation affichées dans la fenêtre Websense Manager principale.

Au-dessous des graphiques de filtrage et d'activité Internet, le **Résumé du Filtering Service** présente l'état de chacun des services Filtering Service associés au serveur Policy Server actuel. Cliquez sur l'adresse IP du service Filtering Service pour obtenir plus d'informations sur l'instance de ce service.

Pour des raisons de sécurité, une session Websense Manager prend fin après 30 minutes d'inactivité. Vous pouvez cependant choisir de continuer à surveiller les données du filtrage et des alertes : cochez la case **Continuer la surveillance des états Aujourd'hui, Historique et Alertes sans délai d'attente** située au bas de la page Aujourd'hui. Les informations de ces trois pages continuent à s'actualiser normalement jusqu'à ce que vous fermiez le navigateur ou que vous naviguiez vers une autre page de Websense Manager.

Important

Si vous activez l'option de surveillance et que vous restez dans les pages Aujourd'hui, Historique et Alertes pendant plus de 30 minutes, toute tentative d'ouverture d'une autre page de Websense Manager vous renvoie à la page de connexion.

Lorsque vous activez cette option, assurez-vous d'enregistrer toutes les modifications mises en cache avant que la période de 30 minutes n'arrive à expiration.

Personnalisation de la page Aujourd'hui

Rubriques connexes :

- *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22
- *Personnalisation de la page Historique*, page 27

La page **Aujourd'hui > Personnaliser** permet de sélectionner jusqu'à 4 graphiques pour la page État > Aujourd'hui. Seuls les Super administrateurs qui disposent de droits sans condition (y compris WebsenseAdministrator) peuvent personnaliser la page Aujourd'hui.

Les graphiques que vous sélectionnez s'affichent dans la page Aujourd'hui pour tous les Super administrateurs et pour tous les administrateurs délégués autorisés à afficher les graphiques sur cette page. Voir *Modification des rôles*, page 257.

Certains graphiques présentent des informations potentiellement sensibles, telles que des noms d'utilisateur ou des adresses IP. Assurez-vous que les graphiques sélectionnés soient appropriés pour tous les administrateurs qui pourront les afficher.

Pour sélectionner des graphiques, cochez ou désactivez la case accolée au nom du graphique. Lorsque vos sélections sont terminées, cliquez sur **OK** pour revenir dans la page Aujourd'hui et voir les graphiques. Pour revenir à la page Aujourd'hui sans apporter de modifications, cliquez sur **Annuler**.

Pour une brève description des informations affichées dans chaque graphique, consultez *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22.

Historique : 30 derniers jours

Rubriques connexes :

- *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22
- *Navigation dans Websense Manager*, page 20
- *Personnalisation de la page Historique*, page 27

La page **État > Historique : 30 derniers jours** présente un aperçu du comportement du filtrage au cours des 30 derniers jours. Les graphiques de la page sont actualisés tous les jours à 00:01h pour intégrer les données du jour précédent, sur la base de l'heure définie dans l'ordinateur de la Base de données d'activité.

La période exacte couverte par les graphiques et les tableaux de résumé dépend du temps passé par Websense à assurer le filtrage. Au cours du premier mois d'installation de Websense, la page présente les données correspondant au nombre de jours écoulés depuis l'installation. Après quoi les rapports couvrent les 30 jours précédant la date du jour.

Les **Estimations de l'utilité**, situées en haut de la page, présentent une estimation des économies réalisées grâce à Websense en termes de temps et de bande passante, de même qu'un résumé des requêtes bloquées pour les catégories présentant de l'importance pour de nombreuses organisations.

Pour savoir comment l'estimation a été calculée, placez la souris sur l'élément **Temps** ou **Bande passante** (sous Économies) (voir *Économies de temps et de bande passante*, page 27). Vous pouvez cliquer sur **Personnaliser** pour modifier le mode de calcul des valeurs.

La zone **Demandes bloquées** montre avec plus de détails comment Websense a protégé votre réseau en affichant une liste de plusieurs catégories qui intéressent de

nombreuses organisations et en présentant le nombre total de demandes bloquées pour chacune au cours de la période définie.

Selon les droits de génération de rapports accordés au rôle, les administrateurs délégués peuvent ou non voir les graphiques décrits ci-dessous. Voir *Modification des rôles*, page 257.

La page comprend également jusqu'à 4 graphiques présentant les principales caractéristiques du filtrage. Il vous faudra peut-être faire défiler la fenêtre pour voir tous les graphiques. Les informations des graphiques sont actualisées une fois par jour. Cliquez sur un graphique pour ouvrir un rapport d'investigation plus détaillé.

Nom du graphique	Description
Activité Internet par demandes	Vérifiez le nombre de demandes Internet filtrées et traitées dans la Base de données d'activité chaque jour.
Principaux risques de sécurité par demandes	Identifiez les catégories de Risque pour la sécurité les plus consultées récemment, et regardez si les stratégies de filtrage protègent correctement votre réseau.
Principales catégories par demandes	Identifiez les catégories les plus accédées. Découvrez des précisions sur les problèmes potentiels de sécurité, de bande passante ou de productivité.
Principaux sites non catégorisés	Identifiez les sites non classés par la Base de données principale Websense que les utilisateurs consultent le plus souvent. Ouvrez la page **Tâches communes > Recatégoriser l'URL** pour attribuer un site à une catégorie de filtrage.
Principaux protocoles par bande passante	Identifiez les protocoles qui ont utilisé le plus de bande passante sur votre réseau récemment. Utilisez ces informations pour évaluer les besoins en bande passante et un besoin éventuel de changement de stratégie.
Application des stratégies par classe de risque	Découvrez combien de demandes ont été autorisées et bloquées récemment pour chaque classe de risques (voir *Classes de risque*, page 41). Déterminez si les stratégies actuelles sont efficaces ou si des modifications sont nécessaires.
Principaux utilisateurs bloqués	Identifiez les demandes Internet des utilisateurs les plus souvent bloquées. Obtenez un aperçu du respect des règles d'utilisation Internet de l'organisation.
Résumé de l'application des stratégies	Obtenez une présentation des demandes récemment autorisées, des demandes bloquées pour les sites appartenant à la classe de risque de sécurité, et des demandes bloquées pour d'autres sites. Étudiez quels aspects du filtrage nécessitent une évaluation plus détaillée.

Trois boutons apparaissent sur la page :

- **Personnaliser**, réservé aux Super administrateurs, ouvre une page qui permet de choisir les graphiques devant s'afficher sur la page et de modifier le mode de calcul des économies estimées (voir *Personnalisation de la page Historique*, page 27).

- **Imprimer**, disponible pour tous les administrateurs, ouvre une fenêtre secondaire présentant une version imprimable des graphiques affichés sur la page Historique. Servez-vous des options du navigateur pour imprimer la page, qui omet toutes les options de navigation affichées dans la fenêtre Websense Manager principale.

Économies de temps et de bande passante

Outre la sécurité renforcée due au filtrage, Websense permet également de réduire le temps et la bande passante gaspillés dans les activités Internet non productives.

La section Économies de la zone Estimations des valeurs présente une estimation de ces économies de temps et de bande passante. Ces valeurs sont calculées comme suit :

- Économies de temps : multiplication du **temps moyen par visite** par le nombre de **sites bloqués**. Au départ, Websense utilise une valeur par défaut tel que le nombre moyen de secondes qu'un utilisateur passe à consulter un site Web demandé. La valeur des sites bloqués représente le nombre total de demandes bloquées au cours de la période couverte dans la page Historique.
- Économies de bande passante : multiplication de la **bande passante moyenne par visite** par le nombre de **sites bloqués**. Au départ, Websense utilise une valeur par défaut tel que le nombre moyen d'octets consommés par le site Web moyen. La valeur des sites bloqués représente le nombre total de demandes bloquées au cours de la période couverte dans la page Historique.

Pour plus d'informations sur la modification des valeurs utilisées dans ces calculs afin de refléter l'utilisation dans votre organisation, consultez la section *Personnalisation de la page Historique*, page 27.

Personnalisation de la page Historique

Rubriques connexes :

- *Historique : 30 derniers jours*, page 25
- *Personnalisation de la page Aujourd'hui*, page 24

La page **Historique > Personnaliser** permet de déterminer les graphiques devant s'afficher sur la page État > Historique, et de définir le mode de calcul des économies de temps et de bande passante.

Cochez la case accolée à chaque nom de graphique, 4 au maximum, que vous souhaitez inclure dans la page Historique. Pour une brève description de chaque graphique, consultez *Historique : 30 derniers jours*, page 25. Seuls les Super administrateurs qui disposent de droits sans condition (y compris WebsenseAdministrator) peuvent personnaliser les graphiques de la page Historique.

Certains graphiques présentent des informations potentiellement sensibles, telles que les noms d'utilisateur. Assurez-vous que les graphiques sélectionnés soient appropriés pour tous les administrateurs qui pourront les afficher.

Les Super administrateurs et les administrateurs délégués peuvent personnaliser le mode de calcul des économies de temps et de bande passante. Pour accéder à ces champs, les administrateurs délégués doivent cliquer sur le lien **Personnaliser** de la fenêtre contextuelle décrivant les calculs d'économie de temps et de bande passante.

Entrez les nouvelles mesures des moyennes de bande passante et de temps à utiliser comme base du calcul :

Option	Description
Valeur moyenne de secondes économisées par page bloquée	Entrez le nombre moyen de secondes qu'un utilisateur passe à consulter des pages individuelles selon les estimations de votre organisation. Websense multiplie cette valeur par le nombre de pages bloquées pour déterminer les économies de temps présentées dans la page Historique.
Bande passante moyenne [Ko] économisée par page bloquée	Entrez une taille moyenne, en kilo-octets (Ko), pour les pages consultées. Websense multiplie cette valeur par le nombre de pages bloquées pour déterminer les économies de bande passante présentées dans la page Historique.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Historique et voir les graphiques d'estimations de temps et de bande passante. Pour revenir à la page Historique sans apporter de modifications, cliquez sur **Annuler**.

Votre abonnement

Les abonnements à Websense sont générés par client. Un client est un utilisateur ou un ordinateur de votre réseau.

Lorsque vous achetez un abonnement, une clé d'abonnement vous est fournie par courrier électronique. Chaque clé sert pour l'installation d'un serveur Websense Policy Server. Si vous installez plusieurs serveurs Policy Server, vous devez disposer d'une clé distincte pour chacun d'eux.

Pour pouvoir commencer le filtrage, vous devez fournir une clé d'abonnement valide (voir *Configuration des informations de votre compte*, page 30). Cela vous autorise à télécharger la Base de données principale (voir *Base de données principale Websense*, page 32), qui permet au logiciel Websense de filtrer les clients.

Après le succès du premier téléchargement de la base de données, Websense Manager affiche le nombre de clients qui sont couverts par votre abonnement.

Websense assure la maintenance d'une table d'abonnement des clients filtrés chaque jour. La table d'abonnement est purgée chaque nuit. Dès qu'un client fait sa première requête Internet après la purge de la table, son adresse IP est entrée dans la table.

Lorsque le nombre de clients présents dans la table atteint le niveau d'abonnement, tous les client non listés précédemment qui demandent un accès Internet sortent du

cadre de l'abonnement. Dans ce cas, soit ils sont totalement privés d'accès Internet, soit ils reçoivent un accès non filtré, selon le paramètre choisi. De même, lorsqu'un abonnement arrive à expiration, tous les clients sont soit entièrement bloqués, soit non filtrés, selon ce paramètre.

Pour configurer le comportement du filtrage en cas d'abonnement périmé, consultez *Configuration des informations de votre compte*, page 30.

Pour configurer Websense de sorte qu'il envoie des alertes par courrier électronique lorsque votre abonnement touche à sa fin ou est périmé, consultez *Configuration des alertes système*, page 290.

Le nombre de catégories filtrées dépend de votre abonnement Websense. Ce dernier filtre tous les sites de toutes les catégories activées par votre achat.

Gestion de votre compte via le portail MyWebsense

Websense, Inc., gère un portail destiné aux clients à l'adresse www.mywebsense.com. Il vous permet d'accéder aux mises à jour, aux correctifs, aux informations sur le produit, aux évaluations et aux ressources du support technique pour votre logiciel Websense.

Lorsque vous créez un compte, vous êtes invité(e) à saisir toutes les clés d'abonnement Websense. Cela facilite votre accès aux informations, aux alertes et aux correctifs appropriés à votre produit et à votre version de Websense.

Lorsque vous disposez d'un compte MyWebsense, s'il vous arrive de ne pas pouvoir vous connecter à Websense Manager après avoir perdu votre mot de passe WebsenseAdministrator, cliquez simplement sur **Mot de passe oublié** dans la page de connexion de Websense Manager. Vous êtes alors invité(e) à vous connecter à MyWebsense et à suivre les instructions données pour générer et activer un nouveau mot de passe.

Important

Lorsque vous demandez un nouveau mot de passe, la clé d'abonnement que vous sélectionnez dans le portail MyWebsense doit correspondre à celle qui a été saisie dans la page Compte de Websense Manager.

Plusieurs membres de votre organisation peuvent créer des connexions MyWebsense associées à la même clé d'abonnement.

Pour accéder au portail MyWebsense depuis Websense Manager, ouvrez la page **Aide > MyWebsense**.

Activation de Websense Web Protection Services™

Les abonnements à Websense Web Security comprennent un accès aux services Websense Web Protection Services : SiteWatcher™, BrandWatcher™ et

ThreatWatcher™. Une fois activés, ces services protègent les sites, les marques et les serveurs Internet de votre organisation.

Service	Description
SiteWatcher	Vous avertit lorsque les sites Web de votre organisation ont été infectés par du code malveillant, ce qui vous permet de prendre des mesures immédiates pour protéger les clients, les prospects et les partenaires susceptibles de visiter le site.
BrandWatcher	• Vous avertit lorsque les sites Web où les marques de votre organisation ont été visées par des attaques d'hameçonnage (phishing) ou d'enregistreurs de frappe malveillants. • Fournit des informations relatives à la sécurité incluant entre autres les détails de l'attaque, de sorte que vous puissiez alors prendre des mesures, prévenir les clients et réduire l'impact sur les relations publiques de votre organisation.
ThreatWatcher	• Offre un aperçu de ce que voit le pirate sur le serveur Web de votre organisation, en recherchant les vulnérabilités connues et les menaces potentielles. • Indique les niveaux de risque et fournit des recommandations par l'intermédiaire d'un portail de type Web. • Permet de protéger vos serveurs Web des attaques malveillantes avant qu'elles ne se produisent.

Pour activer les services de protection Websense, connectez-vous au portail MyWebsense. Une fois que ThreatWatcher est activé, connectez-vous à MyWebsense pour accéder aux rapports sur les menaces pour les serveurs Web inscrits.

Configuration des informations de votre compte

Rubriques connexes :

- *Votre abonnement*, page 28
- *Configuration des téléchargements de la base de données*, page 33
- *Fonctionnement des protocoles*, page 184

La page **Paramètres > Compte** permet de saisir et de consulter les informations sur l'abonnement, et de modifier le mot de passe WebsenseAdministrator utilisé pour accéder à Websense Manager. WebsenseAdministrator est le compte d'administration principal utilisé par défaut pour gérer le logiciel Websense.

Cette page vous permet également d'autoriser le logiciel Websense à envoyer anonymement des données d'utilisation des protocoles à Websense, Inc. Ces informations peuvent être utilisées pour actualiser la Base de données principale Websense, une collection de plus de 36 millions de sites Internet et de plus de 100 définitions de protocoles (voir *Base de données principale Websense*, page 32).

1. Après l'installation de Websense, ou dès que vous recevez une nouvelle clé d'abonnement, utilisez le champ **Clé d'abonnement** pour entrer la clé.

   Lorsque vous entrez une nouvelle clé d'abonnement et que vous cliquez sur OK, le téléchargement de la base de données principale commence automatiquement.

2. Après le premier téléchargement de la base de données principale, les informations suivantes s'affichent :

Date d'expiration de la clé	Date d'expiration de votre abonnement actuel. Après cette date, vous devez renouveler l'abonnement pour continuer à télécharger la base de données principale et filtrer votre réseau.
Utilisateurs abonnés du réseau	Nombre d'utilisateurs du réseau pouvant être filtrés.
Utilisateurs abonnés distants	Nombre d'utilisateurs pouvant être filtrés à l'extérieur du réseau (requiert la fonction de filtrage à distance en option).

3. Sélectionnez **Bloquer les utilisateurs lorsque l'abonnement expire ou est dépassé** pour :
   - Bloquer tous les accès Internet de tous les utilisateurs lorsque l'abonnement arrive à expiration.
   - Bloquer tous les accès Internet des utilisateurs qui ont dépassé le nombre d'utilisateurs abonnés.

   Si cette option n'est pas activée, les utilisateurs ont dans ce cas accès à Internet sans être filtrés.

4. Pour modifier le mot de passe WebsenseAdministrator, entrez d'abord le mot de passe actuel, puis le nouveau mot de passe à deux reprises.
   - Le mot de passe doit comprendre 4 à 25 caractères. Il respecte la casse et peut être constitué de lettres, de chiffres, de caractères spéciaux et d'espaces.
   - Il est généralement préférable de créer un mot de passe renforcé pour le compte WebsenseAdministrator. Ce mot de passe doit être formé d'au moins 8 caractères et inclure au moins une majuscule, une minuscule, un chiffre et un caractère spécial.

5. Cochez la case **Envoyer les données de catégorie ou de protocole à Websense, Inc.** pour que Websense collecte les données d'utilisation sur les protocoles et les catégories Websense, et les envoie anonymement à Websense, Inc.

   Ces données d'utilisation aident Websense, Inc. à améliorer constamment les capacités de filtrage du logiciel Websense.

Base de données principale Websense

Rubriques connexes :

- *Mise à jour de la base de données en temps réel*, page 33
- *Real-Time Security Updates™*, page 33
- *Filtrage des catégories et des protocoles*, page 38
- *Fonctionnement de Filtering Service*, page 282
- *Vérification de l'état du téléchargement de la base de données principale*, page 283
- *Reprise des téléchargements de la base de données principale*, page 283

La base de données principale de Websense héberge les définitions de catégories et de protocoles qui constituent la base du filtrage du contenu Internet (voir *Filtrage des catégories et des protocoles*, page 38).

- Les **Catégories** servent à regrouper les sites Internet (identifiés par URL et par adresse IP) de contenu similaire.
- Les définitions de **Protocole** regroupent les protocoles de communication Internet utilisés pour des objectifs similaires, par exemple pour transférer des fichiers ou envoyer des messages instantanés.

Une version limitée de la base de filtrage est installée en même temps que Websense, mais il est conseillé de télécharger la Base de données principale complète dès que possible pour profiter de l'ensemble des capacités de filtrage Internet. Pour télécharger la Base de données principale pour la première fois, entrez votre clé d'abonnement à la page **Paramètres > Compte** (voir *Configuration des informations de votre compte*, page 30).

Si Websense doit passer par un proxy pour effectuer le téléchargement, utilisez également la page **Paramètres > Téléchargement de base de données** pour configurer les paramètres du serveur proxy (voir *Configuration des téléchargements de la base de données*, page 33).

Le téléchargement de la base de données complète peut prendre quelques minutes ou plus d'une heure, selon la vitesse de la connexion Internet, la bande passante, la mémoire et l'espace disque disponibles.

Après le téléchargement initial, Websense télécharge les modifications apportées à la base de données en fonction du planning défini (voir *Configuration des téléchargements de la base de données*, page 33). La Base de données principale étant fréquemment mise à jour, par défaut, les téléchargements sont planifiés chaque jour.

Si la Base de données principale date de plus de 14 jours, Websense ne filtre plus les demandes Internet.

Pour déclencher un téléchargement de la base de données à tout moment, ou pour consulter l'état et la date du dernier téléchargement ou le numéro de version de la base

de données actuelle, ouvrez la page **Etat > Aujourd'hui**, puis cliquez sur **Téléchargement de base de données**.

Mise à jour de la base de données en temps réel

Outre les téléchargements programmés, Websense effectue des mises à jour d'urgence de la base de données lorsque cela est nécessaire. Une mise à jour en temps réel peut être utilisée, par exemple, pour reclasser un site placé temporairement dans une catégorie incorrecte. Ces mises à jour permettent de s'assurer que les sites et les protocoles sont filtrés de façon appropriée.

Websense vérifie la présence de mises à jour de la base de données toutes les heures.

Les mises à jour les plus récentes sont énumérées à la page **Etat > Alertes** (voir *Vérification de l'état du système en cours*, page 294).

Real-Time Security Updates™

En plus de recevoir les habituelles mises à jour en temps réel de la base de données, les utilisateurs de Websense Web Security peuvent activer le service Real-Time Security Updates afin de recevoir des mises à jour liées à la sécurité de la Base de données principale dès leur publication par Websense, Inc.

Le service Real-Time Security Updates fournit une couche de protection supplémentaire contre les menaces pour la sécurité de type Internet. L'installation de ces mises à jour dès leur publication réduit la vulnérabilité relative aux attaques de type phishing (identification des fraudes), aux applications malveillantes et au code viral infectant les applications ou les sites Web.

Le service de filtrage vérifie la présence de mises à jour de sécurité toutes les 5 minutes. Cependant, les mises à jour n'étant envoyées qu'en cas de menace pour la sécurité, les modifications réelles sont occasionnelles et n'affectent pas l'activité normale du réseau.

Pour activer le service Real-Time Security Updates, ouvrez la page **Paramètres > Téléchargement de base de données** (voir *Configuration des téléchargements de la base de données*, page 33).

Configuration des téléchargements de la base de données

Rubriques connexes :

- *Configuration des informations de votre compte*, page 30
- *Base de données principale Websense*, page 32
- *Vérification de l'état du téléchargement de la base de données principale*, page 283

La page **Paramètres > Téléchargement de base de données** permet de définir le planning des téléchargements automatiques de la Base de données principale. Elle permet également de fournir des informations importantes sur un serveur proxy ou un pare-feu par lequel Websense doit passer pour télécharger la base de données.

1. Sélectionnez les **Jours de téléchargement** pour les téléchargements automatiques.

   Vous devez télécharger la base de données principale au moins une fois tous les 14 jours pour que Websense poursuive le filtrage sans interruption. Si vous désactivez tous les jours de téléchargement, Websense tente automatiquement de télécharger la base de données lorsque celle-ci a plus de 7 jours.

   > **Remarque**
   > Les jours de téléchargement sont désactivés lorsque le service Real-Time Security Updates est activé (voir Étape 3). Les téléchargements sont effectués automatiquement tous les jours afin de s'assurer que la base de données standard la plus récente est disponible pour les mises à jour de sécurité.

2. Sélectionnez les heures de début (**De**) et de fin (**À**) du **Délai de téléchargement**. Si aucune heure n'est sélectionnée, le téléchargement de la base de données intervient entre 21:00h et 06:00h.

   Websense sélectionne une heure aléatoire au cours de cette période pour contacter le serveur de la Base de données principale. Pour configurer des alertes en cas d'échec du téléchargement, consultez *Configuration des alertes système*, page 290.

   > **Remarque**
   > Après le téléchargement de la base de données principale, ou des mises à jour, l'utilisation du processeur peut atteindre 90 % pendant le chargement de la base de données dans la mémoire locale.

3. (*Websense Web Security*) Sélectionnez **Activer les mises à jour de sécurité en temps réel** pour que Websense vérifie la présence de mises à jour de sécurité de la Base de données principale toutes les 5 minutes. Lorsqu'une mise à jour de sécurité est détectée, elle est immédiatement téléchargée.

   Les mises à jour de sécurité en temps réel protègent rapidement votre réseau contre toute vulnérabilité relative aux attaques de type phishing (identification des fraudes), aux applications malveillantes et au code viral infectant les applications ou les sites Web.

4. Sélectionnez **Utiliser un serveur proxy ou un pare-feu** si Websense doit accéder à Internet par l'intermédiaire d'un serveur proxy ou d'un pare-feu (autre que le produit d'intégration avec lequel Websense communique) pour télécharger la Base de données principale. Configurez ensuite les éléments suivants :

Adresse IP ou nom du serveur	Entrez l'adresse IP ou le nom de l'ordinateur hébergeant le serveur proxy ou le pare-feu.
Port	Entrez le numéro de port par lequel le téléchargement de la base de données doit passer (8080 par défaut).

5. Si le serveur proxy ou le pare-feu configuré à l'étape 4 requiert une authentification pour accéder à Internet, sélectionnez **Utiliser l'authentification** et entrez le **Nom d'utilisateur** et le **Mot de passe** que Websense doit utiliser pour accéder à Internet.

Remarque

Si l'option Utiliser l'authentification est activée, le serveur proxy ou le pare-feu doit être configuré pour accepter une authentification de base ou en texte clair pour permettre les téléchargements de la base de données principale.

Par défaut, le nom d'utilisateur et le mot de passe sont codés au format du jeu de caractères défini dans les paramètres régionaux de l'ordinateur Policy Server. Cet encodage peut être configuré manuellement via la page **Paramètres > Services d'annuaire** (voir *Paramètres de l'annuaire avancés*, page 65).

Test de la configuration du réseau

Pour pouvoir filtrer les demandes Internet, Websense doit reconnaître le trafic Internet à destination et en provenance des ordinateurs de votre réseau. Pour vérifier que le logiciel de filtrage peut voir cette communication Internet, utilisez l'outil Détecteur de trafic réseau. Reportez-vous à la section *Vérification de la configuration de Network Agent*, page 352 pour obtenir des instructions.

Si le Détecteur de trafic ne peut pas voir tous les segments de votre réseau, reportez-vous à la section *Configuration du réseau*, page 343 pour des instructions sur la configuration.

Support technique de Websense

Websense, Inc., s'engage à donner satisfaction à ses clients. Vous pouvez accéder à tout moment au site du support technique Websense pour obtenir les dernières

informations sur les versions, pour accéder à la base de connaissances ou à la documentation sur les produits ou pour créer une demande d'assistance.

www.websense.com/SupportPortal/

Le temps de réponse aux requêtes en ligne pendant les heures de bureau est d'environ 4 heures. Les requêtes effectuées en dehors des heures de bureau sont traitées le jour ouvrable suivant.

Une assistance téléphonique est également disponible. Pour obtenir des réponses rapides et efficaces aux requêtes téléphoniques, veuillez préparer les éléments suivants :

- Clé d'abonnement Websense
- Accès à Websense Manager
- Accès aux ordinateurs exécutant Filtering Service et Log Server, et au serveur de base de données (Microsoft SQL Server ou MSDE)
- Autorisations d'accès à la base de données d'activité Websense
- Connaissance de l'architecture de votre réseau, ou accès à une personne disposant de ces connaissances
- Caractéristiques des ordinateurs exécutant Filtering Service et Websense Manager
- Liste des autres applications s'exécutant sur l'ordinateur Filtering Service

En cas de problème grave, d'autres informations peuvent se révéler nécessaires.

L'assistance téléphonique est disponible pendant les heures habituelles de bureau du lundi au vendredi aux numéros suivants :

- San Diego, Californie, États-Unis : **+1 858.458.2940**
- Londres, Angleterre : **+44 (0) 1932 796244**

Consultez le site Web de support technique indiqué ci-dessus pour plus d'informations sur les heures de fonctionnement et sur les autres options d'assistance.

Les clients japonais peuvent contacter leurs distributeurs pour obtenir un service plus rapide.

2 Filtres d'utilisation Internet

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 38
- *Fonctionnement des filtres*, page 48
- *Configuration des paramètres de filtrage de Websense*, page 56
- *Stratégies de filtrage Internet*, page 73
- *Affinage des stratégies de filtrage*, page 167

Les stratégies régissent l'accès à Internet des utilisateurs. Une stratégie est un programme qui indique à Websense comment et quand filtrer les sites et les applications Internet. À leur niveau le plus simple, les stratégies se composent de :

- **Filtres de catégories**, utilisés pour appliquer des actions (autoriser, bloquer) sur des catégories de sites Web
- **Filtres de protocoles**, utilisés pour appliquer des actions à des applications Internet et à des protocoles non HTTP
- Un planning qui détermine à quel moment chaque filtre est imposé

Le filtrage basé sur les stratégies vous permet d'attribuer divers niveaux d'accès Internet aux clients (utilisateurs, groupes et ordinateurs de votre réseau). Commencez par créer des filtres pour définir des restrictions d'accès Internet précises, puis servez-vous de ces filtres pour élaborer une stratégie.

Dans le cas d'une première installation, Websense crée une stratégie **Par défaut** et l'utilise pour commencer la surveillance des demandes Internet dès qu'une clé d'abonnement a été saisie (voir *La stratégie Par défaut*, page 74). Au départ, la stratégie par défaut autorise toutes les demandes.

Remarque

Lorsque vous effectuez une mise à niveau à partir d'une version antérieure du logiciel Websense, les paramètres de stratégie existants sont préservés. Après la mise à niveau, vérifiez que vos stratégies sont toujours appropriées.

Pour appliquer des restrictions de filtrage différentes selon les clients, commencez par définir des filtres de catégories. Vous pouvez définir :

- Un filtre de catégories bloquant l'accès à tous les sites Web à l'exception de ceux des catégories Commerce et économie, Enseignement et Actualités et médias
- Un second filtre de catégories autorisant tous les sites Web à l'exception de ceux qui constituent un risque pour la sécurité ou réservés aux adultes
- Un troisième filtre de catégories qui surveille l'accès aux sites Web sans les bloquer (voir *Création d'un filtre de catégories*, page 49)

Pour accompagner ces filtres de catégories, vous pouvez définir :

- Un filtre de protocoles qui bloque les groupes de protocoles Messagerie instantanée/Chat, Partage de fichiers en P2P, Antiblocage de proxy et Médias en temps réel.
- Un second filtre de protocoles qui autorise tous les protocoles non HTTP sauf ceux qui sont associés à l'antiblocage de proxy
- Un troisième filtre de protocoles qui autorise tous les protocoles non HTTP (voir *Création d'un filtre de protocoles*, page 51)

Dès que vous avez défini un jeu de filtres correspondant aux règles d'accès à Internet de votre organisation, vous pouvez les ajouter aux stratégies et les appliquer aux clients (voir *Stratégies de filtrage Internet*, page 73).

Filtrage des catégories et des protocoles

La Base de données principale de Websense classe les sites Web similaires (identifiés par les URL et les adresses IP) dans des **catégories**. Chaque catégorie à un nom descriptif, tel que Section pour adultes, Jeux de hasard ou Partage de fichiers P2P. Vous pouvez également créer vos propres catégories personnalisées afin de regrouper des sites qui intéressent particulièrement votre organisation (voir *Création d'une catégorie personnalisée*, page 178). Combinées, les catégories de la Base de données principale et les catégories définies par l'utilisateur constituent la base du filtrage Internet.

Websense, Inc., ne porte pas de jugement de valeur sur les catégories ou les sites de la base de données principale. Les catégories sont conçues pour créer des regroupements pratiques de sites pouvant constituer un problème pour les clients abonnés. Elles n'ont pas pour objectif de caractériser les sites, les groupes de sites, les personnes ou les intérêts à l'origine de leur publication, et ne doivent pas être interprétées comme tel. De même, les titres associés aux catégories Websense sont des raccourcis pratiques et ne constituent pas, ni ne doivent être considérés comme constituant, une opinion ou une position, d'approbation ou autre, quant aux sujets ou aux sites répertoriés.

La liste actualisée des catégories de la Base de données principale est disponible à l'adresse :

www.websense.com/global/fr/ProductsServices/MasterDatabase/URLCategories.php

Pour suggérer l'ajout d'un site dans la Base de données principale, cliquez sur **Suggérer une nouvelle catégorie** dans le panneau de raccourcis droits de Websense Manager, ou accédez au site :

www.websense.com/SupportPortal/SiteLookup.aspx

Une fois connecté(e) au portail MyWebsense, vous êtes dirigé(e) vers l'outil de recherche sur le site et de suggestion de catégorie (Site Lookup and Category Suggestion).

Lorsque vous créez un **filtre de catégories** dans Websense Manager, vous choisissez les catégories qui doivent être bloquées ou autorisées.

En plus d'héberger les catégories d'URL, la Base de données principale de Websense comprend des groupes de protocoles utilisés pour gérer le trafic Internet non HTTP. Chaque groupe de protocoles définit des types similaires de protocoles Internet (tels que FTP ou IRC) et d'applications (telles qu'AOL Instant Messenger ou BitTorrent). Les définitions sont vérifiées et mises à jour chaque nuit.

Comme pour les catégories, vous pouvez définir des protocoles personnalisés à utiliser pour le filtrage Internet.

La liste actualisée des protocoles de la base de données principale est disponible à l'adresse :

www.websense.com/global/fr/ProductsServices/MasterDatabase/ProtocolCategories.php

Lorsque vous créez un **filtre de protocoles**, vous choisissez les protocoles qui doivent être bloqués ou autorisés.

Remarque

L'agent Network Agent doit être installé pour que le filtrage à base de protocoles puisse s'effectuer.

Certains protocoles définis par Websense permettent de bloquer le trafic Internet sortant et destiné à un serveur externe, par exemple à un certain serveur de messagerie instantanée. Seuls les protocoles définis par Websense associés à des numéros de port attribués dynamiquement peuvent être bloqués en tant que trafic sortant.

Nouveaux protocoles et nouvelles catégories

Lorsque de nouveaux protocoles et de nouvelles catégories sont ajoutés à la base de données principale, une action de filtrage par défaut est affectée à chacun, par exemple **Autoriser** ou **Bloquer** (voir *Actions de filtrage*, page 44).

- L'action par défaut est appliquée dans tous les filtres de catégories et de protocoles actifs (voir *Fonctionnement des filtres*, page 48). Pour modifier la façon dont la catégorie ou le protocole est filtré(e), modifiez les filtres actifs.
- L'action par défaut repose sur le renvoi d'informations relatives au caractère professionnel approprié des sites ou des protocoles concernés.

Vous pouvez également configurer Websense de sorte qu'il génère une alerte système et vous avertisse à chaque ajout de nouvelles catégories ou de nouveaux protocoles dans la base de données principale. Pour plus d'informations, consultez *Alertes*, page 287.

Catégories spéciales

La base de données principale contient des catégories spéciales qui simplifient la gestion de types spécifiques d'utilisation Internet. Les catégories suivantes sont disponibles dans toutes les éditions du logiciel Websense :

- La catégorie **Événements spéciaux** est utilisée pour classer les sites considérés comme sujets sensibles, afin de vous aider à gérer les hausses de trafic Internet liées à certains événements. Par exemple, le site officiel de la Coupe du monde de football apparaît généralement dans la catégorie Sports mais peut être placé dans la catégorie Événements spéciaux pendant la compétition.

  Les mises à jour de la catégorie Événements spéciaux sont ajoutées dans la base de données principale pendant les téléchargements planifiés. Les sites sont ajoutés dans cette catégorie pour une courte période, après quoi ils sont soit déplacés vers une autre catégorie, soit supprimés de la base de données principale.
- La catégorie **Productivité** a pour objectif d'éviter les comportements générant des pertes de temps.
  - Publicités
  - Téléchargement de logiciels et de freewares
  - Messagerie instantanée
  - Courtage en ligne
  - Sites rémunérateurs
- La catégorie **Largeur de bande** a pour objectif d'économiser la bande passante du réseau.
  - Radio et TV sur Internet
  - Téléphonie Internet
  - Partage de fichiers en peer-to-peer (P2P)
  - Stockage/Sauvegarde de réseaux personnels
  - Médias en temps réel

Websense Web Security comprend d'autres catégories de sécurité :

- **Websense Security Filtering** (également appelé **Sécurité**) se concentre sur les sites Internet contenant du code malveillant, capable de contourner les logiciels antivirus. Les sites de cette catégorie sont bloqués par défaut.
  - Réseaux zombies
  - Enregistreurs de frappe
  - Sites Web dangereux
  - Phishing et autres escroqueries
  - Logiciels indésirables

  - Logiciels espion
- **Protection étendue** se concentre sur les sites Web potentiellement malveillants. Les sites des sous-catégories Exposition élevée et Exploits émergeants sont bloqués par défaut.
  - **Exposition élevée** contient des sites qui masquent leur vraie nature ou leur véritable identité, ou qui incluent des éléments suggérant un objectif malveillant latent.
  - **Nouvelles exploitations** contient des sites connus pour héberger du code d'exploit connu et potentiel.
  - **Contenu à risques** regroupe des sites susceptibles de renfermer du contenu inutile ou peu utile.

La catégorie Protection étendue filtre les sites Web potentiellement malveillants sur la base de leur *réputation*. La réputation des sites repose sur des signes précoces d'activités malveillantes potentielles. Un attaquant peut viser une URL contenant une faute d'orthographe, par exemple, ou ressemblant à une URL légitime. Un tel site peut être utilisé pour diffuser du code malveillant aux utilisateurs avant que leurs filtres traditionnels ne soient mis à jour.

Lorsque les chercheurs en sécurité de Websense détectent une menace potentielle, celle-ci est ajoutée dans la catégorie Protection étendue jusqu'à ce que Websense soit sûr à 100 % de la catégorisation finale du site.

Classes de risque

Rubriques connexes :

- *Attribution de catégories aux classes de risque*, page 306
- *Rapports de présentation*, page 98
- *Rapports d'investigation*, page 118

La base de données principale Websense regroupe les catégories dans des **classes de risque**. Les classes de risques suggèrent des types ou des niveaux possibles de vulnérabilité représentés par des sites du groupe de catégories.

Les classes de risques sont essentiellement utilisées dans la génération des rapports. Les pages Aujourd'hui et Historique comprennent des graphiques qui illustrent l'activité Internet par classe de risque et vous permettent de générer une présentation ou des rapports d'investigation triés par classe de risque.

Les classes de risques peuvent également se révéler très utiles pour créer des filtres de catégories. À l'origine, par exemple, le filtre de catégories Sécurité de base bloque toutes les catégories par défaut de la classe Risque pour la sécurité. Lorsque vous créez vos propres filtres de catégories, vous pouvez vous servir des regroupements de la classe de risque comme base pour déterminer si une catégorie doit être autorisée, bloquée ou limitée d'une manière ou d'une autre.

Websense comprend 5 classes de risque, énumérées ci-dessous. Par défaut, Websense regroupe les catégories suivantes dans chaque classe de risque.

- Une catégorie peut apparaître dans plusieurs classes de risques ou n'être attribuée à aucune.
- Les regroupements peuvent changer régulièrement dans la base de données principale.

Responsabilité légale

Section pour adultes (dont Contenu pour adultes, Lingerie et Maillots de bain, Nudité et Sexualité)

Largeur de bande > Partage de fichiers en peer-to-peer

Jeux de hasard

Illégal ou douteux

Technologies de l'information > Piratage et Antiblocage par proxy

Militantisme, extrémisme

Racisme, haine

Mauvais goût

Violence

Armes

Perte de bande passante réseau

Largeur de bande (y compris Radio et TV sur Internet, Téléphonie Internet, Partage de fichiers en peer-to-peer, Stockage/Sauvegarde de réseaux personnels et Médias en temps réel)

Divertissement > Services de téléchargement MP3 et audio

Productivité > Publicités et téléchargement de freewares *et* de logiciels

Utilisation professionnelle

Commerce et économie (y compris Services Financiers)

Enseignement > Matériaux Éducatifs *et* Outils de référence

Gouvernement (Armée)

Technologies de l'information (y compris Sécurité informatique, Moteurs de recherche et portails et Sites de traduction d'URL)

Voyage

Véhicules

Risques pour la sécurité

Largeur de bande > Partage de fichiers en peer-to-peer

Protection étendue (y compris Exposition élevée, Nouvelles exploitations et Contenu à risques) [*Websense Web Security*]

Technologies de l'information > Piratage *et* Antiblocage par proxy

Risques pour la sécurité

Productivité >Téléchargement de logiciels et de freewares

Sécurité (y compris Réseaux zombies, Enregistreurs de frappe, Sites Web dangereux, Phishing et autres escroqueries, Logiciels indésirables et Logiciels espion)

Perte de productivité

Avortement (y compris Pro-Avortement *et* Anti-Avortement)

Section pour adultes > Éducation sexuelle

Groupes activistes/Associations

Largeur de bande > Radio et TV sur Internet, Partage de fichiers en peer-to-peer et Médias en temps réel

Drogues (y compris Abus de drogues, Marijuana, Médicaments sur ordonnance et Compléments/Substances non réglementées)

Enseignement (y compris Institutions culturelles *et* Institutions scolaires)

Divertissement (y compris Services de téléchargement MP3 et audio)

Jeux de hasard

Jeux

Gouvernement > Groupes politiques

Santé

Technologies de l'information > Hébergement de sites Web

Communication Internet (y compris E-mail général et E-mail organisationnel, Messagerie texte et multimédia et Conversations en ligne)

Recherche d'emplois

Actualités et médias (y compris Journaux alternatifs)

Productivité (y compris Téléchargement de logiciels et de freewares, Messagerie instantanée, BBS et forums, Courtage en ligne et Sites rémunérateurs)

Religion (y compris Religions non traditionnelles, religions occultes, et folklore *et* Religions traditionnelles)

Shopping (y compris Ventes aux enchères sur Internet *et* Immobilier)

Associations et organismes sociaux (y compris Organisations professionnelles et de travailleurs, Organisations philanthropiques et Associations caritatives)

Société et style de vie (y compris Alcool et tabac, Homosexuels, lesbiennes et bisexuels, Hobbies, Petites annonces personnelles/Rendez-vous amoureux, Restaurants et Sites de Social Networking et sites personnels)

Événements spéciaux

Sports (y compris Chasse, clubs de tir)

Voyage

Véhicules

Les Super administrateurs peuvent modifier les catégories attribuées à chaque classe de risque à la page **Paramètres > Classe de risque** (voir *Attribution de catégories aux classes de risque*, page 306).

Groupes de protocoles de sécurité

Outre les catégories Sécurité et Protection étendue, Websense Web Security comprend deux protocoles prévus pour faciliter la détection et la protection contre les logiciels espion et le code malveillant ou le contenu transmis par Internet.

- Le groupe de protocoles **Trafic malveillant** comprend le protocole **Réseaux Bot**, conçu pour bloquer le trafic de contrôle et de commande généré par un « bot » tentant de se connecter par le biais d'un réseau « zombie » à des fins malveillantes.
- Le groupe de protocoles **Trafic malveillant - Surveiller uniquement** est utilisé pour identifier le trafic pouvant être associé aux logiciels malveillants.
  - **Vers de messagerie** surveille le trafic SMTP sortant susceptible d'être généré par une attaque de vers de messagerie.
  - **Autre trafic malveillant** surveille le trafic entrant ou sortant susceptible d'être lié à des applications malveillantes.

Le groupe de protocoles Trafic malveillant est bloqué par défaut et peut être configuré dans vos filtres de protocoles (voir *Modification d'un filtre de protocoles*, page 52). Les protocoles Trafic malveillant - Surveiller uniquement peuvent être enregistrés pour la génération de rapports, sans que des actions de filtrage ne soient appliquées.

Instant Messaging Attachment Manager

Instant Messaging (IM) Attachment Manager est une fonction en option. Si vous vous abonnez à cette fonction, vous pouvez limiter le partage de fichiers entre clients de messagerie instantanée dont AOL/ICQ, Microsoft (MSN), et Yahoo. Cela vous permet d'autoriser le trafic de messagerie instantanée tout en bloquant le transfert des pièces jointes par les clients de messagerie instantanée.

Instant Messaging File Attachments est un groupe de protocoles qui comprend des définitions pour plusieurs clients de messagerie instantanée. Lorsque IM Attachment Manager est activé, ces protocoles apparaissent dans la liste des protocoles de tous les filtres de protocoles actifs et sur la page Modifier les protocoles.

Le filtrage de pièces jointes IM peut être appliqué au trafic interne et externe. Pour activer le filtrage du trafic interne, définissez la portion de votre réseau à surveiller à la page **Paramètres > Network Agent > Global** (voir *Configuration des paramètres globaux*, page 346).

Actions de filtrage

Les filtres de catégories et de protocoles attribuent une **action** à chaque catégorie ou protocole. Il s'agit de l'action entreprise par le filtrage Websense en réponse à la demande Internet d'un client. Les actions qui s'appliquent aux catégories et aux protocoles sont :

- **Bloquer** la demande. Les utilisateurs reçoivent une page ou un message de blocage et ne peuvent pas afficher le site ou utiliser l'application Internet.

- **Autoriser** la demande. Les utilisateurs peuvent afficher le site ou utiliser l'application Internet.
- Evaluer l'utilisation actuelle de la **Bande passante** avant de bloquer ou d'autoriser la demande. Lorsque cette action est activée et que l'utilisation de la bande passante atteint un seuil défini, les prochaines demandes Internet pour une catégorie ou un protocole spécifique sont bloquées. Voir *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.

Les autres actions ne peuvent être appliquées qu'aux catégories.

> **Remarque**
>
> Il est préférable de ne pas utiliser les options Confirmer et Contingent lorsque des clients individuels (utilisateurs, groupes et ordinateurs) sont gérés par plusieurs serveurs Policy Server.
>
> Les informations de temps associées à ces fonctions ne sont pas partagées entre les serveurs Policy Server et les clients concernés pourraient se voir accorder plus ou moins d'accès Internet que prévu.

- **Confirmer**—Les utilisateurs reçoivent une page de blocage qui les invite à confirmer qu'ils accèdent au site pour des raisons professionnelles. Si un utilisateur clique sur **Continuer**, il peut consulter le site.

  Un clic sur le bouton Continuer démarre un minuteur. Pendant le délai configuré (60 secondes par défaut), l'utilisateur peut visiter d'autres sites des catégories Confirmer sans recevoir d'autres pages de blocage. Lorsque ce délai est écoulé, la navigation vers un autre site Confirmer entraîne l'apparition d'une autre page de blocage.

  Le délai par défaut peut être modifié à la page **Paramètres > Filtrage**.
- **Contingent**—Les utilisateurs reçoivent une page de blocage qui leur demande s'ils souhaitent utiliser du temps contingenté pour consulter le site. Si un utilisateur clique sur **Utiliser du temps contingenté**, il peut consulter le site.

  Un clic sur le bouton Utiliser du temps contingenté démarre deux minuteurs : un minuteur de session de temps contingenté et un minuteur d'affectation de temps contingenté total.

  - Si l'utilisateur demande d'autres sites de temps contingenté pendant une période de **session** par défaut (10 minutes par défaut), il peut consulter ces sites sans recevoir d'autres pages de blocage.
  - Le temps contingenté **total** est affecté quotidiennement. Une fois écoulé, chaque client doit attendre le jour suivant pour accéder au site des catégories de temps contingenté. Le temps contingenté quotidien par défaut (60 minutes par défaut) est défini à la page **Paramètres > Filtrage**. Les affectations de temps contingenté quotidien peuvent également être accordées aux clients sur une base individuelle. Pour plus d'informations, consultez *Utilisation de temps contingenté pour limiter l'accès Internet*, page 46.
- **Bloquer des mots-clés**—Lorsque vous définissez des mots-clés et activez leur blocage, les utilisateurs qui demandent un site dont l'URL contient un mot-clé bloqué ne peuvent pas accéder au site. Voir *Filtrage par mots-clés*, page 180.

- **Bloquer des types de fichier**—Lorsque le blocage de types de fichiers est activé, les utilisateurs qui tentent de télécharger un fichier dont le type est bloqué reçoivent une page de blocage et le fichier n'est pas téléchargé. Voir *Gestion du trafic en fonction du type de fichiers*, page 193.

Utilisation de temps contingenté pour limiter l'accès Internet

Lorsque l'utilisateur clique sur Utiliser du temps contingenté, il peut consulter les sites d'une catégorie de temps contingenté jusqu'à la fin de la session de temps contingenté. Le délai par défaut d'une session de temps contingenté (configuré dans la page **Paramètres > Filtrage** est de 10 minutes.

> **Remarque**
>
> Il est préférable de ne pas utiliser l'option Contingent lorsque des clients individuels sont gérés par plusieurs serveurs Policy Server.
>
> Les informations de temps associées à cette fonction ne sont pas partagées entre les serveurs Policy Server et les clients concernés pourraient se voir accorder plus ou moins d'accès Internet que prévu.

Lorsque la session de temps contingenté se termine, une demande de site de temps contingenté entraîne l'affichage d'un message de blocage. Les utilisateurs qui n'ont pas épuisé leur temps contingenté quotidien peuvent démarrer une nouvelle session de temps contingenté.

Une fois que le temps contingenté est configuré, Websense utilise une liste de priorité pour déterminer la réponse appropriée lorsqu'un utilisateur demande un site d'une catégorie de ce type. Le logiciel recherche le temps contingenté configuré pour :

1. L'utilisateur
2. L'ordinateur ou le client réseau
3. Les groupes auxquels l'utilisateur appartient

   Si l'utilisateur est membre de plusieurs groupes, Websense accorde le temps contingenté en fonction du paramètre **Utiliser un blocage plus restrictif** de la page **Paramètres > Filtrage** (voir *Configuration des paramètres de filtrage de Websense*, page 56).
4. Le temps contingenté par défaut

Les applets Internet, de type Java ou Flash, peuvent ne pas répondre comme prévu aux restrictions de temps contingenté. Même lorsque l'accès se fait à partir d'un site limité par le temps contingenté, une applet qui s'exécute dans le navigateur peut poursuivre son exécution au-delà du délai configuré.

Cela est dû au fait que les applets sont entièrement téléchargées sur un ordinateur client et s'exécutent comme les applications, sans nouvel échange avec le serveur hôte d'origine. Toutefois, si l'utilisateur clique sur le bouton Actualiser du navigateur,

Websense détecte la communication au serveur hôte et bloque la demande en fonction des restrictions de temps contingenté applicables.

Accès par mot de passe

L'accès par mot de passe permet aux utilisateurs qui disposent de mots de passe valides d'accéder aux sites bloqués par Websense. L'accès par mot de passe peut être accordé à des clients individuels (utilisateurs, groupes, ordinateurs ou réseaux).

Lorsque l'accès par mot de passe est activé, les messages de blocage de Websense comprennent un champ de mot de passe. Les clients qui saisissent un mot de passe valide peuvent accéder aux sites bloqués pour une période limitée.

> **Remarque**
>
> Il est préférable de ne pas utiliser l'option d'accès par mot de passe lorsque des clients individuels sont gérés par plusieurs serveurs Policy Server.
>
> Les informations de temps associées à cette fonction ne sont pas partagées entre les serveurs Policy Server et les clients concernés pourraient se voir accorder plus ou moins d'accès Internet que prévu.

L'option d'accès par mot de passe est activée dans la page **Paramètres > Filtrage** (voir *Configuration des paramètres de filtrage de Websense*, page 56).

Pour accorder des droits d'accès par mot de passe à des clients spécifiques, utilisez la page **Gestion des stratégies > Clients** (voir *Ajout d'un client*, page 68 ou *Modifications des paramètres des clients*, page 70).

Filtrage de la recherche

Le filtrage de la recherche est une fonction offerte par certains moteurs de recherche qui permet de limiter le nombre de résultats inappropriés affichés aux utilisateurs.

En général, les résultats des moteurs de recherche Internet peuvent comprendre des vignettes associées aux sites correspondants aux critères de recherche. Si ces vignettes sont associées à des sites bloqués, Websense empêche les utilisateurs d'accéder au site complet, mais n'empêche pas le moteur de recherche d'afficher l'image.

Lorsque vous activez le filtrage de la recherche, Websense active une fonction du moteur de recherche de sorte que les vignettes associées à des sites bloqués n'apparaissent pas dans les résultats de la recherche. L'activation du filtrage de la recherche affecte à la fois les clients de filtrage locaux et distants.

Websense, Inc., gère une base de données de moteurs de recherche prenant en charge les capacités de filtrage des recherches. Lorsqu'un moteur de recherche est ajouté ou supprimé dans la base de données, une alerte est générée (voir *Alertes*, page 287).

Le filtrage des recherches est activé dans la page **Paramètres > Filtrage**. Pour plus d'informations, consultez *Configuration des paramètres de filtrage de Websense*, page 56.

Fonctionnement des filtres

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 38
- *Stratégies de filtrage Internet*, page 73
- *Création d'un filtre de catégories*, page 49
- *Création d'un filtre de protocoles*, page 51
- *Création d'un filtre d'accès limité*, page 169

La page **Gestion des stratégies > Filtres** de Websense Manager permet d'afficher, de créer et de modifier les filtres de catégories et de protocoles et d'utiliser d'autres outils de filtrage.

La page Filtres comprend 3 sections principales :

- **Filtres de catégories** détermine les catégories à bloquer et à autoriser.
- **Filtres de protocoles** détermine les protocoles non HTTP à bloquer et à autoriser.

  L'agent Network Agent doit être installé pour que le filtrage à base de protocoles puisse s'effectuer.
- **Filtres d'accès limité** définit une liste restrictive de sites Web autorisés (voir *Restriction des utilisateurs à une liste définie de sites Internet*, page 168).

Les filtres de catégories, de protocoles et d'accès limité constituent la base des **stratégies**. Chaque stratégie se compose d'au moins un filtre de catégories ou d'accès illimité, et d'un filtre de protocoles, appliqués aux clients sélectionnés pendant un planning spécifique.

- Pour revoir ou modifier un filtre existant de catégories, de protocoles ou d'accès limité, cliquez sur son nom. Pour plus d'informations, voir :
  - *Modification d'un filtre de catégories*, page 50
  - *Modification d'un filtre de protocoles*, page 52
  - *Modification d'un filtre d'accès limité*, page 170
- Pour créer un nouveau filtre de catégories, de protocoles ou d'accès limité, cliquez sur **Ajouter**. Pour plus d'informations, voir :
  - *Création d'un filtre de catégories*, page 49
  - *Création d'un filtre de protocoles*, page 51
  - *Création d'un filtre d'accès limité*, page 169

Pour dupliquer un filtre existant, cochez la case accolée au nom du filtre, puis cliquez sur **Copier**. La copie porte le nom du filtre original plus un nombre qui rend le nom unique, et est ajoutée à la liste des filtres. Vous pouvez modifier la copie comme tout autre filtre.

Si vous avez créé des rôles d'administration déléguée (voir *Administration déléguée*, page 237), les Super administrateurs peuvent copier les filtres qu'ils ont créés pour d'autres rôles pour que les administrateurs délégués les utilisent.

Pour copier des filtres pour un autre rôle, cochez la case accolée au nom du filtre, puis cliquez sur **Copier dans le rôle**. Pour plus d'informations, consultez *Copie de filtres et de stratégies vers des rôles*, page 172.

Création d'un filtre de catégories

Rubriques connexes :

- *Fonctionnement des filtres*, page 48
- *Modification d'un filtre de catégories*, page 50

La page **Gestion des stratégies > Filtres > Ajouter un filtre de catégories** permet de créer un nouveau filtre de catégories. Vous pouvez partir d'un modèle prédéfini ou copier un filtre de catégories existant et l'utiliser comme point de départ du nouveau filtre.

1. Entrez un **nom de filtre** unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Les noms de filtre peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez une brève **Description** du filtre. Cette description apparaît à côté du nom du filtre dans la section Filtres de catégories de la page Filtres et doit décrire l'objectif du filtre.

   Les restrictions de caractères qui s'appliquent aux noms de filtre s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).
3. Sélectionnez une entrée dans la liste déroulante pour choisir d'utiliser un modèle ou de copier un filtre existant. Pour plus d'informations sur les modèles, consultez *Modèles de filtres de catégories et de protocoles*, page 55.
4. Pour voir et modifier le nouveau filtre, cliquez sur **OK**. Le filtre est ajouté dans la liste **Filtres de catégories** de la page Filtres.

Pour personnaliser le filtre, cliquez sur son nom et passez à la section *Modification d'un filtre de catégories*.

Modification d'un filtre de catégories

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 38
- *Actions de filtrage*, page 44
- *Utilisation de temps contingenté pour limiter l'accès Internet*, page 46
- *Accès par mot de passe*, page 47
- *Fonctionnement des filtres*, page 48
- *Fonctionnement des catégories*, page 175

La page **Gestion des stratégies > Filtres > Modifier un filtre de catégories** permet de modifier les filtres de catégories existants.

Important

Lorsque vous éditez un filtre de catégories, les modifications apportées affectent toutes les stratégies qui imposent le filtre.

Les stratégies qui imposent un filtre de catégories portant le même nom dans un autre rôle d'administration déléguée ne sont pas affectées.

Le nom du filtre et sa description s'affichent en haut de la page.

- Cliquez sur **Renommer** pour modifier le nom du filtre.
- Entrez simplement votre texte dans le champ **Description** pour modifier la description du filtre.

Le nombre accolé aux **Stratégies utilisant ce filtre** indiquent le nombre de stratégies qui utilisent actuellement le filtre sélectionné. Si le filtre de catégories est actif, cliquez sur **Afficher les stratégies** pour obtenir la liste des stratégies qui imposent le filtre.

La partie inférieure de la page présente la liste des catégories et des actions actuellement appliquées à chacune d'elles.

1. Sélectionnez une entrée dans la liste **Catégories** pour voir des informations sur la catégorie ou pour modifier l'action de filtrage qui lui est associée.
2. Avant de modifier l'action appliquée à une catégorie, utilisez la section **Détails sur la catégorie** pour vérifier les attributs spéciaux associés à la catégorie.
   - Pour vérifier les URL recatégorisées ou non filtrées éventuellement affectées à la catégorie, cliquez sur **Afficher les URL personnalisées dans cette catégorie**. Voir *Redéfinition du filtrage pour des sites spécifiques*, page 182.
   - Pour vérifier les mots-clés affectés à la catégorie, cliquez sur **Afficher les mots-clés dans cette catégorie**. Voir *Filtrage par mots-clés*, page 180.

- Pour vérifier les expressions régulières utilisées pour définir des URL personnalisées ou des mots-clés pour la catégorie, cliquez sur **Afficher les expressions régulières dans cette catégorie**.

3. Servez-vous des boutons situés au bas de la liste des catégories pour modifier l'action appliquée à la catégorie sélectionnée. Pour plus d'informations sur les actions disponibles, consultez *Actions de filtrage*, page 44.

   Les administrateurs délégués ne peuvent pas modifier l'action associée aux catégories verrouillées par un Super administrateur. Pour plus d'informations, consultez *Définition de restrictions de filtrage pour tous les rôles*, page 267.

4. Servez-vous des cases à cocher situées au bas de la liste Catégories pour appliquer des actions de filtrage avancées à la catégorie sélectionnée :

   - Pour modifier la façon dont les mots-clés sont utilisés dans le filtrage de la catégorie sélectionnée, activez ou désactivez la case à cocher **Bloquer des mots-clés**. *Filtrage par mots-clés*, page 180
   - Pour indiquer si les utilisateurs peuvent accéder à certains types de fichiers provenant des sites de la catégorie sélectionnée, activez ou désactivez la case à cocher **Bloquer des types de fichiers**. Voir *Gestion du trafic en fonction du type de fichiers*, page 193.

     Si vous avez choisi de bloquer certains types de fichiers, sélectionnez un ou plusieurs types de fichiers à bloquer.
   - Pour spécifier si l'accès au site de la catégorie est limité en fonction de certains seuils de bande passante, activez ou désactivez la case à cocher **Bloquer avec Bandwidth Optimizer**. Voir *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.

     Si vous avez choisi un blocage dépendant de la bande passante, définissez les limites de seuil à utiliser.

5. Répétez les étapes 1 à 3 pour modifier les actions de filtrage appliquées aux autres catégories.
6. Après avoir modifié le filtre, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Filtres. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour activer un nouveau filtre de catégories, ajoutez-le à une stratégie et attribuez cette dernière à des clients. Voir *Stratégies de filtrage Internet*, page 73.

Création d'un filtre de protocoles

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 38
- *Actions de filtrage*, page 44
- *Modification d'un filtre de protocoles*, page 52
- *Fonctionnement des protocoles*, page 184

La page **Gestion des stratégies > Filtres > Ajouter un filtre de protocoles** permet de définir un nouveau filtre de protocoles. Vous pouvez partir d'un modèle prédéfini ou copier un filtre de protocoles existant et l'utiliser comme point de départ du nouveau filtre.

1. Entrez un **nom de filtre** unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Les noms de filtre peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez une brève **Description** du filtre. Cette description apparaît à côté du nom du filtre dans la section Filtres de protocoles de la page Filtres et doit décrire l'objectif du filtre.

   Les restrictions de caractères qui s'appliquent aux noms de filtre s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).
3. Sélectionnez une entrée dans la liste déroulante pour choisir d'utiliser un modèle (voir *Modèles de filtres de catégories et de protocoles*, page 55) ou de copier un filtre existant.
4. Pour voir et modifier le nouveau filtre, cliquez sur **OK**. Le filtre est ajouté dans la liste **Filtres de protocoles** de la page Filtres.

Pour finir de personnaliser le nouveau filtre, passez à la section *Modification d'un filtre de protocoles*.

Modification d'un filtre de protocoles

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 38
- *Création d'un filtre de protocoles*, page 51
- *Actions de filtrage*, page 44
- *Fonctionnement des protocoles*, page 184
- *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191

La page **Gestion des stratégies > Filtres > Modifier un filtre de protocoles** permet de modifier les filtres de protocoles existants.

Important

Les modifications apportées ici concernent toutes les stratégies qui appliquent ce filtre.

Les stratégies qui imposent un filtre de protocoles portant le même nom dans un autre rôle d'administration déléguée ne sont pas affectées.

Le nom du filtre et sa description s'affichent en haut de la page.

- Cliquez sur **Renommer** pour modifier le nom du filtre.
- Entrez simplement votre texte dans le champ **Description** pour modifier la description du filtre.

Le nombre accolé aux **Stratégies utilisant ce filtre** indiquent le nombre de stratégies qui utilisent actuellement le filtre sélectionné. Si le filtre de protocoles est actif, cliquez sur **Afficher les stratégies** pour obtenir la liste des stratégies qui imposent le filtre.

La partie inférieure de la page présente la liste des protocoles et des actions actuellement appliquées à chacune d'elles.

Pour modifier la façon dont les protocoles sont filtrés et journalisés :

1. Sélectionnez un protocole dans la liste **Protocoles**. Les actions de filtrage avancées liées au protocole sélectionné s'affichent à droite de la liste.
2. Servez-vous des boutons **Autoriser** et **Bloquer** situés au bas de la liste Protocoles pour modifier l'action appliquée au protocole sélectionné.

   Remarque

   Websense peut bloquer les demandes de protocole de type TCP, mais pas celles de type UDP.

   Certaines applications utilisent à la fois des messages de type TCP et UDP. Si une demande initiale d'application est effectuée sur le réseau via TCP, mais que les données suivantes sont envoyées via UDP, Websense bloque la demande TCP initiale, puis le trafic UDP qui s'ensuit.

   Les demandes UDP peuvent être journalisées comme bloquées, même lorsqu'elles sont autorisées.

   Pour appliquer la même action aux autres protocoles du groupe de protocoles sélectionné, cliquez sur **Appliquer au groupe**.
3. Si vous voulez que les informations relatives à l'utilisation du protocole sélectionné soient disponibles pour les alertes ou les rapports, cochez la case **Journaliser les données de protocole**.
4. Pour imposer des limites de bande passante à l'utilisation de ce protocole, cliquez sur **Bloquer avec Bandwidth Optimizer** et définissez les seuils de bande passante à utiliser. Pour plus d'informations, consultez *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.
5. Après avoir modifié le filtre, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Filtres. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour activer un nouveau filtre de protocoles, ajoutez-le à une stratégie et attribuez cette dernière à des clients (voir *Stratégies de filtrage Internet*, page 73).

> **Remarque**
> Vous pouvez créer des stratégies qui imposent un filtre de protocoles à partir d'une heure spécifique. Si l'utilisateur démarre une session de protocole avant que ce filtre ne s'applique, il peut accéder au protocole, même si le filtre le bloque, tant que la session se poursuit. Lorsque l'utilisateur met fin à la session, les autres demandes pour ce protocole sont bloquées.

Filtres de catégories et de protocoles définis par Websense

Websense comprend plusieurs exemples de filtres de catégories et de protocoles. Vous pouvez utiliser ces filtres en l'état ou les modifier en fonction de vos besoins de filtrage. Si vous n'avez pas besoin des filtres prédéfinis, la plupart d'entre eux peuvent être supprimés.

Les filtres de catégories prédéfinis sont :

- De base
- Sécurité de base
- Bloquer tout
- Par défaut
- Surveiller uniquement
- Autoriser tout

Les filtres de catégories Bloquer tout et Autoriser tout n'apparaissent pas dans la liste de la page Filtres, mais peuvent être ajoutés à des stratégies. Ces filtres jouent un rôle particulier dans le filtrage et ne peuvent être ni supprimés ni modifiés. Lorsqu'une demande Internet est filtrée, Websense commence par vérifier si le filtre Bloquer tout ou Autoriser tout s'applique, avant de vérifier les autres filtres (voir *Filtrage d'un site*, page 81).

Les filtres de protocoles prédéfinis sont :

- Sécurité de base
- Par défaut
- Surveiller uniquement
- Autoriser tout

Le filtre de protocoles Autoriser tout, comme le filtre de catégories équivalent, n'apparaît pas dans la liste de la page Filtres et ne peut être ni modifié ni supprimé. Il est également prioritaire dans le filtrage.

Les filtres de catégories et de protocoles Par défaut peuvent être modifiés, mais ne peuvent pas être supprimés. Dans les environnements mis à niveau, si la stratégie Par défaut présente des différences, les filtres Par défaut sont utilisés pour filtrer les demandes auxquelles aucune stratégie ne s'applique.

Modèles de filtres de catégories et de protocoles

Lorsque vous créez un nouveau filtre de catégories ou de protocoles, vous pouvez commencer par copier un filtre existant de la page Filtres, choisir un filtre existant comme modèle dans la page Ajouter un filtre, ou utiliser un **modèle** de filtre.

Websense comprend 5 modèles de filtres de catégories :

- **Surveiller uniquement** et **Autoriser tout** autorisent toutes les catégories.
- **Bloquer tout** bloque toutes les catégories.
- **De base** bloque les catégories généralement bloquées et autorise le reste.
- **Par défaut** applique les actions Bloquer, Autoriser, Continuer et Contingent aux catégories.
- **Sécurité de base** bloque uniquement les catégories par défaut de la classe Risque pour la sécurité (voir *Classes de risque*, page 41).

Websense comprend également 3 modèles de filtres de protocoles :

- **Surveiller uniquement** et **Autoriser tout** autorisent tous les protocoles.
- **Sécurité de base** bloque les protocoles Partage de fichiers P2P et Antiblocage par proxy, de même que Pièces jointes de messagerie instantanée (en cas d'abonnement) et Trafic malveillant (Websense Web Security).
- **Par défaut** bloque les protocoles Messagerie instantanée, de même que Partage de fichiers P2P, Antiblocage par proxy, Pièces jointes de messagerie instantanée (en cas d'abonnement) et Trafic malveillant (Websense Web Security).

Bien que vous puissiez modifier ou supprimer la plupart des filtres de protocoles et de catégories définis par Websense, vous ne pouvez ni modifier ni supprimer les modèles. De même, vous pouvez créer autant de filtres personnalisés que nécessaire, mais vous ne pouvez pas créer de nouveaux modèles.

Les modèles ne pouvant pas être modifiés, ils constituent une référence constante aux actions de filtrage originales appliquées par les filtres définis par Websense. Par exemple, les modèles de filtres de catégories et de protocoles Standard appliquent les mêmes actions que les filtres de catégories et de protocoles Par défaut d'origine. Cela signifie que vous pouvez toujours restaurer la configuration du filtrage original de Websense en créant des filtres qui utilisent les paramètres par défaut des modèles.

Pour obtenir des instructions sur l'utilisation d'un modèle pour créer un nouveau filtre, consultez les sections *Création d'un filtre de catégories*, page 49 ou *Création d'un filtre de protocoles*, page 51.

Configuration des paramètres de filtrage de Websense

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 38
- *Clients*, page 59
- *Pages de blocage*, page 85
- *Actions de filtrage*, page 44
- *Accès par mot de passe*, page 47
- *Ordre du filtrage*, page 80
- *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191
- *Filtrage par mots-clés*, page 180

La page **Paramètres > Filtrage** permet de définir les paramètres de base d'un grand nombre de fonctions de filtrage.

Sous **Bandwidth Optimizer**, entrez les informations nécessaires pour filtrer l'utilisation d'Internet en fonction de la bande passante disponible. Pour plus d'informations sur le filtrage basé sur la bande passante, consultez *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.

1. Pour spécifier une **vitesse de connexion à Internet**, procédez de l'une des manières suivantes :
   - Sélectionnez une vitesse standard dans la liste déroulante.
   - Entrez la vitesse du réseau en Kbits/s dans le champ de texte.
2. Servez-vous du champ **Bande passante par défaut pour le réseau** pour définir un seuil par défaut (pourcentage du trafic total du réseau) à utiliser lorsque le filtrage de la bande passante du réseau est activé.
3. Servez-vous du champ **Bande passante par défaut par protocole** pour définir un seuil par défaut à utiliser lorsque le filtrage de la bande passante des protocoles est activé.

Utilisez la section **Filtrage général** pour déterminer comment les utilisateurs sont filtrés lorsque plusieurs stratégies de groupe s'appliquent, pour spécifier des options de recherche de mots-clés, et pour définir les comportements d'accès par mot de passe, de prolongation et de temps contingenté.

1. Pour spécifier comment les utilisateurs sont filtrés lorsque plusieurs stratégies de groupe s'appliquent, activez ou désactivez l'option **Utiliser la stratégie de groupe la plus restrictive** (voir *Ordre du filtrage*, page 80).
   - Lorsque l'option est activée, la stratégie assurant le paramètre de filtrage le plus restrictif est appliquée. En d'autres termes, si une stratégie de groupe applicable bloque l'accès à une catégorie alors qu'une autre en autorise l'accès, la demande de l'utilisateur pour un site de cette catégorie est bloquée.

- Lorsque l'option n'est pas activée, le paramètre le plus permissif est utilisé.

2. Sélectionnez l'une des **options de recherche de mots-clés** suivantes (voir *Filtrage par mots-clés*, page 180).

CGI uniquement	Bloque les sites lorsque des mots-clés apparaissent dans les chaînes de requête CGI (après le « ? » dans une adresse Internet). Exemple : **search.yahoo.com/search?p=test** Websense ne recherche pas les mots-clés placés avant le « ? » lorsque cette option est activée.
URL uniquement	Bloque les sites lorsque des mots-clés apparaissent dans l'URL. Si l'adresse demandée contient une chaîne de requête CGI, Websense recherche les mots-clés jusqu'au « ? ».
URL et CGI	Bloque les sites lorsque des mots-clés apparaissent dans l'adresse. Si une chaîne de requête CGI est présente, Websense recherche les mots-clés placés avant et après le « ? ».
Désactiver le blocage par mot-clé	Cette option doit être utilisée avec précaution. **Désactiver le blocage par mot-clé** désactive le blocage par mot-clés, même lorsque l'option **Bloquer les mots-clés** est activée pour un filtre de catégories.

3. Dans le champ **Délai d'attente d'accès par mot de passe**, entrez le nombre maximal de secondes (3600 au maximum, 60 par défaut) pendant lesquelles un utilisateur peut accéder aux sites de toutes les catégories après avoir sélectionné un accès par mot de passe (voir *Accès par mot de passe*, page 47).
4. Dans le champ **Délai de prolongation**, entrez le nombre maximal de secondes (3600 au maximum, 60 par défaut) pendant lesquelles un utilisateur qui clique sur Continuer peut accéder aux sites des catégories régies par l'action Confirmer (voir *Actions de filtrage*, page 44).
5. Dans le champ **Durée de la session de temps contingenté**, entrez l'intervalle (60 minutes maximum, 10 par défaut) durant lequel les utilisateurs peuvent visiter les sites des catégories limitées par du temps contingenté (voir *Utilisation de temps contingenté pour limiter l'accès Internet*, page 46).

   La session commence lorsque l'utilisateur clique sur le bouton Utiliser du temps contingenté.
6. Entrez le **Temps contingenté par défaut par jour** (240 minutes maximum, 60 par défaut) pour tous les utilisateurs.

   Pour modifier le temps contingenté des utilisateurs individuels, accédez à la page **Stratégies > Clients**.

   Au fur et à mesure que vous modifiez la longueur de la session de temps contingenté et le temps contingenté par défaut par jour, les **Sessions de temps contingenté par défaut par jour** sont calculées et affichées.

Utilisez la section **Messages de blocage** pour entrer l'URL ou le chemin d'une autre page de blocage HTML que vous avez créée pour le cadre supérieur des messages de blocage de type navigateur (voir *Création d'autres messages de blocage*, page 92).

- Des pages distinctes peuvent être utilisées pour les différents protocoles : **FTP**, **HTTP** (y compris **HTTPS**) et **Gopher**.
- Pour utiliser le message de blocage par défaut fourni par Websense, ou une version personnalisée de ce message, ne renseignez pas ces champs (voir *Personnalisation du message de blocage*, page 88).

Sous **Filtrage de la recherche**, sélectionnez **Activer le filtrage de la recherche** pour que Websense active un paramètre intégré à certains moteurs de recherche, de sorte que les vignettes et autres contenus explicites associés à des sites bloqués ne s'affichent pas dans les résultats de la recherche (voir *Filtrage de la recherche*, page 47).

Les moteurs de recherche pour lesquels cette fonction est prise en charge sont affichés au bas de la section.

Lorsque la configuration des paramètres du filtrage est terminée, cliquez sur **OK** pour mettre en cache les modifications apportées. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

3 Clients

Vous pouvez personnaliser la façon dont Websense filtre les demandes provenant d'utilisateurs ou d'ordinateurs spécifiques en les ajoutant en tant que **clients** dans Websense Manager. Ces clients peuvent être des :

- **Ordinateurs** : ordinateurs individuels de votre réseau, définis par leur adresse IP.
- **Réseaux** : groupes d'ordinateurs, définis collectivement sous forme de plage d'adresses IP.
- **Utilisateurs** : comptes d'utilisateur, de groupe ou de domaine présents dans un service d'annuaire pris en charge.

Au départ, Websense filtre tous les clients de la même manière, à l'aide de la stratégie **Par défaut** (voir *La stratégie Par défaut*, page 74). Lorsque vous ajoutez un client dans la page Clients de Websense Manager, vous pouvez lui affecter une stratégie de filtrage spécifique.

Lorsque plusieurs stratégies s'appliquent à un même client (par exemple lorsque des stratégies différentes sont attribuées à l'utilisateur et son ordinateur), Websense Express détermine les priorités comme suit :

1. Application de la stratégie attribuée à **l'utilisateur** à l'origine de la demande. Si cette stratégie n'a pas de filtre planifié au moment de la demande, la prochaine stratégie applicable est utilisée.
2. Lorsque aucune stratégie spécifique à l'utilisateur n'est détectée, ou lorsque la stratégie ne présente pas de filtre actif au moment de la demande, le système recherche une stratégie attribuée à **l'ordinateur** (en premier) ou au **réseau** (en second) d'où provient la demande.
3. Lorsque aucune stratégie spécifique à l'ordinateur ou au réseau n'est détectée, ou lorsque la stratégie ne présente pas de filtre actif au moment de la demande, le système recherche une stratégie attribuée à un **groupe** auquel l'utilisateur appartient. Si utilisateur appartient à plusieurs groupes, Websense tient compte de toutes les stratégies de groupes qui s'appliquent (voir *Ordre du filtrage*, page 80).
4. En l'absence d'une stratégie de groupe, le système recherche une stratégie affectée au **domaine** (OU) de l'utilisateur.
5. Lorsque aucune stratégie applicable n'est détectée, ou lorsque la stratégie ne présente pas de filtre de catégories au moment de la demande, le système applique la stratégie **Par défaut** affectée au rôle attribué au client.

Pour plus d'informations sur l'application des stratégies de filtrage aux clients par Websense, consultez la section *Filtrage d'un site*, page 81.

Fonctionnement des clients

Rubriques connexes :

- *Clients*, page 59
- *Travail avec des ordinateurs et des réseaux*, page 61
- *Travail avec des utilisateurs et des groupes*, page 62
- *Ajout d'un client*, page 68
- *Modifications des paramètres des clients*, page 70

La page **Gestion des stratégies > Clients** permet d'afficher des informations sur les clients existants, d'ajouter, de modifier ou de supprimer des clients, ou de déplacer des clients vers un rôle d'administration déléguée.

Si vous êtes administrateur délégué, vous devez ajouter des clients dans la liste de vos clients gérés pour qu'ils apparaissent dans la page Clients. Reportez-vous à la section *Ajout d'un client*, page 68 pour obtenir des instructions.

Les clients sont divisés en 3 groupes :

- **Annuaire**, qui comprend les utilisateurs, les groupes et les domaines de votre service d'annuaire (voir *Travail avec des utilisateurs et des groupes*, page 62).
- **Réseaux**, plages d'adresse IP au sein du réseau filtré pouvant être gérées par une seule et même stratégie (voir *Travail avec des ordinateurs et des réseaux*, page 61).
- **Ordinateurs**, ordinateurs individuels du réseau filtré, identifiés par leur adresse IP (voir *Travail avec des ordinateurs et des réseaux*, page 61).

Cliquez sur le signe (+) accolé au type de client pour voir la liste des clients existants du type sélectionné. Chaque liste de clients comprend :

- Le nom du client, l'adresse IP ou la plage d'adresses IP.
- La **stratégie** actuellement affectée au client. La stratégie **Par défaut** est utilisée jusqu'à ce que vous en affectiez une autre (voir *Stratégies de filtrage Internet*, page 73).
- L'indication si le client peut ou non utiliser l'option d'**accès par mot de passe** pour afficher des sites bloqués (voir *Accès par mot de passe*, page 47).
- L'indication si une quantité personnalisée de **temps contingenté** est attribuée au client (voir *Utilisation de temps contingenté pour limiter l'accès Internet*, page 46).

Pour rechercher un client spécifique, localisez le nœud approprié dans l'arborescence.

Pour modifier les paramètres des stratégies des clients, d'accès par mot de passe, de temps contingenté ou d'authentification, sélectionnez un ou plusieurs clients dans la

liste, puis cliquez sur **Éditer**. Pour plus d'informations, consultez *Modifications des paramètres des clients*, page 70.

Pour ajouter un client, ou pour appliquer une stratégie à un client géré qui n'apparaît pas encore dans la page Clients, cliquez sur **Ajouter**, puis passez à la section *Ajout d'un client*, page 68 pour plus d'informations.

Si vous avez créé des rôles d'administration déléguée (voir *Administration déléguée*, page 237), les Super administrateurs peuvent déplacer leurs clients vers d'autres rôles. Commencer par cocher la case accolée à l'entrée du client, puis cliquez sur **Déplacer vers le rôle**. Lorsqu'un client est déplacé vers un rôle d'administration déléguée, la stratégie et les filtres qui lui sont appliqués sont copiés vers le rôle. Pour plus d'informations, consultez *Déplacements de clients vers des rôles*, page 70.

Si vous avez configuré Websense pour qu'il communique avec un service d'annuaire de type LDAP, le bouton **Gérer les groupes LDAP personnalisés** s'affiche dans la barre d'outils en haut de la page. Cliquez sur ce bouton pour ajouter ou modifier les groupes en fonction d'un attribut LDAP (voir *Travail avec des groupes LDAP personnalisés*, page 66).

Pour supprimer un client de Websense Manager, sélectionnez-le, puis cliquez sur **Supprimer**.

Travail avec des ordinateurs et des réseaux

Rubriques connexes :

- *Fonctionnement des clients*, page 60
- *Travail avec des utilisateurs et des groupes*, page 62
- *Ajout d'un client*, page 68
- *Attribution d'une stratégie aux clients*, page 79

Dans Websense Manager, un **ordinateur** est une adresse IP (par exemple 10.201.3.1) associée à un ordinateur filtré. Un **réseau** est une plage d'adresses IP (par exemple 10.201.3.2 à 10.201.3.44) associée à un groupe d'ordinateurs filtrés.

Vous pouvez affecter des stratégies à des clients ordinateur et réseau de la même façon que pour les clients utilisateur, groupe ou domaine.

- Affectez par exemple une stratégie à un **ordinateur** qui n'oblige pas les utilisateurs à se connecter, ou auquel les utilisateurs peuvent accéder avec un compte Invité.
- Affectez une stratégie à un **réseau** pour appliquer simultanément la même stratégie de filtrage à plusieurs ordinateurs.

Lorsque vous affectez une stratégie à un ordinateur ou à un réseau, elle s'applique quelle que soit la personne connectée sur l'ordinateur filtré, **sauf** si vous avez affecté

une stratégie à l'utilisateur connecté. Cette stratégie d'ordinateur ou de réseau est prioritaire sur toute stratégie de **groupe** susceptible de s'appliquer à l'utilisateur.

Travail avec des utilisateurs et des groupes

Rubriques connexes :

- *Fonctionnement des clients*, page 60
- *Services d'annuaire*, page 63
- *Travail avec des groupes LDAP personnalisés*, page 66
- *Travail avec des ordinateurs et des réseaux*, page 61
- *Ajout d'un client*, page 68
- *Attribution d'une stratégie aux clients*, page 79

Pour appliquer des stratégies à desutilisateurs et à des groupes de votre réseau, configurez Websense pour qu'il accède à votre service d'annuaire et récupère les informations des objets de l'annuaire (utilisateur, groupe, domaine et unité d'organisation).

Websense peut communiquer avec Windows NT Directory / Active Directory (mode mixte) et avec Windows Active Directory, Novell eDirectory et Sun Java System Directory accessibles via LDAP (Lightweight Directory Access Protocol).

Remarque

Lorsque vous utilisez un service d'annuaire de type LDAP, les noms d'utilisateur en double ne sont pas pris en charge. Assurez-vous que le même nom d'utilisateur n'apparaisse pas dans plusieurs domaines.

De même, si vous utilisez Windows Active Directory ou Sun Java System Directory, les noms d'utilisateur associés à des mots de passe vides ne sont pas pris en charge. Assurez-vous que des mots de passe aient été attribués à tous les utilisateurs.

Websense User Service transmet les informations provenant du service d'annuaire à Policy Server et Filtering Service pour leur application dans les stratégies de filtrage.

Websense, Inc. recommande d'installer User Service sur un ordinateur Windows (bien qu'il puisse résider sur un ordinateur Linux). En général, il s'agit de l'ordinateur sur lequel Policy Server est installé.

Pour savoir comment configurer Websense pour qu'il communique avec votre service d'annuaire, consultez la section *Services d'annuaire*.

Services d'annuaire

Un service d'annuaire est un outil qui stocke des informations sur les utilisateurs et les ressources d'un réseau. Avant de pouvoir ajouter des clients utilisateur (utilisateurs, groupes, domaines ou unités d'organisation) dans Websense Manager, vous devez configurer Websense pour qu'il récupère les informations dans votre service d'annuaire.

Utilisez la page **Paramètres > Services d'annuaire** pour identifier le service d'annuaire utilisé dans votre réseau. Vous ne pouvez configurer les paramètres que d'un type de service d'annuaire par serveur Policy Server.

Commencez par sélectionner un service d'annuaire dans la liste Annuaires. Votre choix détermine les paramètres affichés sur la page.

Pour obtenir des instructions sur la configuration, consultez la section appropriée :

- *Annuaire Windows NT / Active Directory (mode mixte)*, page 63
- *Windows Active Directory (Native Mode)*, page 63
- *Novell eDirectory et Sun Java System Directory*, page 65

Annuaire Windows NT / Active Directory (mode mixte)

Si votre service d'annuaire est Windows NT Directory ou Active Directory en Mode mixte, aucune configuration supplémentaire n'est nécessaire.

Dans de rares cas, si vous utilisez un autre service d'annuaire, vous devrez éventuellement fournir des informations supplémentaires dans cet écran. Cela se produit dans les cas suivants :

- DC Agent est utilisé pour l'identification transparente (voir *DC Agent*, page 213)

  et
- User Service s'exécute sur un ordinateur Linux

Si cela correspond à votre configuration, fournissez les informations d'identification administratives énumérées sous Windows NT Directory / Active Directory (mode mixte). Si votre installation n'utilise pas cette configuration, les champs d'informations d'identification sont désactivés.

Windows Active Directory (Native Mode)

Windows Active Directory stocke les informations des utilisateurs dans un ou plusieurs *catalogues globaux*. Le catalogue global permet aux individus et aux applications de rechercher des objets (utilisateurs, groupes, etc.) dans un domaine Active Directory.

Pour que Websense puisse communiquer avec Active Directory en mode natif, vous devez fournir des informations sur les serveurs de catalogue global de votre réseau.

1. Cliquez sur **Ajouter**, à côté de la liste des serveurs de catalogue global. La page Ajouter un serveur de catalogue global apparaît.

2. Utilisez le champ **IP ou nom du serveur** pour identifier le serveur de catalogue global :
   - Si plusieurs serveurs de catalogue global sont configurés pour le basculement, entrez le nom de domaine DNS.
   - Si vos serveurs de catalogue global ne sont pas configurés pour le basculement, entrez l'adresse IP ou le nom d'hôte (si la résolution de noms est activée dans votre réseau) du serveur à ajouter.
3. Entrez le numéro de **Port** que Websense doit utiliser pour communiquer avec le catalogue global (par défaut **3268**).
4. Éventuellement, entrez le **Contexte racine** que Websense doit utiliser pour rechercher les informations sur les utilisateurs. Si vous entrez une valeur, le contexte doit être valide dans votre domaine.
   - Si vous avez défini le port de communication 3268 ou 3269, le contexte racine n'est pas nécessaire.
   - Si le port spécifié est 389 ou 636, vous devez fournir un contexte racine.
   - Si le champ Contexte racine n'est pas renseigné, Websense commence ses recherches au premier niveau du service d'annuaire.

   Remarque
   Assurez-vous que le même nom d'utilisateur n'apparaisse pas dans plusieurs domaines. Si Websense détecte des noms de compte en double pour un utilisateur, ce dernier ne peut pas être identifié de manière transparente.

5. Définissez le compte d'administration que Websense doit utiliser pour récupérer les informations de nom d'utilisateur et de chemin dans le service d'annuaire. Ce compte doit pouvoir interroger et lire le service d'annuaire, mais n'a pas besoin de pouvoir le modifier ni d'être un administrateur de domaine.

   Sélectionnez **Nom distinctif par composants** ou **Nom distinctif complet** pour spécifier vos préférences de saisie des informations de compte.
   - Si vous activez Nom distinctif par composants, entrez le **Nom affiché**, le **Mot de passe**, le **Dossier du compte** et le **Nom du domaine DNS** du compte d'administration. Utilisez la forme de nom commun (cn) du nom d'utilisateur d'administration, et non la forme ID utilisateur (uid).

     Remarque
     Le champ **Dossier du compte** ne prend pas en charge les valeurs avec balise d'unité d'organisation (ou) (par exemple, *ou=Économie*). Si votre nom de compte d'administration contient une balise 'ou', entrez le Non distinctif complet du compte d'administration.

   - Si vous activez Nom distinctif complet, entrez le nom distinctif sous forme de chaîne dans le champ **Nom distinctif de l'utilisateur** (par exemple, *cn=Admin, cn=Utilisateurs, ou=InfoSysteme, dc=societe, dc=net*), puis le **Mot de passe** de ce compte.

6. Cliquez sur **OK**.
7. Reprenez la procédure ci-dessus pour chaque serveur de catalogue global.
8. Cliquez sur **Paramètres avancés de l'annuaire**, puis passez à la section *Paramètres de l'annuaire avancés*, page 65.

Novell eDirectory et Sun Java System Directory

Pour récupérer les informations du service d'annuaire, Websense a besoin du nom distinctif, du contexte racine et du mot de passe d'un compte d'utilisateur disposant de droits d'administrateur.

1. Entrez l'adresse IP ou le nom du serveur d'annuaire dans le champ **IP du serveur**.
2. Entrez le numéro de **Port** que Websense doit utiliser pour communiquer avec l'annuaire. Le port par défaut est 389.
3. Si votre service d'annuaire requiert des droits d'administrateur pour un accès en lecture, entrez le **Nom distinctif de l'administrateur** et le **Mot de passe**.
4. Éventuellement, entrez le **Contexte racine** que Websense doit utiliser pour rechercher les informations sur les utilisateurs. Par exemple *o=domain.com*.

   Limiter le contexte accroît la vitesse et l'efficacité de la récupération des informations des utilisateurs.

   Remarque

   Assurez-vous que le même nom d'utilisateur n'apparaisse pas dans plusieurs domaines. Si Websense détecte des noms de compte en double pour un utilisateur, ce dernier ne peut pas être identifié de manière transparente.

5. Cliquez sur **Paramètres avancés de l'annuaire**, puis passez à la section *Paramètres de l'annuaire avancés*, page 65.

Paramètres de l'annuaire avancés

Rubriques connexes :

- *Windows Active Directory (Native Mode)*, page 63
- *Novell eDirectory et Sun Java System Directory*, page 65

Ces paramètres permettent de définir :

- La façon dont Websense recherche des informations sur les utilisateurs, les groupes et les domaines dans le service d'annuaire.
- Si Websense utilise une connexion cryptée pour communiquer avec le service d'annuaire.
- Quel jeu de caractères est utilisé par Websense pour coder les informations LDAP.

Configurez ces paramètres de façon appropriée pour tous les services d'annuaire de type LDAP.

1. Si vous utilisez des types de classes d'objets personnalisés (noms d'attributs) dans votre service d'annuaire, activez **Utiliser des filtres personnalisés**. Les chaînes des filtres par défaut s'affichent dans les champs Filtres.
2. Modifiez les chaînes de filtrage existantes, en les remplaçant par les types de classes d'objets spécifiques à votre annuaire. Par exemple, si votre annuaire utilise un type de classes d'objets tel que **dept** au lieu de **ou** (unité d'organisation), insérez une nouvelle valeur dans le champ Filtre de recherche de domaine.

   Les attributs sont toujours les chaînes utilisées lors des recherches effectuées sur le contenu du service d'annuaire. Les filtres personnalisés offrent les fonctions décrites ici.

   - **Filtre de recherche d'utilisateur** détermine comment User Service recherche des utilisateurs.
   - **Filtre de recherche de groupe** détermine comment User Service recherche des groupes.
   - **Filtre de recherche de domaine** détermine comment User Service recherche des domaines et des unités d'organisation.
   - **Filtre de recherche des groupes d'utilisateurs** détermine comment User Service associe les utilisateurs aux groupes.
3. Pour sécuriser les communications entre Websense et votre service d'annuaire, activez l'option **Utiliser SSL**.
4. Pour définir le jeu de caractères utilisé par Websense pour coder les informations LDAP, activez **UTF-8** ou **MBCS**.

   Le jeu de caractères MBCS (MultiByte Character Set) est généralement utilisé pour le codage des langues d'Extrême-Orient telles que le chinois, le japonais et le coréen.
5. Cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Travail avec des groupes LDAP personnalisés

Rubriques connexes :

- *Travail avec des utilisateurs et des groupes*, page 62
- *Services d'annuaire*, page 63
- *Ajout ou modification d'un groupe LDAP personnalisé*, page 67

La page **Gérer les groupes LDAP personnalisés** permet de gérer les groupes personnalisés en fonction des attributs définis dans votre service d'annuaire. Cette

option est uniquement disponible si vous avez configuré Websense pour qu'il communique avec un service d'annuaire de type LDAP.

> **Important**
>
> Lorsque vous ajoutez des groupes LDAP dans Websense Manager, les définitions de groupes sont stockées par le serveur Policy Server actif et n'affectent pas les autres instances de Policy Server. Pour ajouter des groupes LDAP personnalisés dans plusieurs serveurs Policy Server, utilisez Websense Manager pour vous connecter à chaque serveur Policy Server et saisissez les informations nécessaires.
>
> Si vous ajoutez des groupes LDAP personnalisés, et que vous modifiez ensuite les services d'annuaire ou l'emplacement du serveur d'annuaire, les groupes existants deviennent invalides. Vous devez alors rajouter les groupes, puis définir chacun d'eux en tant que client.

- Pour ajouter un groupe, cliquez sur **Ajouter** (voir *Ajout ou modification d'un groupe LDAP personnalisé*, page 67).
- Pour modifier une entrée de la liste, cliquez sur le nom de son groupe (voir *Ajout ou modification d'un groupe LDAP personnalisé*).
- Pour supprimer une entrée, sélectionnez-la, puis cliquez sur **Supprimer**.

Lorsque la modification des groupes LDAP personnalisés est terminée, cliquez sur **OK** pour mettre en cache les modifications et revenir à la page précédente. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout ou modification d'un groupe LDAP personnalisé

Utilisez la page **Ajouter un groupe LDAP personnalisé** pour définir un groupe dans Websense Manager en fonction de l'un des attributs définis dans votre service d'annuaire. La page **Éditer Groupes LDAP personnalisés** permet de modifier une définition existante.

> **Important**
>
> Si vous ajoutez des groupes LDAP personnalisés, et que vous modifiez ensuite les services d'annuaire ou l'emplacement du serveur d'annuaire, les groupes existants deviennent invalides. Vous devez alors rajouter les groupes, puis définir chacun d'eux en tant que client.

1. Entrez ou modifiez le **Nom du groupe**. Utilisez un nom descriptif indiquant clairement l'objectif du groupe LDAP.

   Les noms des groupes ne respectent pas la casse et doivent être uniques.
2. Entrez ou modifiez la description qui définit ce groupe dans votre service d'annuaire. Par exemple :

```
(WorkStatus=parttime)
```

Dans cet exemple, **WorkStatus** est un attribut d'utilisateur qui indique le statut de l'emploi, et **parttime** une valeur indiquant que l'utilisateur est un employé à temps partiel.

3. Cliquez sur **OK** pour revenir à la page Gérer les groupes LDAP personnalisés. La nouvelle entrée ou l'entrée modifiée apparaît dans la liste.
4. Ajoutez ou modifiez une autre entrée ou cliquez sur **OK** pour mettre en cache les modifications et revenir à la page précédente. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout d'un client

Rubriques connexes :

- *Fonctionnement des clients*, page 60
- *Travail avec des ordinateurs et des réseaux*, page 61
- *Travail avec des utilisateurs et des groupes*, page 62
- *Recherche dans le service d'annuaire*, page 69
- *Modifications des paramètres des clients*, page 70

La page **Gestion des stratégies > Clients > Ajouter des clients** permet d'ajouter des clients utilisateur, groupe, ordinateur et réseau dans Websense Manager de manière à pouvoir ensuite leur affecter une stratégie.

Si vous êtes connecté(e) avec un rôle d'administration déléguée, vous ne pouvez ajouter que les clients qui apparaissent dans votre liste de clients gérés. Dans le cadre de la procédure d'ajout de clients gérés à la page Clients, vous devez leur affecter une stratégie.

1. Identifiez un ou plusieurs clients :
   - Pour ajouter un client utilisateur, groupe ou domaine, parcourez l'arborescence **Annuaire** pour rechercher des entrées dans votre service d'annuaire. Si vous utilisez un service d'annuaire de type LDAP, vous pouvez également cliquer sur **Rechercher** pour activer un outil de recherche d'annuaire (voir *Recherche dans le service d'annuaire*, page 69).
   - Pour ajouter un client ordinateur ou réseau, entrez une **adresse IP** ou une **plage d'adresses IP**. Deux définitions de réseau ne peuvent pas se chevaucher, mais un client réseau peut inclure une adresse IP identifiée séparément en tant que client ordinateur. Dans le cas d'un tel chevauchement, la stratégie affectée à l'ordinateur a priorité sur celle affectée au réseau.
2. Cliquez sur une flèche (>) pour ajouter chaque client à la liste des **Clients sélectionnés**.

   Pour supprimer une entrée de la liste Clients sélectionnés, sélectionnez le client, puis cliquez sur **Supprimer**.

3. Sélectionnez une **Stratégie** à affecter à tous les clients de la liste Clients sélectionnés.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Les clients sont ajoutés dans la liste appropriée de la page **Gestion des stratégies > Clients**. Pour modifier la stratégie affectée à un ou plusieurs clients, ou pour configurer d'autres paramètres de clients, sélectionnez chaque entrée de client, puis cliquez sur **Éditer**. Pour plus d'informations, consultez *Modifications des paramètres des clients*, page 70.

Recherche dans le service d'annuaire

Si vous avez configuré Websense pour qu'il communique avec un service d'annuaire de type LDAP, vous pouvez utiliser une fonction de recherche pour identifier les utilisateurs à ajouter sous forme de clients dans Websense Manager. La recherche est également disponible pour l'ajout de clients gérés et d'administrateurs à des rôles d'administration déléguée.

Pour rechercher des informations sur les utilisateurs, groupes et unités d'organisation dans un service d'annuaire :

1. Cliquez sur **Rechercher**.
2. Entrez une partie ou la totalité du **Nom** de l'utilisateur, du groupe ou de l'unité d'organisation.
3. Utilisez la liste **Type** pour préciser le type d'entrée d'annuaire (utilisateur, groupe, unité d'organisation, ou tous) à rechercher.

   Dans le cas d'un vaste service d'annuaire, l'option **Tous** peut entraîner des recherches très longues.
4. Dans l'arborescence du **Contexte de recherche**, spécifiez dans quelle partie de l'annuaire doit porter la recherche. Plus le contexte est précis, plus la recherche est rapide.
5. Cliquez sur **Aller**.

   La liste des résultats de la recherche s'affiche.
6. Sélectionnez une ou plusieurs entrées dans les résultats de la recherche, puis cliquez sur la flèche droite (>) pour ajouter chaque sélection en tant que client ou administrateur.
7. Cliquez sur **Nouvelle recherche** pour entrer d'autres critères de recherche.
8. Cliquez sur **Parcourir** pour recommencer à parcourir l'annuaire.
9. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Modifications des paramètres des clients

La page **Gestion des stratégies > Clients > Modifier le client** permet de modifier les paramètres de stratégie et d'authentification d'un ou plusieurs clients. Si vous sélectionnez plusieurs clients avant de cliquer sur Éditer, les modifications de configuration apportées dans la page Modifier le client seront appliquées à tous les clients sélectionnés.

1. Sélectionnez une **Stratégie** à appliquer aux clients sélectionnés. La stratégie Par défaut régit les clients jusqu'à ce qu'une autre stratégie leur soit affectée.
2. Pour autoriser les utilisateurs à contourner une page de blocage Websense en saisissant un mot de passe, cliquez sur **Activé** sous Accès par mot de passe, puis entrez et confirmez le mot de passe.

   Pour supprimer le droit d'accès par mot de passe d'un client, cliquez sur **Désactivé**.
3. Pour affecter une quantité personnalisée de **Temps contingenté** aux clients sélectionnés, cliquez sur **Personnalisé** et entrez le nombre de minutes de temps contingenté à affecter.

   Pour réinitialiser les paramètres de temps contingenté par défaut, cliquez sur **Par défaut**.
4. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Clients. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Les nouveaux paramètres des clients s'affichent dans la liste des clients de la page **Gestion des stratégies > Clients**.

Déplacements de clients vers des rôles

Les Super administrateurs peuvent utiliser la page **Déplacer le client dans le rôle** pour déplacer un ou plusieurs clients vers un rôle d'administration déléguée. Une fois qu'un client a été déplacé, il apparaît dans la liste des Clients gérés et sur la page Clients dans le rôle visé.

- La stratégie appliquée au client dans le rôle Super administrateurs et les filtres imposés sont copiés vers le rôle d'administration déléguée.
- Les administrateurs délégués peuvent modifier les stratégies appliquées à leurs clients gérés.
- Les restrictions de verrouillage des filtres n'affectent pas les clients gérés par les Super administrateurs, mais affectent les clients gérés dans les rôles d'administration déléguée.
- Si un groupe, un domaine ou une unité d'organisation est ajoutée dans un rôle en tant que client géré, les administrateurs délégués de ce rôle peuvent affecter des stratégies aux utilisateurs individuels du groupe, du domaine ou de l'unité d'organisation.

- Si un réseau (plage d'adresses IP) est ajouté dans un rôle en tant que client géré, les administrateurs délégués de ce rôle peuvent affecter des stratégies aux ordinateurs individuels de ce réseau.
- Un même client ne peut pas être déplacé vers plusieurs rôles.

Pour déplacer les clients sélectionnés vers un rôle d'administration déléguée :

1. Utilisez la liste déroulante **Sélectionner un rôle** pour sélectionner un rôle de destination.
2. Cliquez sur **OK**.

   Une fenêtre contextuelle signale que les clients sélectionnés sont déplacés. Le processus de déplacement peut prendre un certain temps.
3. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Si des administrateurs délégués du rôle sélectionné sont connectés avec un accès de stratégie pendant le processus de déplacement, ils devront se déconnecter de Websense Manager et se reconnecter à nouveau pour voir les nouveaux clients dans leurs listes de Clients gérés.

4 Stratégies de filtrage Internet

Rubriques connexes :

- *Filtres d'utilisation Internet*, page 37
- *Clients*, page 59
- *La stratégie Par défaut*, page 74
- *Fonctionnement des stratégies*, page 75
- *Ordre du filtrage*, page 80

Les stratégies régissent l'accès à Internet des utilisateurs. Une stratégie se compose de :

- Filtres de catégories, utilisés pour appliquer des actions (autoriser, bloquer) sur des catégories de sites Web (voir *Filtrage des catégories et des protocoles*, page 38)
- Filtres d'accès limité, utilisés pour autoriser l'accès à une liste restreinte de sites Web uniquement (voir *Restriction des utilisateurs à une liste définie de sites Internet*, page 168)
- Filtres de protocoles, utilisés pour appliquer des actions aux protocoles Internet (voir *Filtrage des catégories et des protocoles*, page 38)
- Un planning qui détermine à quel moment chaque filtre de catégories, de protocoles et d'accès limité est imposé

Une nouvelle installation de Websense comprend trois stratégies prédéfinies :

- **Par défaut** filtre l'accès Internet de tous les clients non régis par une autre stratégie. Websense commence à imposer cette stratégie dès la saisie d'une clé d'abonnement (voir *La stratégie Par défaut*, page 74).
- **Illimité** fournit un accès illimité à Internet. Cette stratégie n'est appliquée à aucun client par défaut.
- **Exemple - Utilisateur standard** montre comment plusieurs filtres de catégories et de protocoles peuvent être appliqués dans une stratégie pour assurer des niveaux différents de restriction de filtrage selon les moments. Cette stratégie est utilisée dans le didacticiel de démarrage rapide pour les nouveaux utilisateurs dans la procédure de modification d'une stratégie et de son application aux clients.

Vous pouvez utiliser ces stratégies en l'état, les modifier en fonction des besoins de votre organisation ou créer vos propres stratégies.

La stratégie Par défaut

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 73
- *Fonctionnement des stratégies*, page 75
- *Ordre du filtrage*, page 80

Lorsque vous installez Websense, la stratégie **Par défaut** commence à surveiller l'utilisation Internet dès que vous saisissez votre clé d'abonnement. Au départ, la stratégie par défaut autorise toutes les demandes.

Remarque

Lorsque vous effectuez une mise à niveau à partir d'une version antérieure du logiciel Websense, les paramètres de stratégie existants sont préservés. Après la mise à niveau, vérifiez que vos stratégies sont toujours appropriées.

Au fur et à mesure que vous créez et que vous appliquez vos propres stratégies de filtrage, la stratégie Par défaut continue à jouer le rôle de filet de sécurité, en filtrant l'accès Internet des clients non régis par une autre stratégie.

Dans une nouvelle installation, la stratégie Par défaut doit assurer le filtrage Internet (appliquer une combinaison de filtres de catégories ou d'accès limité et, le cas échéant, de filtres de protocole) 24 heures sur 24, 7 jours sur 7.

Important

La stratégie par défaut de ces mises à niveau à partir d'une version antérieure de Websense peut ne pas couvrir toutes ces périodes. Vous n'êtes pas obligé(e) de modifier votre stratégie Par défaut. Si, toutefois, vous modifiez la stratégie ultérieurement, Websense ne vous permettra pas d'enregistrer les modifications tant que toutes les périodes ne seront pas couvertes.

Modifiez la stratégie Par défaut selon les besoins de votre organisation. La stratégie Par défaut ne peut pas être supprimée.

Fonctionnement des stratégies

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 73
- *Création d'une stratégie*
- *Modification d'une stratégie*
- *Filtres d'utilisation Internet*
- *Affinage des stratégies de filtrage*

La page **Gestion des stratégies > Stratégies** permet de vérifier les informations des stratégies existantes. Cette page sert également de point de départ pour ajouter, modifier et supprimer des stratégies, copier des stratégies vers des rôles d'administration déléguée (Super administrateurs uniquement) et imprimer des informations détaillées sur la configuration de vos stratégies.

La page Stratégies présente la liste des stratégies existantes. Cette liste comprend le nom et la description de chaque stratégie, de même que le nombre de clients utilisateur, réseau et ordinateur auxquels cette stratégie a été affectée.

- Pour ajouter une stratégie, cliquez sur **Ajouter**, puis consultez la section *Création d'une stratégie*, page 76 pour plus d'informations.
- Pour modifier une stratégie, cliquez sur son nom dans la liste, puis consultez la section *Modification d'une stratégie*, page 77 pour plus d'informations.
- Pour découvrir les clients filtrés par la stratégie, cliquez sur un nombre dans la colonne Utilisateurs, Réseaux ou Ordinateurs. Les informations sur les clients s'affichent dans une fenêtre contextuelle.

Pour imprimer la liste de toutes vos stratégies et de leurs composants, y compris les filtres, les catégories et protocoles personnalisés, les mots-clés, les URL personnalisées et les expressions régulières, cliquez sur **Imprimer les stratégies dans un fichier**. Cette fonction crée une feuille de calcul détaillée des informations de stratégies au format Microsoft Excel. Son objectif est de faciliter la revue des informations de stratégie de filtrage par les spécialistes des ressources humaines, les dirigeants et les autres autorités de surveillance.

Si vous avez créé des rôles d'administration déléguée (voir *Administration déléguée*, page 237), les Super administrateurs peuvent copier les stratégies qu'ils ont créées pour d'autres rôles afin que les administrateurs délégués les utilisent. Les filtres imposés par la stratégie sont également copiés.

> **Remarque**
> Comme les administrateurs délégués sont régis par le Verrouillage du filtre, les filtres et les stratégies Autoriser tout qui les imposent ne peuvent pas être copiés vers les rôles.

Pour copier des stratégies vers un autre rôle, cochez la case accolée au nom de la stratégie, puis cliquez sur **Copier dans le rôle**. Pour plus d'informations, consultez *Copie de filtres et de stratégies vers des rôles*, page 172.

Création d'une stratégie

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 73
- *Fonctionnement des stratégies*, page 75
- *Modification d'une stratégie*, page 77
- *Fonctionnement des filtres*, page 48
- *Restriction des utilisateurs à une liste définie de sites Internet*, page 168

La page **Gestion des stratégies > Stratégies > Ajouter une stratégie** permet de créer une nouvelle stratégie personnalisée.

1. Entrez un **Nom de stratégie** unique. Le nom doit être compris entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Les noms de stratégie peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez une **Description** de la stratégie. Pour simplifier la gestion des stratégies à long terme, leur description doit être claire et détaillée.

   Les restrictions de caractères qui s'appliquent aux noms de stratégie s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).
3. Pour utiliser une stratégie existante comme point de départ de la nouvelle stratégie, cochez la case **Baser sur une stratégie existante** et sélectionnez une stratégie dans la liste déroulante.

   Pour commencer avec une stratégie vide, ne cochez pas cette case.
4. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Modifier la stratégie.

   Utilisez la page Modifier la stratégie pour définir la nouvelle stratégie. Voir *Modification d'une stratégie*, page 77.

Modification d'une stratégie

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 73
- *Fonctionnement des stratégies*, page 75
- *Création d'une stratégie*, page 76
- *Fonctionnement des filtres*, page 48
- *Restriction des utilisateurs à une liste définie de sites Internet*, page 168

La page **Gestion des stratégies > Stratégies > Modifier la stratégie** permet de modifier une stratégie existante ou de terminer la définition d'une nouvelle stratégie.

Servez-vous de la partie supérieure de la page pour modifier le nom et la description de la stratégie :

- Cliquez sur **Renommer** pour modifier le nom de la stratégie.
- Entrez simplement votre texte dans le champ **Description** pour modifier la description du filtre.

Sous la description de la stratégie, le champ **Clients** indique le nombre de clients de chaque type (utilisateur, ordinateur et réseau) actuellement filtrés par cette stratégie. Pour découvrir les clients régis par la stratégie, cliquez sur le lien correspondant au type de client approprié.

Pour affecter cette stratégie à d'autres clients, cliquez sur **Appliquer aux clients** dans la barre d'outils située en haut de la page, puis consultez la section *Attribution d'une stratégie aux clients*, page 79.

Utilisez la section **Définition de stratégie** pour définir les filtres appliqués par cette stratégie aux différentes heures :

1. Pour ajouter une plage horaire dans le planning, cliquez sur **Ajouter**.
2. Utilisez les colonnes **Début** et **Fin** du tableau Planification pour définir la période couverte par cette plage horaire.

   Pour définir le filtrage pour une période dépassant minuit (par exemple de 17:00 à 08:00), ajoutez deux plages horaires au planning : l'une qui couvre la période allant de l'heure de début à minuit, l'autre de minuit à l'heure de fin.

   La stratégie **Exemple - Utilisateur standard**, incluse dans Websense, démontre la définition d'une période de filtrage dépassant minuit.
3. Utilisez la colonne **Jours** pour définir les jours de la semaine inclus dans cette plage horaire. Pour sélectionner des jours dans une liste, cliquez sur la flèche dirigée vers le bas dans la partie droite de la colonne. Lorsque la sélection des jours est terminée, cliquez sur la flèche dirigée vers le haut.
4. Utilisez la colonne **Filtre de catégories/d'accès limité** pour sélectionner un filtre à appliquer pendant cette plage horaire.

Pour ajouter un nouveau filtre à appliquer dans cette stratégie, sélectionnez **Ajouter un filtre de catégorie** ou **Ajouter un filtre d'accès limité**. Pour obtenir des instructions, consultez *Création d'un filtre de catégories*, page 49 ou *Création d'un filtre d'accès limité*, page 169.

5. Utilisez la colonne **Filtre de protocoles** pour sélectionner un filtre de protocoles à appliquer pendant cette plage horaire.

   Pour ajouter un nouveau filtre à appliquer dans cette stratégie, sélectionnez **Ajouter un filtre de protocoles**. Reportez-vous à la section *Création d'un filtre de protocoles*, page 51 pour obtenir des instructions.

6. Répétez les étapes 1 à 5 pour ajouter d'autres plages horaires au planning.

Lorsqu'une plage horaire est sélectionnée dans le planning, la partie inférieure de la page Modifier la stratégie présente les filtres appliqués pendant cette plage horaire. Chaque liste de filtres comprend :

- Le type de filtre (filtre de catégories, filtre d'accès limité ou filtre de protocoles)
- Le nom et la description du filtre
- Le contenu du filtre (catégories ou protocoles et les actions impliquées, ou la liste des sites autorisés)
- Le nombre de stratégies qui appliquent le filtre sélectionné
- Les boutons qui permettent de modifier le filtre

Lorsque vous modifiez un filtre dans cette page, les modifications apportées affectent toutes les stratégies qui appliquent ce filtre. Avant de modifier un filtre appliqué par plusieurs stratégies, cliquez sur le lien **Ce filtre est actif dans** pour découvrir quelles stratégies seront affectées.

Les boutons qui s'affichent au bas de la liste des filtres dépendent du type de filtre :

Type de filtre	Boutons
Filtre de catégories	• Servez-vous des boutons **Autoriser**, **Bloquer**, **Confirmer** ou **Contingent** pour modifier l'action appliquée aux catégories sélectionnées (voir *Actions de filtrage*, page 44). • Pour modifier l'action appliquée à une catégorie parente et à toutes ses sous-catégories, commencez par modifier l'action appliquée à la catégorie parente, puis cliquez sur **Appliquer aux sous-catégories**. • Pour activer le blocage des mots-clés, le blocage de types de fichiers ou le blocage en fonction de la bande passante, cliquez sur **Avancé**.

Type de filtre	Boutons
Filtre d'accès limité	• Utilisez le bouton **Ajouter des sites** et **Ajouter des expressions** pour ajouter des URL autorisées, des adresses IP ou des expressions régulières au filtre (voir *Restriction des utilisateurs à une liste définie de sites Internet*, page 168). • Pour supprimer un site du filtre, cochez la case accolée à l'URL, l'adresse IP ou l'expression, puis cliquez sur **Supprimer**.
Filtre de protocoles	• Servez-vous des boutons **Autoriser** ou **Bloquer** pour modifier l'action appliquée aux protocoles sélectionnés (voir *Actions de filtrage*, page 44). • Pour modifier l'action appliquée à tous les protocoles d'un groupe de protocoles, modifiez l'action appliquée à l'un des protocoles du groupe, puis cliquez sur **Appliquer au groupe**. • Pour journaliser les données du protocole sélectionné ou pour activer le blocage en fonction de la bande passante, cliquez sur **Avancé**.

Lorsque la modification d'une stratégie est terminée, cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Attribution d'une stratégie aux clients

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 73
- *Création d'une stratégie*, page 76
- *Modification d'une stratégie*, page 77
- *Clients*, page 59
- *Ajout d'un client*, page 68

La page **Stratégies > Modifier la stratégie > Appliquer une stratégie à des clients** permet d'affecter la stratégie sélectionnée à des clients.

La liste Clients répertorie tous les clients utilisateur, ordinateur et réseau disponibles, ainsi que la stratégie actuellement appliquée à chacun d'eux.

Cochez la case accolée à chaque client à filtrer par la stratégie sélectionnée, puis cliquez sur **OK** pour revenir à la page Modifier la stratégie. Cliquez de nouveau sur **OK** pour mettre en cache vos modifications.

Cliquez sur **Enregistrer tout** pour inviter Websense à commencer à utiliser la nouvelle stratégie pour filtrer les demandes des clients sélectionnés.

Ordre du filtrage

Websense utilise plusieurs filtres, appliqués dans un ordre spécifique, pour déterminer si les données Internet demandées sont autorisées, limitées, ou si elles doivent être bloquées.

Pour chaque demande reçue, Websense :

1. Vérifie la conformité de l'abonnement, en s'assurant que l'abonnement est actif et que le nombre de clients abonnés n'est pas dépassé.
2. Détermine la stratégie devant s'appliquer, en recherchant dans l'ordre suivant :
   a. Stratégie attribuée à **l'utilisateur**.
   b. Stratégie attribuée à **l'adresse IP** (ordinateur ou réseau) de l'ordinateur utilisé.
   c. Stratégies attribuées aux **groupes** dont est membre l'utilisateur.
   d. Stratégies attribuées au **domaine** de l'utilisateur.
   e. La stratégie **Par défaut**.

   La première stratégie applicable détectée est utilisée.
3. Filtre la demande en fonction des restrictions de la stratégie.

Il arrive parfois qu'un utilisateur appartienne à plusieurs groupes ou domaines et qu'aucune stratégie d'utilisateur, d'ordinateur ou de réseau ne s'applique. Dans ce cas, Websense vérifie les stratégies attribuées à chacun des groupes de l'utilisateur.

- Si tous les groupes ont la même stratégie, Websense filtre la requête en fonction de celle-ci.
- Si l'un des groupes est associé à une stratégie différente, Websense filtre la demande en fonction du paramètre **Utiliser un blocage plus restrictif** de la page **Paramètres > Filtrage**.

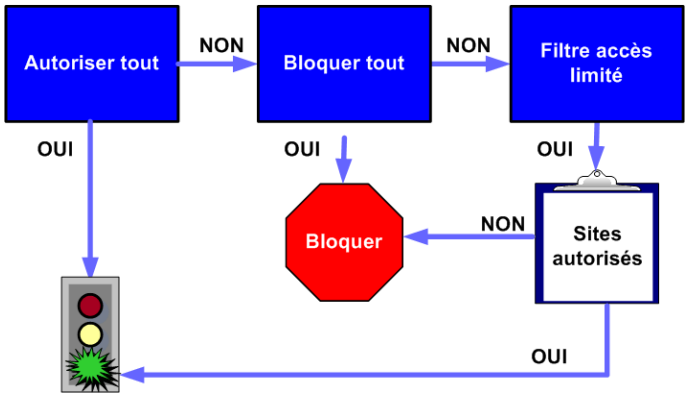
  Si l'option **Utiliser un blocage plus restrictif** est activée, et que l'une des stratégies applicables bloque l'accès à la catégorie demandée, Websense bloque le site.

  Si l'option n'est pas activée, et que l'une des stratégies applicables autorise l'accès à la catégorie demandée, Websense autorise le site.

Si l'une des stratégies applicables impose un filtre d'accès limité, l'option **Utiliser un blocage plus restrictif** peut avoir un effet imprévu. Voir *Filtres d'accès limité et priorités du filtrage*, page 168.

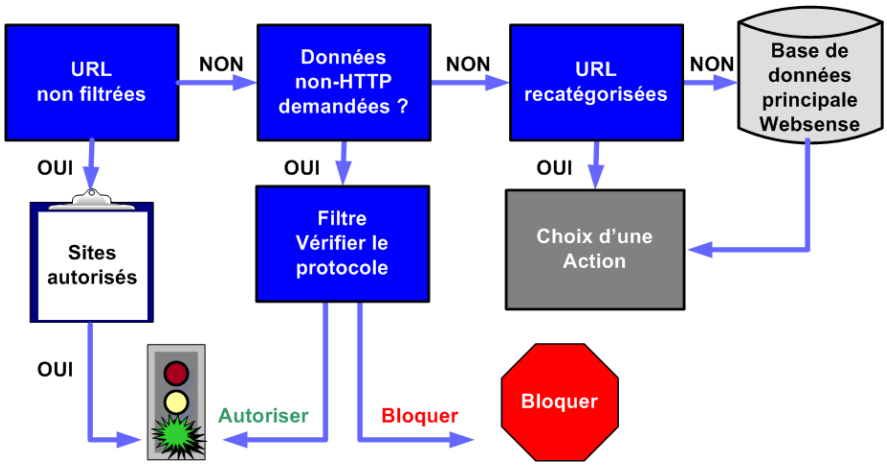
Filtrage d'un site

Websense évalue les restrictions de stratégie comme suit pour déterminer si le site demandé doit être autorisé ou bloqué.

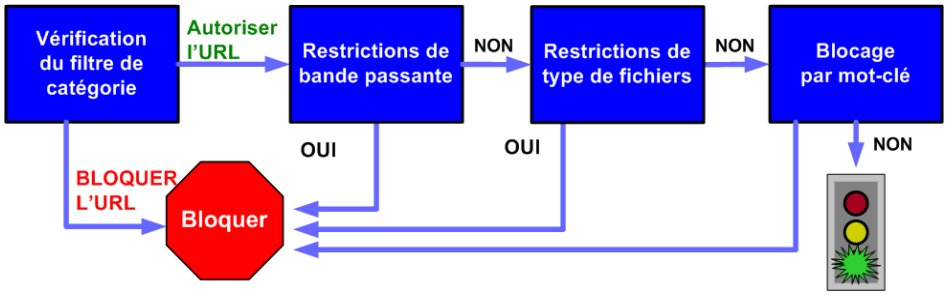


1. Il détermine le **filtre de catégories** ou le **filtre d'accès limité** appliqué par la stratégie pour le jour et la date en cours.
   - Si le filtre de catégories actif est **Autoriser tout**, il autorise le site.
   - Si le filtre de catégories actif est **Bloquer tout**, il bloque le site.
   - Si le filtre est **d'accès limité**, il vérifie si le filtre contient l'URL ou l'adresse IP. Dans l'affirmative, il autorise le site. Dans le cas contraire, il bloque le site.
   - Si un autre filtre de catégories s'applique, il passe à l'étape 2.

> **Remarque**
> Websense filtre les URL consultées à partir d'un cache de moteur de recherche Internet comme toute autre URL. Les URL stockées de cette manière sont filtrées en fonction des stratégies actives pour leurs catégories d'URL. Les enregistrements de journal des URL mises en cache présentent l'URL complète mise en cache, avec les paramètres du moteur de recherche.



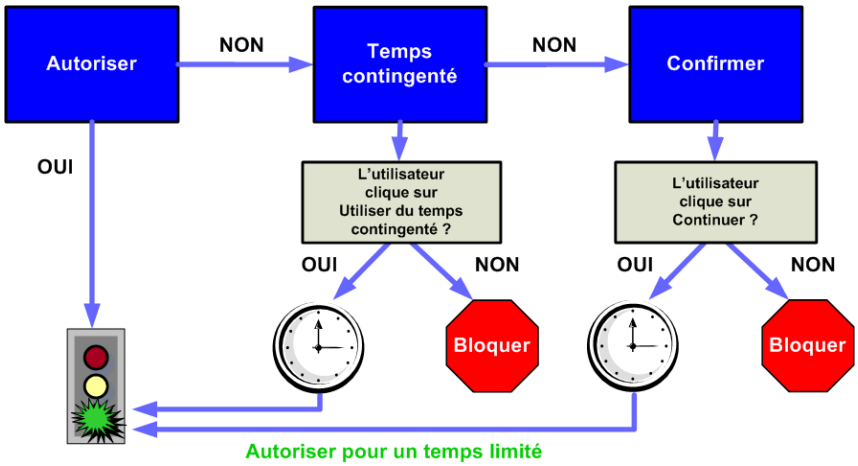
2. Il tente d'associer le site à une entrée de la liste **URL non filtrées**.
   - Si l'URL apparaît dans la liste, il autorise le site.
   - Si l'URL n'est pas dans la liste, il passe à l'étape 3.
3. Il vérifie le **filtre de protocoles** actif et détermine si des protocoles non HTTP sont associés à la demande.
   - Dans l'affirmative, il applique les paramètres de filtrage de protocole aux données pouvant être transmises.
   - Sinon, il passe à l'étape 4.
4. Il tente d'associer le site à une entrée de la liste **URL recatégorisées**.
   - S'il trouve une correspondance, il identifie la catégorie du site et passe à l'étape 6.
   - S'il ne peut pas établir de correspondance, il passe à l'étape 5.
5. Il tente d'associer le site à une entrée de la **Base de données principale**.
   - Si l'URL apparaît dans la Base de données principale, il identifie la catégorie du site et passe à l'étape 6.
   - S'il ne peut pas établir de correspondance, il classe le site dans la catégorie Divers/Non catégorisées et passe à l'étape 6.



6. Il vérifie le filtre de catégories d'URL actif et identifie l'action appliquée à la catégorie contenant le site demandé.
   - Si l'action est **Bloquer**, il bloque le site.
   - Si une autre action s'applique, il passe à l'étape 7.
7. Il vérifie les paramètres de **Bandwidth Optimizer** dans le filtre de catégories actif (voir *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191).
   - Si l'utilisation de la bande passante en cours dépasse les limites configurées, il bloque le site.
   - Si l'utilisation de la bande passante en cours ne dépasse pas les limites spécifiées, ou si aucune action basée sur la bande passante ne s'applique, il passe à l'étape 8.
8. Il recherche les restrictions de **type de fichier** appliquées à la catégorie d'URL active (voir *Gestion du trafic en fonction du type de fichiers*, page 193).
   - Si le site contient des fichiers dont les extensions sont bloquées, il bloque l'accès à ces fichiers. Si le site lui-même contient un type de fichier bloqué, il bloque l'accès au site.

- Si le site ne contient pas de fichiers dont les extensions sont bloquées, il passe à l'étape 9.

9. Il recherche des **mots-clés** dans l'URL et le chemin CGI, si le blocage des mots-clés est activé (voir *Filtrage par mots-clés*, page 180).
   - S'il trouve un mot clé bloqué, il bloque le site.
   - S'il ne trouve pas de mot clé bloqué, il passe à l'étape 10.



10. Il gère le site en fonction des actions appliquées à la catégorie.
    - **Autoriser** : il autorise le site.
    - **Limiter par quota** : il affiche le message de blocage avec la possibilité de consulter le site à l'aide du temps contingenté ou de revenir à la page précédente.
    - **Confirmer** : il affiche le message de blocage avec une possibilité d'afficher le site pour des raisons professionnelles.

Websense continue ainsi jusqu'à ce que le site demandé soit bloqué ou explicitement autorisé. À ce stade, Websense ne tente pas d'autres actions de filtrage. Par exemple, si le site demandé appartient à une catégorie bloquée et contient un mot-clé bloqué, Websense bloque le site au niveau de la catégorie sans vérifier le filtre du mot-clé. Log Server enregistre alors la demande en tant que bloquée du fait de la catégorie bloquée, pas du fait d'un mot-clé.

Remarque

Les utilisateurs qui disposent de droits d'accès par mot de passe peuvent accéder aux sites Internet, quelle que soit la raison pour laquelle le site a été bloqué.

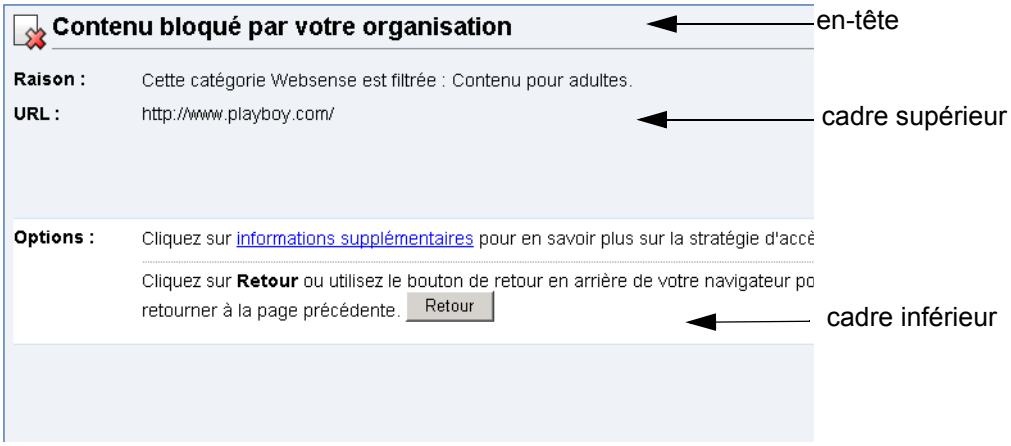
5 Pages de blocage

Rubriques connexes :

- *Messages de blocage de protocole*, page 86
- *Fonctionnement des pages de blocage*, page 87
- *Création d'autres messages de blocage*, page 92
- *Utilisation d'une autre page de blocage sur un autre ordinateur*, page 92

Lorsque Websense bloque un site Web, il affiche une page de blocage dans le navigateur du client. Si le site est bloqué parce qu'il appartient à une catégorie de la classe Risque pour la sécurité (voir *Classes de risque*, page 41), une version spéciale de la page de blocage s'affiche.

Par défaut, une page de blocage comprend 3 sections principales.



- L'**en-tête** explique que le site est bloqué.
- Le **cadre supérieur** contient le message de blocage, l'URL demandée et la raison du blocage.
- Le **cadre inférieur** présente les options proposées à l'utilisateur, par exemple la possibilité de revenir à la page précédente, ou de cliquer sur un bouton Continuer ou Utiliser du temps contingenté pour consulter le site.

Les pages de blocage sont conçues à partir de fichiers HTML. Des fichiers de pages de blocage par défaut sont inclus dans Websense. Vous pouvez utiliser ces fichiers par défaut ou créer vos propres versions personnalisées.

- Personnalisez les fichiers par défaut pour modifier le message de blocage (voir *Fonctionnement des pages de blocage*, page 87).
- Configurez Websense pour qu'il utilise des messages de blocage (par défaut ou personnalisés) hébergés sur un serveur Web distant (voir *Utilisation d'une autre page de blocage sur un autre ordinateur*, page 92).

Messages de blocage de protocole

Rubriques connexes :

- *Fonctionnement des pages de blocage*, page 87
- *Création d'autres messages de blocage*, page 92
- *Utilisation d'une autre page de blocage sur un autre ordinateur*, page 92

Lorsqu'un utilisateur ou une application demande un protocole non HTTP bloqué, Websense affiche généralement un message de blocage de protocole.

Toutefois, lorsqu'un utilisateur demande un site FTP, HTTPS ou Gopher bloqué à partir d'un navigateur, et que la requête passe par un proxy, une page de blocage de type HTML apparaît à la place dans le navigateur.

Si une application demande le protocole bloqué, l'utilisateur peut également recevoir un message d'erreur de l'application, indiquant qu'elle ne peut pas s'exécuter. Les messages d'erreur des applications ne sont pas générés par Websense.

Une certaine configuration du système peut être requise pour afficher les messages de blocage de protocole sur les ordinateurs Windows :

- Pour afficher des messages de blocage de protocoles sur les ordinateurs client fonctionnant sous Windows NT, XP ou 200x, le service Windows Messenger doit être activé. Ce service est désactivé par défaut. Vous pouvez vérifier dans la boîte de dialogue Services de Windows de l'ordinateur client, si le service Messenger s'exécute (voir *Boîte de dialogue Services de Windows*, page 399).
- Pour afficher des messages de blocage de protocoles sur un ordinateur Windows 98, lancez **winpopup.exe**, situé dans le répertoire Windows. Exécutez cette application depuis une invite de commande ou configurez-la pour qu'elle s'exécute automatiquement en la copiant dans le dossier Démarrage.

Les messages de blocage de protocoles ne s'affichent pas sur les ordinateurs Linux. Les pages de blocage HTML s'affichent quel que soit le système d'exploitation.

Si le filtrage de protocoles est activé, Websense filtre les demandes de protocole, que les messages de blocage de protocole soient ou non configurés pour s'afficher sur les ordinateurs client.

Fonctionnement des pages de blocage

Rubriques connexes :

- *Messages de blocage de protocole*, page 86
- *Personnalisation du message de blocage*, page 88
- *Création d'autres messages de blocage*, page 92
- *Utilisation d'une autre page de blocage sur un autre ordinateur*, page 92

Les fichiers utilisés pour créer les pages de blocage Websense sont stockés dans le répertoire **Websense\BlockPages\en\Default** :

- **master.html** construit le cadre d'information de la page de blocage et utilise l'un des fichiers suivants pour afficher les options appropriées dans le cadre inférieur.

Nom du fichier	Contenu
blockFrame.html	Texte et bouton (option Retour) des sites appartenant aux catégories bloquées
continueFrame.html	Texte et boutons des sites appartenant aux catégories auxquelles l'action **Confirmer** est appliquée
quotaFrame.html	Texte et boutons des sites appartenant aux catégories auxquelles l'action **Contingent** est appliquée
moreInfo.html	Contenu de la page qui apparaît lorsqu'un utilisateur clique sur le lien **Plus d'informations** de la page de blocage.

- **block.html** contient le texte du cadre supérieur du message de blocage, expliquant que l'accès est limité, énumérant le site demandé et donnant la raison de la restriction.

Personnalisation du message de blocage

Rubriques connexes :

- *Modification de la taille du cadre du message*, page 89
- *Modification du logo affiché sur la plage de blocage*, page 89
- *Utilisation des variables du contenu de la page de blocage*, page 90
- *Réinitialisation des pages de blocage par défaut*, page 91

Vous pouvez faire une copie des fichiers de la page de blocage par défaut, puis utiliser la copie pour personnaliser le cadre supérieur de la page de blocage présentée aux utilisateurs.

- Ajoutez des informations sur les stratégies d'utilisation d'Internet dans votre organisation.
- Fournissez un moyen de contacter les Ressources humaines ou un administrateur Websense à propos des stratégies d'utilisation Internet.

1. Naviguez jusqu'au répertoire des pages de blocage de Websense :

   `<chemin du répertoire d'installation>\BlockPages\en\Default`

2. Copiez les fichiers de la page de blocage dans le répertoire des pages de blocage personnalisées :

   `<chemin du répertoire d'installation>\BlockPages\en\Custom`

   Remarque

   Ne modifiez **pas** les fichiers des messages de blocage originaux situés dans le répertoire **BlockPages\en\Default**. Copiez-les dans le répertoire **BlockPages\en\Custom**, puis modifiez leurs copies.

3. Ouvrez le fichier dans un éditeur de texte, tel que Notepad ou vi.

   Avertissement

   Pour modifier les fichiers des messages de blocage, servez-vous d'un éditeur de texte brut. Certains éditeurs HTML modifient le code HTML, ce qui peut corrompre les fichiers et entraîner des problèmes d'affichage des messages de blocage.

4. Modifiez le texte. Les fichiers contiennent des commentaires qui vous guident pendant vos modifications.

   Ne modifiez **pas** les jetons (entourés par les symboles $* et *$), ni la structure du code HTML. Ces derniers permettent à Websense d'afficher des informations spécifiques dans le message de blocage.

5. Enregistrez le fichier.

6. Redémarrez Filtering Service (voir *Arrêt et démarrage des services Websense*, page 286 pour plus d'instructions).

Modification de la taille du cadre du message

Selon les informations que vous souhaitez afficher dans le message de blocage, il est possible que la largeur du message de blocage et la hauteur du cadre supérieur ne soient pas appropriées. Pour modifier ces paramètres de taille dans le fichier **master.html** :

1. Copiez le fichier **master.html** du répertoire **Websense\BlockPages\en\Default** vers **Websense\BlockPages\en\Custom**.
2. Ouvrez le fichier dans un éditeur de texte, tel que Notepad ou vi (pas dans un éditeur HTML).
3. Pour modifier la largeur du cadre du message, modifiez la ligne suivante :

   ```
   <div style="border: 1px solid #285EA6;width: 600px...">
   ```

   Modifiez la valeur du paramètre **width** selon vos besoins.
4. Pour qu'il soit possible de faire défiler le cadre supérieur du message afin d'afficher des informations supplémentaires, modifiez la ligne suivante :

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
   scrolling="no" style="width:100%; height: 6em;">
   ```

   Définissez la valeur du paramètre **scrolling** sur **auto** pour qu'une barre de défilement s'affiche lorsque le texte du message dépasse la hauteur du cadre.

   Vous pouvez également modifier la valeur du paramètre **height** pour modifier la hauteur du cadre.
5. Enregistrez et fermez le fichier.
6. Redémarrez Filtering Service pour implémenter les modifications (voir *Arrêt et démarrage des services Websense*, page 286).

Modification du logo affiché sur la plage de blocage

Le fichier **master.html** comprend également le code HTML utilisé pour afficher un logo Websense sur la page de blocage. Pour remplacer ce logo par celui de votre organisation :

1. Copiez les fichiers de la page de blocage du répertoire **Websense\BlockPages\en\Default** dans **Websense\BlockPages\en\Custom**, si cela n'est pas déjà fait.
2. Copiez un fichier image contenant le logo de votre organisation au même emplacement.
3. Ouvrez **master.html** dans un éditeur de texte, par exemple Notepad ou vi (pas un éditeur HTML), puis modifiez la ligne suivante pour remplacer le logo Websense par celui de votre organisation :

   ```
   <img title="Websense" src="/en/Custom/wslogo_block_page.png"
   ...>
   ```

- Remplacez **wslogo_block_page.png** par le nom du fichier image contenant le logo de votre organisation.
- Remplacez les valeurs du paramètre **title** par le nom de votre organisation.

4. Enregistrez et fermez le fichier.
5. Redémarrez Filtering Service pour implémenter les modifications (voir *Arrêt et démarrage des services Websense*, page 286).

Utilisation des variables du contenu de la page de blocage

Les variables du contenu contrôlent les informations apparaissant dans les pages de blocage HTML. Les variables suivantes sont incluses dans le code des messages de blocage par défaut.

Nom de la variable	Contenu affiché
WS_DATE	Date en cours
WS_USERNAME	Nom d'utilisateur en cours (sans le nom de domaine)
WS_USERDOMAIN	Nom de domaine de l'utilisateur en cours
WS_IPADDR	Adresse IP de l'ordinateur à l'origine de la requête
WS_WORKSTATION	Nom de l'ordinateur bloqué (si le nom n'est pas disponible, son adresse IP apparaît)

Pour utiliser une variable, insérez son nom entre les symboles $* *$ dans la balise HTML appropriée :

```
<p id="NomUtilisateur">$*WS_USERNAME*$</p>
```

Ici, *WS_USERNAME* représente la variable.

Le code des messages de blocage contient d'autres variables, présentées ci-après. Certaines d'entre elles se révéleront peut-être très utiles pour la conception de vos propres messages de blocage personnalisés. Toutefois, lorsque ces variables apparaissent dans les fichiers des messages de blocage définis par Websense, ne les modifiez **pas**. Comme Filtering Service utilise ces variables pour traiter les requêtes bloquées, elles doivent rester en place.

Nom de la variable	Objectif
WS_URL	Affiche l'URL demandée
WS_BLOCKREASON	Affiche la raison pour laquelle le site a été bloqué (c'est-à-dire l'action de filtrage appliquée)
WS_ISSECURITY	Indique si le site demandé appartient à l'une des catégories par défaut de la classe Risque pour la sécurité. Si TRUE, la page de blocage de sécurité est affichée.
WS_PWOVERRIDECGIDATA	Renseigne un champ de saisie du code HTML de la page de blocage avec les informations relatives à l'utilisation du bouton **Accès par mot de passe**.

Nom de la variable	Objectif
WS_QUOTA_CGIDATA	Renseigne un champ de saisie du code HTML de la page de blocage avec les informations relatives à l'utilisation du bouton **Utiliser du temps contingenté**.
WS_PASSWORDOVERRID_BEGIN, WS_PASSWORDOVERRID_END	Impliqué dans l'activation de la fonction d'accès par mot de passe
WS_MOREINFO	Présente des informations détaillées (apparaissant lorsque l'utilisateur clique sur le lien **Plus d'informations**) sur le motif de blocage du site
WS_POLICYINFO	Indique la stratégie surveillant le client à l'origine de la demande
WS_MOREINFOCGIDATA	Envoie des données au service Filtering Service sur l'utilisation du lien **Plus d'informations**
WS_QUOTATIME	Présente la quantité de temps contingenté restant pour le client à l'origine de la demande
WS_QUOTAINTERVALTIME	Présente la longueur de la session de temps contingenté configurée pour le client à l'origine de la demande
WS_QUOTABUTTONSTATE	Indique si le bouton **Utiliser du temps contingenté** est activé ou désactivé pour une demande particulière
WS_SESSIONID	Joue le rôle d'identifiant interne associée à une requête
WS_TOPFRAMESIZE	Indique la taille (sous forme de pourcentage) de la partie supérieure d'une page de blocage envoyée par un serveur de blocage personnalisé, lorsqu'un tel serveur est configuré
WS_BLOCKMESSAGE_PAGE	Indique la source à utiliser pour le cadre supérieur d'une page de blocage
WS_CATEGORY	Présente la catégorie de l'URL bloquée
WS_CATEGORYID	Identifiant unique de la catégorie de l'URL demandée

Réinitialisation des pages de blocage par défaut

Si des utilisateurs signalent des erreurs après l'implémentation de messages de blocage personnalisés, vous pouvez restaurer les messages de blocage par défaut en procédant comme suit :

1. Supprimez tous les fichiers du répertoire **Websense\BlockPages\en\Custom**. Par défaut, Websense réutilisera les fichiers du répertoire Default.
2. Redémarrez Filtering Service (voir *Arrêt et démarrage des services Websense*, page 286).

Création d'autres messages de blocage

Rubriques connexes :

- *Fonctionnement des pages de blocage*, page 87
- *Personnalisation du message de blocage*, page 88

Vous pouvez également créer vos propres fichiers HTML contenant le texte à afficher dans la partie supérieure de la page de blocage. Servez-vous des fichiers HTML existants, créez entièrement d'autres fichiers, ou faites des copies du fichier **block.html** pour l'utiliser comme modèle.

- Créez des messages de blocage distincts pour chacun des trois protocoles : HTTP, FTP et Gopher.
- Placez les fichiers sur l'ordinateur Websense, ou sur votre serveur Web interne (voir *Utilisation d'une autre page de blocage sur un autre ordinateur*, page 92).

Après avoir créé d'autres fichiers de message de blocage, vous devez configurer Websense pour qu'il affiche ces nouveaux messages (voir *Configuration des paramètres de filtrage de Websense*, page 56). Cette procédure vous permet de définir le message utilisé pour chacun des protocoles configurables.

Utilisation d'une autre page de blocage sur un autre ordinateur

Rubriques connexes :

- *Fonctionnement des pages de blocage*, page 87
- *Personnalisation du message de blocage*, page 88
- *Création d'autres messages de blocage*, page 92

Au lieu d'utiliser les pages de blocage Websense et de personnaliser simplement le message du cadre supérieur, vous pouvez créer vos propres pages de blocage HTML et les héberger sur un serveur Web interne.

Remarque

Les pages de blocage peuvent également être stockées sur un serveur Web externe. Toutefois, si ce serveur héberge un site répertorié dans la Base de données principale et appartenant à une catégorie bloquée, la page de blocage est elle-même bloquée.

Certaines organisations utilisent d'autres pages de blocage distantes pour masquer l'identité du serveur Websense.

La page de blocage distante peut être un fichier HTML et ne doit pas nécessairement reproduire le format des pages de blocage Websense par défaut. Toutefois, l'utilisation de cette méthode pour créer des pages de blocage vous empêche d'utiliser les fonctions Continuer, Utiliser du temps contingenté et Accès par mot de passe disponibles avec les pages de blocage définies par Websense (par défaut ou personnalisées).

Lorsque les fichiers sont en place, modifiez le fichier **eimserver.ini** pour qu'il pointe vers la nouvelle page de blocage.

1. Arrêtez les services Websense Filtering Service et Policy Server, dans cet ordre (voir *Arrêt et démarrage des services Websense*, page 286).
2. Sur l'ordinateur Filtering Service, localisez le répertoire Websense **bin** (par défaut, \Program Files\Websense\bin ou /opt/websense/bin).
3. Créez une copie de sauvegarde du fichier **eimserver.ini** et stockez-la dans un autre répertoire.
4. Ouvrez le fichier **eimserver.ini** dans un éditeur de texte, puis localisez la section **[WebsenseServer]** (en haut du fichier).
5. Entrez le nom d'hôte ou l'adresse IP du serveur hébergeant la page de blocage dans le format suivant :

   ```
   UserDefinedBlockPage=http://<nom d'hôte ou adresse IP>
   ```

   La partie du protocole de l'URL (http://) est obligatoire.
6. Enregistrez le fichier et fermez l'éditeur de texte.
7. Redémarrez les services Websense Filtering Service et Policy Server, dans cet ordre.

Après le démarrage des services, les utilisateurs reçoivent la page de blocage hébergée sur l'autre ordinateur.

6 Utilisation des rapports pour évaluer l'efficacité des stratégies de filtrage

Rubriques connexes :

- *Présentation de la génération de rapports*, page 96
- *Rapports de présentation*, page 98
- *Rapports d'investigation*, page 118
- *Rapports sur activité propre*, page 144

Websense Manager peut fournir plusieurs outils de génération de rapports à utiliser pour évaluer l'efficacité des stratégies de filtrage. (Websense Manager et les composants de génération de rapports Websense doivent être installés sur les serveurs Windows.)

- La page **Aujourd'hui** s'affiche lorsque vous ouvrez Websense Manager. Elle présente l'état de fonctionnement de Websense et peut afficher des graphiques sur les activités de filtrage du réseau depuis minuit. (Voir *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22.)
- La page **Historique** présente des graphiques sur les activités de filtrage du réseau allant jusqu'aux 30 derniers jours, selon la quantité d'informations disponibles dans la Base de données d'activité. Ces graphiques ne comprennent pas les activités du jour. (Voir *Historique : 30 derniers jours*, page 25.)
- Les rapports de **présentation** et **d'investigation** offrent de nombreuses options qui permettent de générer, de personnaliser et de planifier les rapports. Pour plus d'informations, consultez *Présentation de la génération de rapports*, page 96.

Si votre organisation a installé Websense Manager sur un serveur Linux, ou choisi le programme de création de rapports Websense Explorer pour Linux à la place des composants de création de rapport fonctionnant sous Windows, les options de création de rapports ne s'affichent pas dans Websense Manager. Aucun graphique de filtrage Internet ne s'affiche dans les pages Aujourd'hui et Historique. Reportez-vous au *Guide d'administration d'Explorer pour Linux* pour plus d'informations sur l'installation de ce programme et l'exécution des rapports.

Présentation de la génération de rapports

Rubriques connexes :

- *Utilisation des rapports pour évaluer l'efficacité des stratégies de filtrage*, page 95
- *Rapports de présentation*, page 98
- *Rapports d'investigation*, page 118
- *Rapports sur activité propre*, page 144

Outre les graphiques des pages Aujourd'hui et Historique, Websense offre 2 options de génération de rapports : les rapports de présentation et les rapports d'investigation.

Remarque

Lorsque l'organisation utilise l'administration déléguée, il est possible que certains administrateurs n'aient pas accès à toutes les fonctions de génération de rapports. Voir *Administration déléguée*, page 237.

Les **rapports de présentation** présentent la liste des définitions de rapport. Certains rapports se présentent sous forme de tableaux, d'autres combinent un graphique à barres et un tableau. Pour générer un rapport de présentation :

1. Sélectionnez un rapport dans la liste.
2. Cliquez sur **Exécuter**.
3. Sélectionnez la plage de dates.
4. Cliquez sur **Exécuter maintenant**.

En plus de générer les graphiques prédéfinis, vous pouvez les copier et appliquer un filtre de rapport personnalisé identifiant des clients spécifiques, des catégories, des protocoles ou des actions à inclure. Enregistrez les définitions de rapport utilisées le plus fréquemment sous forme de Favoris pour les retrouver plus facilement.

Vous pouvez planifier l'exécution d'un rapport de présentation à un moment spécifique ou pour un cycle récurrent. Pour des informations complètes, consultez la section *Rapports de présentation*, page 98.

Les **rapports d'investigation** vous permettent de parcourir le contenu de la journalisation de façon interactive. La page principale présente un graphique à barres qui résume l'activité par classe de risques. Cliquez sur les différents éléments de la page pour actualiser le graphique ou obtenir une vue différente des données.

- Cliquez sur le nom de la classe de risque, puis sélectionnez un niveau de détails plus fin. Par exemple, vous pouvez afficher l'activité par utilisateur pour la classe de risque Responsabilité légale engagée.

- Cliquez sur un nom d'utilisateur dans le graphique résultant pour afficher davantage de détails sur cet utilisateur.
- Choisissez une autre option dans la liste **Utilisation d'Internet par** pour modifier le graphique à barres résumé.
- Renseignez les champs situés juste au-dessus du graphique à barres pour afficher simultanément deux niveaux d'informations. Par exemple, à partir d'un graphique résumé des catégories, vous pouvez sélectionner **10**, **Utilisateur** et **5** pour afficher l'activité des 5 premiers utilisateurs situés dans les 10 premières catégories.
- Cliquez sur une barre ou sur un numéro pour ouvrir un rapport détaillé pour cet élément (classe de risque, catégorie, utilisateur ou autre).
- Cliquez sur **Rapports favoris** pour enregistrer un format de rapport particulièrement utile en vue d'une utilisation ultérieure ou pour générer un Favori enregistré précédemment.

Les possibilités offertes sont quasiment infinies. Consultez la section *Rapports d'investigation*, page 118 pour plus d'informations sur les nombreuses manières d'afficher les données d'utilisation Internet.

Temps de navigation sur Internet

Rubriques connexes :

- *Travaux de base de données*, page 322
- *Configuration des options du temps de navigation sur Internet*, page 328

Vous pouvez générer des rapports de présentation et d'investigation en fonction du temps de navigation sur Internet (IBT), temps passé par un individu à naviguer sur des sites Internet. Aucun logiciel ne peut vous dire avec précision combien de temps un individu consulte réellement un site spécifique une fois que ce dernier est ouvert. L'utilisateur peut ouvrir un site, l'afficher quelques secondes, puis répondre à un appel téléphonique professionnel avant de demander un autre site. L'utilisateur peut également lire chaque site pendant quelques minutes avant de passer au suivant.

Websense comprend une tâche Log Database qui permet de calculer le temps de navigation sur Internet, à l'aide d'une formule basée sur certaines valeurs configurables. Cette tâche s'exécutant une fois par jour, certaines informations relatives au temps de navigation peuvent ne pas figurer dans les données de journalisation réelles.

Pour les calculs du temps de navigation, la session Internet commence lorsque l'utilisateur ouvre un navigateur. Elle se poursuit tant que l'utilisateur demande d'autres pages Internet au moins toutes les 3 minutes. (Le seuil de temps de lecture par défaut est configurable.)

La session Internet se termine lorsque plus de 3 minutes se sont écoulées sans que l'utilisateur ne demande un autre site. Websense calcule le temps total de la session, à

partir de l'heure de la première requête jusqu'à ce que 3 minutes se soient écoulées après la dernière.

Une nouvelle session commence si l'utilisateur demande d'autres sites après plus de 3 minutes. En général, le temps de navigation d'un utilisateur se compose de plusieurs sessions quotidiennes.

Consultez les sections *Travaux de base de données*, page 322 et *Configuration des options du temps de navigation sur Internet*, page 328 pour plus d'informations sur la tâche Temps de navigation Internet et ses options de configuration.

Rapports de présentation

Rubriques connexes :

- *Copie d'un rapport de présentation*, page 101
- *Copie d'un rapport de présentation*, page 101
- *Fonctionnement des favoris*, page 108
- *Exécution des rapports de présentation*, page 109
- *Planification des rapports de présentation*, page 110
- *Affichage de la liste des tâches planifiées*, page 115

La page **Génération de rapports > Rapports de présentation** énumère la liste des graphiques prédéfinis et des rapports tabulaires, illustrant chacun des informations spécifiques issues de la Base de données d'activité Log Database (voir *Présentation de la base de données d'activité*, page 321). Sélectionnez un rapport dans ce Catalogue de rapports pour afficher une brève description.

Vous pouvez copier un rapport prédéfini et personnaliser le filtre du rapport, en indiquant les clients, les catégories, les protocoles et les actions à y inclure. Les rapports fréquemment utilisés sont marqués comme Favoris pour vous aider à les retrouver plus rapidement.

Exécutez le rapport choisi immédiatement ou planifiez l'exécution des rapports sélectionnés à un moment ultérieur ou de façon périodique. Choisissez le format de sortie et diffusez les rapports planifiés vers un groupe sélectionné de destinataires.

Si vous générez un rapport directement à partir de la page Rapports de présentation au format HTML, le rapport n'est pas enregistré lorsque vous passez à une autre page. Si vous générez et affichez immédiatement un rapport au format PDF ou XLS, le rapport n'est pas enregistré lorsque vous fermez le programme associé (Adobe Reader ou Microsoft Excel).

Vous pouvez également choisir d'enregistrer le fichier PDF ou XLS au lieu de l'afficher immédiatement, ou utiliser l'option Enregistrer du programme associé. Dans ce cas, n'oubliez pas de supprimer ou de déplacer régulièrement les fichiers de rapport pour éviter les problèmes d'espace disque.

Les rapports planifiés sont automatiquement enregistrés dans le répertoire suivant :

```
<chemin_installation>\ReportingOutput
```

Le chemin d'installation par défaut est C:\Program Files\Websense.

Après l'exécution d'un rapport de présentation planifié, le fichier du rapport est envoyé aux destinataires sous forme de pièce jointe de messagerie électronique appelée **presentationreport_0**. Le nombre est incrémenté en fonction du nombre de rapports joints. Notez que le nom de la pièce jointe ne correspond pas à celui du fichier stocké dans le répertoire ReportingOutput. Pour localiser un rapport spécifique dans ce répertoire, recherchez les fichiers créés le jour de l'exécution du travail planifié.

Les rapports sont automatiquement supprimés du répertoire ReportingOutput au bout de 15 jours. Si vous souhaitez conserver les rapports plus longtemps, incluez-les dans votre routine de sauvegarde ou planifiez-les et enregistrez les fichiers envoyés par email dans un emplacement autorisant le stockage à long terme.

Selon le nombre de rapports générés chaque jour, leurs fichiers peuvent occuper une quantité considérable d'espace disque. Assurez-vous que l'ordinateur Websense Manager dispose de suffisamment d'espace disque. Si la taille du répertoire ReportingOutput devient trop importante avant la suppression automatique des fichiers, vous pouvez supprimer ces derniers manuellement.

Websense génère le rapport au format choisi : PDF (Adobe Reader), XLS (Microsoft Excel) ou HTML. Si vous choisissez le format HTML, le rapport s'affiche dans le panneau de contenu de Websense Manager. Ces rapports ne peuvent pas être imprimés ou enregistrés dans un fichier. Pour imprimer ou enregistrer un rapport dans un fichier, choisissez le format PDF ou XLS.

Si vous choisissez un format PDF ou XLS , vous avez la possibilité d'enregistrer le fichier du rapport sur disque ou de l'afficher dans une fenêtre distincte.

Important

Pour pouvoir afficher les rapports de présentation au format PDF, Adobe Reader v7.0 ou version ultérieure doit être installé sur l'ordinateur à partir duquel vous accédez à Websense Manager.

Pour pouvoir afficher les rapports de présentation au format XLS, Microsoft Excel 2003 ou version ultérieure doit être installé sur l'ordinateur à partir duquel vous accédez à Websense Manager.

Dans la page Rapports de présentation, parcourez le Catalogue de rapports et sélectionnez celui qui vous intéresse. Utilisez ensuite les contrôles de la page pour exécuter le rapport, créer une copie pour personnaliser le filtre de rapport, etc.

Bouton	Action
Afficher uniquement les favoris	Sélectionnez cette option pour que le Catalogue de rapports n'affiche que les rapports marqués comme Favoris. Désactivez cette option pour restaurer la liste complète des rapports.
Modifier le filtre du rapport	Cette option est uniquement disponible lorsqu'une copie d'un rapport prédéfini est sélectionnée. Elle vous permet de sélectionner des catégories, des protocoles, des utilisateurs et des actions spécifiques à inclure dans le rapport. Voir *Copie d'un rapport de présentation*, page 101.
Copier	Crée une copie du rapport sélectionné et l'ajoute dans le Catalogue de rapports en tant que rapport personnalisé. Voir *Copie d'un rapport de présentation*, page 101. Sélectionnez le rapport personnalisé, puis définissez ses paramètres spécifiques en cliquant sur **Modifier le filtre du rapport**.
Favori	Marque le rapport sélectionné en tant que Favori, ou retire la désignation Favori. Voir *Fonctionnement des favoris*, page 108. Dans le Catalogue de rapports, un symbole en forme d'étoile s'affiche à côté du nom des rapports désignés comme Favoris. Servez-vous de la case à cocher **Afficher uniquement les favoris** pour contrôler les rapports devant s'afficher dans le Catalogue de rapports.
Supprimer	Supprime la copie du rapport sélectionné du Catalogue de rapports. Les rapports prédéfinis installés avec le logiciel ne peuvent pas être supprimés. Si les rapports supprimés apparaissent dans des travaux planifiés, ils continuent à être générés avec ces tâches.
Exécuter	Génère le rapport sélectionné lorsque la plage de date et le format de sortie ont été définis. Voir *Exécution des rapports de présentation*, page 109. Pour contrôler les autres aspects de rapports personnalisés (copie d'un rapport prédéfini), consultez la section *Copie d'un rapport de présentation*, page 101. Pour planifier l'exécution d'un rapport de présentation à un autre moment ou de façon périodique, cliquez sur Planificateur.

Les boutons situés au-dessus de la page fournissent d'autres options pour les rapports de présentation.

Bouton	Action
File d'attente de tâches	Affiche une page répertoriant les tâches planifiées déjà créées, avec l'état de chacune d'elles. Voir *Affichage de la liste des tâches planifiées*, page 115.
Planificateur	Permet de définir une tâche contenant un ou plusieurs rapports à exécuter un moment spécifique ou de façon périodique. Voir *Planification des rapports de présentation*, page 110.

Copie d'un rapport de présentation

Rubriques connexes :

- *Définition du filtre du rapport*, page 102
- *Rapports de présentation*, page 98

Au départ, la page **Rapports de présentation** affiche le Catalogue de rapports répertoriant tous les rapports prédéfinis installés avec le logiciel. Pour générer l'un de ces rapports pour une période de temps spécifique, sélectionnez le rapport, puis cliquez sur Exécuter.

Ces rapports prédéfinis peuvent également servir de modèles pouvant être copiés pour créer un filtre de rapport personnalisé. Créez un filtre de rapport pour contrôler les éléments tels que les utilisateurs, les catégories, les protocoles et les actions à inclure lorsque vous générez un rapport à partir d'une copie.

Après avoir copié un rapport et modifié ses filtres, vous pouvez copier le nouveau rapport pour créer des variations à partir de cette copie.

1. Sélectionnez un rapport dans le Catalogue de rapports.
2. Cliquez sur **Copier**.

   Un double du nom du rapport s'affiche dans le Catalogue de rapports, avec un code indiquant qu'il s'agit d'une copie.
3. Sélectionnez la copie dans le Catalogue de rapports, puis cliquez sur **Modifier le filtre du rapport** pour en modifier les éléments. Voir *Définition du filtre du rapport*, page 102.

Définition du filtre du rapport

Rubriques connexes :

- *Copie d'un rapport de présentation*, page 101
- *Exécution des rapports de présentation*, page 109

Les filtres de rapport permettent de contrôler les informations incluses dans un rapport. Par exemple, vous pouvez choisir de limiter un rapport aux clients, catégories, classes de risques ou protocoles sélectionnés, ou encore à des actions de filtrage sélectionnées (autoriser, bloquer, etc.). Vous pouvez également saisir un nouveau nom et une nouvelle description dans le Catalogue de rapports, spécifier un logo personnalisé devant s'afficher et définir d'autres options générales via le filtre de rapport.

Remarque

L'utilisation d'un logo personnalisé requiert une certaine préparation avant la définition du filtre de rapport. Vous devez en effet créer le graphique désiré dans un format pris en charge et placer son fichier dans l'emplacement approprié. Voir *Personnalisation du logo des rapports*, page 107.

Les différentes options disponibles dans le filtre dépendent du rapport sélectionné. Par exemple, si vous avez sélectionné un rapport d'informations de groupe, tel que Principaux groupes bloqués par demandes, vous pouvez contrôler les groupes s'affichant dans le rapport mais pas choisir les utilisateurs individuels.

Le filtre des rapports prédéfinis ne peut pas être modifié. Vous pouvez modifier le filtre d'une copie d'un rapport prédéfini :

1. Sélectionnez un rapport dans le Catalogue de rapports.

   Si le bouton Modifier le filtre du rapport est désactivé, passez à l'étape 2.

   Si le bouton Modifier le filtre du rapport est activé, passez à l'étape 3.
2. Cliquez sur **Copier** pour créer une copie personnalisable.

   Un double du nom du rapport s'affiche dans le Catalogue de rapports, avec un code indiquant qu'il s'agit d'une copie.
3. Cliquez sur le bouton **Modifier le filtre du rapport**.

   La page Filtre du rapport s'affiche, avec des onglets distincts permettant de gérer les différents éléments du rapport. Sélectionnez les éléments désirés sur chaque onglet, puis cliquez sur **Suivant** pour passer à l'onglet suivant. Pour plus d'informations, consultez :

   - *Sélection des clients pour un rapport*, page 103
   - *Sélection des catégories pour un rapport*, page 104
   - *Sélection des protocoles pour un rapport*, page 105
   - *Sélection des actions pour un rapport*, page 105

- *Définition des options du rapport*, page 106

4. Dans l'onglet **Confirmer**, choisissez d'exécuter ou de planifier le rapport, en plus d'enregistrer son filtre. Voir *Confirmation de la définition du filtre de rapport*, page 108.

Sélection des clients pour un rapport

Rubriques connexes :

- *Sélection des catégories pour un rapport*, page 104
- *Sélection des protocoles pour un rapport*, page 105
- *Sélection des actions pour un rapport*, page 105
- *Définition des options du rapport*, page 106
- *Confirmation de la définition du filtre de rapport*, page 108

L'onglet **Clients** de la page Rapports de présentation > Filtre de rapport permet de contrôler les clients inclus dans le rapport. Vous ne pouvez sélectionner qu'un type de client pour chaque rapport. Par exemple, vous ne pouvez pas sélectionner des utilisateurs et des groupes pour le même rapport.

Lorsque la définition du rapport spécifie un type de client particulier, vous pouvez choisir des clients de ce type ou des clients représentant un regroupement plus large. Par exemple, si vous avez défini un filtre pour un rapport basé sur Principaux groupes bloqués par demandes, vous pouvez sélectionner des groupes, des domaines ou des unités d'organisation pour le rapport, mais pas sélectionner des utilisateurs individuels.

Si vous souhaitez que le rapport porte sur tous les clients correspondants, aucune sélection n'est nécessaire dans cet onglet.

1. Sélectionnez un type de client dans la liste déroulante.
2. Définissez le nombre maximal de résultats de la recherche dans la liste **Recherche de limite**.

   Selon le trafic présent dans l'organisation, le nombre d'utilisateurs, de groupes ou de domaines présents dans la Base de données d'activité peut être important. Cette option permet de gérer la longueur de la liste des résultats et le temps nécessaire pour afficher ces résultats.
3. Entrez un ou plusieurs caractères de recherche, puis cliquez sur **Rechercher**.

   Servez-vous de l'astérisque (*) comme caractère générique remplaçant des caractères manquants. Par exemple, J*n peut renvoyer Jackson, Jan, Jason, Jon, John, etc.

   Définissez soigneusement votre chaîne de recherche pour être certain que tous les résultats désirés soient inclus dans le nombre de résultats limitant la recherche.
4. Mettez en surbrillance une ou plusieurs entrées dans la liste des résultats, puis cliquez sur la flèche droite (>) pour les déplacer vers la liste **Sélectionné**.

5. Répétez les étapes 2 à 4 autant de fois que nécessaire pour effectuer d'autres recherches et ajouter d'autres clients dans la liste Sélectionné.
6. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Catégories. Voir *Sélection des catégories pour un rapport*, page 104.

Sélection des catégories pour un rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 103
- *Sélection des protocoles pour un rapport*, page 105
- *Sélection des actions pour un rapport*, page 105
- *Définition des options du rapport*, page 106
- *Confirmation de la définition du filtre de rapport*, page 108

L'onglet **Catégories** de la page Rapports de présentation > Filtre de rapport permet de contrôler les informations incluses dans le rapport en fonction des catégories ou des classes de risques. Voir *Classes de risque*, page 41.

Si vous souhaitez que le rapport porte sur toutes les catégories ou classes de risques correspondantes, aucune sélection n'est nécessaire dans cet onglet.

1. Sélectionnez une classification : **Catégorie** ou **Classe de risques**.

   Développez une catégorie parente pour afficher ses sous-catégories. Développez une classe de risque pour afficher la liste des catégories qui lui sont actuellement affectées.

   Si le rapport associé porte sur une classe de risque spécifique, seule la classe de risque et les catégories correspondantes qu'il représente sont disponibles pour la sélection.

   Remarque
   Si vous sélectionnez un sous-ensemble de catégories pour la classe de risque nommée dans le rapport, pensez à modifier le titre du rapport pour refléter vos sélections.

2. Cochez la case de chaque catégorie ou classe de risque à inclure dans le rapport.

   Utilisez les boutons **Sélectionner tout** et **Effacer tout** situées au-dessous de la liste pour réduire le nombre de sélections individuelles requises.
3. Cliquez sur la flèche droite (>) pour déplacer vos sélections vers la liste **Sélectionné**.

   Lorsque vous cochez une classe de risques, un clic sur la flèche droite place toutes les catégories associées dans la liste Sélectionné.
4. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Protocoles. Voir *Sélection des protocoles pour un rapport*, page 105.

Sélection des protocoles pour un rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 103
- *Sélection des catégories pour un rapport*, page 104
- *Sélection des actions pour un rapport*, page 105
- *Définition des options du rapport*, page 106
- *Confirmation de la définition du filtre de rapport*, page 108

L'onglet **Protocoles** de la page Rapports de présentation > Filtre de rapport permet de contrôler les protocoles inclus dans le rapport.

Si vous souhaitez que le rapport porte sur tous les protocoles correspondants, aucune sélection n'est nécessaire dans cet onglet.

1. Cliquez sur l'icône placée à côté du nom du groupe pour développer et réduire les groupes de protocoles.
2. Cochez la case de chaque protocole à inclure dans le rapport.

   Utilisez les boutons **Sélectionner tout** et **Effacer tout** situées au-dessous de la liste pour réduire le nombre de sélections individuelles requises.
3. Cliquez sur la flèche droite (>) pour déplacer vos sélections vers la liste **Sélectionné**.
4. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Actions. Voir *Sélection des actions pour un rapport*, page 105.

Sélection des actions pour un rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 103
- *Sélection des catégories pour un rapport*, page 104
- *Sélection des protocoles pour un rapport*, page 105
- *Définition des options du rapport*, page 106
- *Confirmation de la définition du filtre de rapport*, page 108

L'onglet **Actions** de la page Rapports de présentation > Filtre de rapport permet de contrôler avec précision les actions de filtrage, par exemple Autorisés par filtre d'accès limité ou Bloqués par temps contingenté, incluses dans le rapport. Si le rapport spécifie un type particulier d'action, par exemple Bloquer, vous ne pouvez sélectionner que les actions de ce type pour le rapport.

Si vous souhaitez que le rapport porte sur toutes les actions correspondantes, aucune sélection n'est nécessaire dans cet onglet.

1. Cliquez sur l'icône placée à côté du nom du groupe pour développer et réduire les groupes d'actions.
2. Cochez la case de chaque action à inclure dans le rapport.

   Utilisez les boutons **Sélectionner tout** et **Effacer tout** situées au-dessous de la liste pour réduire le nombre de sélections individuelles requises.
3. Cliquez sur la flèche droite (>) pour déplacer vos sélections vers la liste **Sélectionné**.
4. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Options. Voir *Définition des options du rapport*, page 106.

Définition des options du rapport

Rubriques connexes :

- *Personnalisation du logo des rapports*, page 107
- *Sélection des clients pour un rapport*, page 103
- *Sélection des catégories pour un rapport*, page 104
- *Sélection des protocoles pour un rapport*, page 105
- *Sélection des actions pour un rapport*, page 105
- *Définition des options du rapport*, page 106
- *Confirmation de la définition du filtre de rapport*, page 108

L'onglet **Options** de la page Rapports de présentation > Modifier le filtre du rapport permet de configurer plusieurs aspects du rapport.

1. Modifiez le **nom** devant s'afficher dans le Catalogue de rapports. Ce nom peut comprendre jusqu'à 85 caractères.

   Ce nom n'apparaît pas dans le rapport lui-même mais permet uniquement d'identifier une combinaison unique de format de rapport et de filtre dans le Catalogue de rapports.
2. Modifiez le **Titre du rapport** affiché dans le rapport. Ce titre peut comprendre jusqu'à 85 caractères.
3. Modifiez la **Description** affichée dans le Catalogue de rapports. Cette description peut comprendre jusqu'à 336 caractères.

   La description doit permettre d'identifier cette combinaison unique de format de rapport et de filtre dans le Catalogue de rapports.
4. Sélectionnez le logo devant s'afficher dans le rapport.

   Tous les fichiers image pris en charge dans le répertoire approprié sont énumérés. Voir *Personnalisation du logo des rapports*, page 107.
5. Cochez la case **Enregistrer comme favori** pour que le rapport apparaisse dans les Favoris.

Le Catalogue de rapports désigne les rapports Favoris par un symbole en forme d'étoile. Vous pouvez sélectionner **Afficher uniquement les favoris** dans la page Catalogue de rapports pour réduire le nombre de rapports apparaissant dans la liste et localiser plus rapidement un rapport spécifique.

6. Cochez la case **Afficher seulement la partie supérieure** et entrez un nombre compris entre 1 et 20 pour limiter le nombre d'éléments présentés.

   Cette option n'apparaît que si le rapport sélectionné est au format N premiers, conçu pour n'afficher qu'un nombre limité d'éléments. L'élément limité dépend du rapport. Par exemple, dans le cas d'un rapport Principales catégories visitées, cette entrée détermine le nombre de catégories présentées dans le rapport.

7. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Confirmer. Voir *Confirmation de la définition du filtre de rapport*, page 108.

Personnalisation du logo des rapports

Les rapports de présentation prédéfinis affichent le logo Websense dans le coin supérieur gauche. Lorsque vous copiez un rapport prédéfini et que vous définissez son filtre, vous pouvez choisir un logo différent.

1. Créez un fichier image dans l'un des formats suivants :

   - .bmp
   - .gif
   - .jfif
   - .jpe
   - .jpg
   - .jpeg
   - .png
   - .ttf

2. Le nom du fichier image ne doit pas dépasser 25 caractères, extension comprise.
3. Placez le fichier image dans le répertoire suivant :

   ```
   <chemin_installation>\Manager\ReportingTemplates\images
   ```

   Le chemin d'installation par défaut est C:\Program Files\Websense.

Tous les fichiers image pris en charge dans ce répertoire apparaissent automatiquement dans la liste déroulante de l'onglet Options de la page Filtre de rapport. L'image est automatiquement mise à l'échelle en fonction de l'espace affecté au logo. (Voir *Définition des options du rapport*, page 106.)

Remarque

Ne supprimez pas les images actives dans les filtres de rapport provenant de ce répertoire. En l'absence du fichier de logo spécifié, le rapport ne peut pas être généré.

Confirmation de la définition du filtre de rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 103
- *Sélection des catégories pour un rapport*, page 104
- *Sélection des protocoles pour un rapport*, page 105
- *Sélection des actions pour un rapport*, page 105
- *Définition des options du rapport*, page 106

L'onglet **Confirmer** de la page Rapports de présentation > Filtre derapport présente le nom et la description qui s'afficheront dans le Catalogue de rapports et vous permet de choisir comment procéder.

1. Vérifiez le **Nom** et la **Description**.

   Si des modifications sont nécessaires, cliquez sur **Précédent** pour revenir à l'onglet Options et apporter les modifications désirées. (Voir *Définition des options du rapport*, page 106.)

2. Indiquez ensuite ce que vous souhaitez faire :

Option	Description
Enregistrer	Enregistre le filtre de rapport et rouvre le Catalogue de rapports. Voir *Rapports de présentation*, page 98.
Enregistrer et exécuter	Enregistre le filtre de rapport et ouvre la page Exécuter le rapport. Voir *Exécution des rapports de présentation*, page 109.
Enregistrer et planifier	Enregistre le filtre de rapport et ouvre la page Planifier le rapport. Voir *Planification des rapports de présentation*, page 110.

3. Cliquez sur **Terminer** pour implémenter la sélection faite à l'étape 2.

Fonctionnement des favoris

Rubriques connexes :

- *Rapports de présentation*, page 98
- *Exécution des rapports de présentation*, page 109
- *Planification des rapports de présentation*, page 110

Vous pouvez désigner tout rapport de présentation, prédéfini ou personnalisé, en tant que Favori. Utilisez cette option pour identifier les rapports que vous générez le plus

souvent et que vous souhaitez pouvoir localiser rapidement dans le Catalogue de rapports.

1. Dans la page **Rapports de présentation**, mettez en surbrillance un rapport que vous générez fréquemment ou que vous souhaitez pouvoir localiser rapidement.
2. Cliquez sur **Favori**.

   Un symbole en forme d'étoile s'affiche dans la liste à côté du nom des rapports Favoris, ce qui vous permet de les identifier rapidement lorsque tous les rapports sont affichés.
3. Cochez la case **Afficher uniquement les favoris** située au-dessus du Catalogue de rapports pour limiter la liste aux rapports désignés comme Favoris. Désactivez cette option pour restaurer la liste complète des rapports.

Lorsqu'un rapport Favori n'est plus utilisé aussi fréquemment, vous pouvez supprimer la désignation Favori.

1. Mettez en surbrillance un rapport désigné comme Favori par le symbole en forme d'étoile.
2. Cliquez sur **Favori**.

   Le symbole est retiré du nom du rapport dans le Catalogue de rapports. Le rapport n'apparaît plus dans la liste si vous choisissez **Afficher uniquement les favoris**.

Exécution des rapports de présentation

Rubriques connexes :

- *Rapports de présentation*, page 98
- *Planification des rapports de présentation*, page 110

L'exécution immédiate d'un seul rapport comprend quelques étapes présentées ci-dessous.

Remarque

Avant de générer un rapport au format PDF, assurez-vous qu'Adobe Reader v7.0 ou version ultérieure est installé sur l'ordinateur à partir duquel vous accédez à Websense Manager.

Avant de générer un rapport au format XLS, assurez-vous que Microsoft Excel 2003 ou version ultérieure est installé sur l'ordinateur à partir duquel vous accédez à Websense Manager.

Si le logiciel approprié n'est pas installé, vous avez la possibilité d'enregistrer le fichier.

Vous pouvez également créer des tâches avec un ou plusieurs rapports et les planifier pour qu'ils s'exécutent une seule fois ou de façon récurrente avec la fonction de

planification d'un rapport de présentation. Voir *Planification des rapports de présentation*, page 110.

1. Dans la page **Rapports de présentation**, mettez un rapport en surbrillance dans l'arborescence du Catalogue de rapports, puis cliquez sur **Exécuter**.
2. Sélectionnez la **Date de début** et la **Date de fin** des données du rapport.
3. Sélectionnez le **Format de sortie** du rapport.

Format	Description
PDF	Portable Document Format. Les fichiers PDF s'affichent dans Adobe Reader.
HTML	HyperText Markup Language. Les fichiers HTML peuvent s'afficher directement dans votre navigateur Internet Explorer ou Firefox.
XLS	Feuille de calcul Excel. Les fichiers XLS s'affichent Microsoft Excel.

4. Si vous sélectionnez un rapport **N premiers**, choisissez le nombre d'éléments devant apparaître dans le rapport.
5. Cliquez sur **Exécuter**.

   Les rapports HTML apparaissent dans le panneau de contenu. Si vous sélectionnez une sortie PDF ou XLS, vous avez la possibilité d'ouvrir le rapport dans une fenêtre distincte ou d'enregistrer le rapport sur le disque.
6. Pour imprimer un rapport, utilisez la commande Imprimer du programme dans lequel le rapport est affiché.

   Pour de meilleurs résultats, générez une sortie PDF ou XLS pour l'impression. Utilisez ensuite les options d'impression d'Adobe Reader ou de Microsoft Excel, respectivement.

Vous pouvez enregistrer un rapport sélectionné pour une sortie au format PDF ou XLS en utilisant la fonction Enregistrer d'Adobe Reader ou de Microsoft Excel.

Planification des rapports de présentation

Rubriques connexes :

- *Rapports de présentation*, page 98
- *Exécution des rapports de présentation*, page 109
- *Affichage de la liste des tâches planifiées*, page 115
- *Copie d'un rapport de présentation*, page 101

Vous pouvez exécuter les rapports de présentation lorsqu'ils sont nécessaires ou utiliser la page **Rapports de présentation > Planificateur** pour créer des tâches qui définissent un planning d'exécution d'un ou plusieurs rapports.

Les rapports générés par les tâches planifiées sont envoyés à un ou plusieurs destinataires par courrier électronique. Lorsque vous créez des travaux planifiés, tenez compte de la taille et de la quantité de fichiers de rapport joints que peut gérer votre serveur de messagerie.

Pour accéder au Planificateur :

- Cliquez sur le bouton **Planificateur** situé en haut de la page Rapports de présentation (au-dessus du Catalogue de rapports).
- Lorsque vous ajoutez ou modifiez le filtre d'un rapport, choisissez **Enregistrer et planifier** dans l'onglet Confirmer, puis cliquez sur **Terminer**. (Voir *Copie d'un rapport de présentation*, page 101.)
- Cliquez sur le lien du nom de la tâche dans la page File d'attente des tâches pour modifier une tâche.
- Cliquez sur **Ajouter** dans la page File d'attente des tâches pour créer une nouvelle tâche.

La page Planificateur contient plusieurs onglets permettant de sélectionner les rapports à exécuter et leur planning d'exécution. Pour plus d'informations, consultez :

- *Définition du planning*, page 111
- *Sélection des rapports à planifier*, page 113
- *Définition de la plage de dates*, page 114
- *Sélection des options de sortie*, page 115

Après avoir créé des tâches, vous pouvez afficher une liste présentant l'état et d'autres informations utiles sur les tâches. Voir *Affichage de la liste des tâches planifiées*, page 115.

Définition du planning

Rubriques connexes :

- *Planification des rapports de présentation*, page 110
- *Sélection des rapports à planifier*, page 113
- *Sélection des options de sortie*, page 115
- *Définition de la plage de dates*, page 114

Pour définir une tâche de création de rapport à n'exécuter qu'une seule fois ou de façon périodique, utilisez l'onglet **Planificateur** de la page Rapports de présentation > Planificateur.

> **Remarque**
> Il est préférable de planifier les tâches de rapport à des heures et des jours différents pour éviter une surcharge de la Base de données d'activité et de ralentir les performances de la journalisation et de la création interactive des rapports.

1. Entrez un **nom de tâche** identifiant de façon unique cette tâche planifiée.
2. Sélectionnez le **Modèle de récurrence** et les **Options de récurrence** de la tâche. Les différentes options disponibles dépendent du modèle sélectionné.

Modèle	Options
Une fois	Entrez la date exacte d'exécution de la tâche ou cliquez sur l'icône pour sélectionner la date dans un calendrier.
Quotidien	Aucune autre option de récurrence n'est disponible.
Hebdomadaire	Cochez la case des jours de la semaine pour lesquels la tâche doit s'exécuter.
Mensuel	Entrez les dates du mois pour lesquelles la tâche doit s'exécuter. Les dates doivent correspondre à un nombre compris entre 1 et 31 et doivent être séparées par des virgules (1,10,20). Pour une exécution de la tâche à des dates consécutives chaque mois, entrez les dates de début et de fin séparées par un tiret (3-5).

3. Sous **Planifier l'heure**, définissez l'heure de début d'exécution de la tâche.

   La tâche démarre en fonction de l'heure définie sur l'ordinateur dans lequel s'exécute Websense Manager.

> **Remarque**
> Pour commencer à générer les rapports planifiés le jour même, sélectionnez une heure en tenant compte du temps qu'il vous faudra pour terminer la définition de la tâche.

4. Sous **Planifier la période**, sélectionnez une date de démarrage du travail et une option de terminaison.

Option	Description
Aucune date de fin	Le travail poursuit indéfiniment son exécution selon le planning établi. Pour l'interrompre par la suite, modifiez-le ou supprimez-le. Voir *Affichage de la liste des tâches planifiées*, page 115.
Finir après	Sélectionnez le nombre de fois où la tâche doit s'exécuter. Après ce nombre d'occurrences, la tâche ne s'exécute plus, mais demeure dans la file d'attente jusqu'à ce que vous la supprimiez. Voir *Affichage de la liste des tâches planifiées*, page 115.
Finir le	Définissez la date à laquelle l'exécution de la tâche doit s'arrêter. Après cette date, elle ne s'exécute plus.

5. Cliquez sur **Suivant** pour ouvrir l'onglet Sélectionner rapport. Voir *Sélection des rapports à planifier*, page 113.

Sélection des rapports à planifier

Rubriques connexes :

- *Planification des rapports de présentation*, page 110
- *Définition du planning*, page 111
- *Sélection des options de sortie*, page 115
- *Définition de la plage de dates*, page 114

L'onglet **Sélectionner rapport** de la page Rapports de présentation > Planificateur permet de choisir des rapports pour la tâche.

1. Sélectionnez un rapport pour cette tâche dans le Catalogue de rapports.
2. Cliquez sur la flèche droite (>) pour déplacer ce rapport vers la liste **Sélectionné**.
3. Répétez les étapes 1 et 2 jusqu'à ce que tous les rapports de cette tâche s'affichent dans la liste **Sélectionné**.
4. Cliquez sur **Suivant** pour ouvrir l'onglet Intervalle de dates. Voir *Définition de la plage de dates*, page 114.

Définition de la plage de dates

Rubriques connexes :

- *Planification des rapports de présentation*, page 110
- *Définition du planning*, page 111
- *Sélection des rapports à planifier*, page 113
- *Sélection des options de sortie*, page 115

L'onglet **Intervalle de dates** de la page Rapports de présentation > Planificateur permet de définir la plage des dates de la tâche. Les options disponibles dépendent de l'**intervalle de dates** sélectionné.

Intervalle de dates	Description
Toutes les dates	Les rapports comprennent toutes les dates disponibles dans la Base de données d'activité. Aucune entrée supplémentaire n'est nécessaire. Lorsque cette option est utilisée pour des travaux récurrents, les mêmes informations peuvent apparaître dans des rapports exécutés séparément.
Dates spécifiques	Sélectionnez les heures exactes de début (**Du**) et de fin (**Au**) des rapports de cette tâche. Cette option est idéale pour les tâches qui ne s'exécutent qu'une seule fois. Choisir cette option pour un planning récurrent entraîne des rapports en double.
Dates relatives	Utilisez les listes déroulantes pour sélectionner le nombre de périodes devant faire l'objet des rapports (Ce/cette, Dernier(ère), Deux dernier(ère)s, etc.), et le type de période (Jours, Semaines ou Mois). Par exemple, la tâche peut couvrir les deux dernières semaines ou le mois en cours. Une semaine représente une semaine de calendrier, du dimanche au samedi. Un mois représente un mois du calendrier. Par exemple, Cette semaine produit un rapport allant du dimanche au jour en cours ; Le mois en cours produit un rapport allant du premier jour du mois à la date du jour ; La semaine dernière produit un rapport allant du dimanche au samedi précédent ; etc. Cette option est idéale pour les tâches qui s'exécutent de façon régulière. Il vous permet de choisir la quantité de données apparaissant dans chaque rapport et de réduire le nombre de données en double dans les rapports exécutés séparément.

Après avoir défini la plage de dates pour le travail, cliquez sur **Suivant** pour afficher l'onglet Sortie. Voir *Sélection des options de sortie*, page 115.

Sélection des options de sortie

Rubriques connexes :

- *Planification des rapports de présentation*, page 110
- *Définition du planning*, page 111
- *Sélection des rapports à planifier*, page 113
- *Définition de la plage de dates*, page 114

Après avoir sélectionné les rapports d'une tâche, utilisez l'onglet **Sortie** pour sélectionner le format de sortie et les options de distribution.

1. Sélectionnez le format de fichier du rapport final.

Format	Description
PDF	Portable Document Format. Les destinataires doivent disposer d'Adobe Reader v7.0 ou version ultérieure pour afficher les rapports au format PDF.
XLS	Feuille de calcul Excel. Les destinataires doivent disposer de Microsoft Excel 2003 ou version ultérieure pour afficher les rapports au format XLS.

2. Entrez les adresses électroniques auxquelles le rapport doit être envoyé.

   Chaque adresse doit être placée sur une ligne distincte.
3. Au besoin, cochez la case **Personnaliser le sujet et le corps du courrier électronique**. Dans ce cas, entrez le texte personnalisé **Objet** et **Corps** du courrier électronique de cette tâche.
4. Cliquez sur **Enregistrer une tâche** pour enregistrer et implémenter la définition de la tâche et afficher la page File d'attente des tâches.
5. Vérifiez cette tâche et les autres tâches planifiées. Voir *Affichage de la liste des tâches planifiées*, page 115.

Affichage de la liste des tâches planifiées

Rubriques connexes :

- *Rapports de présentation*, page 98
- *Planification des rapports de présentation*, page 110
- *Sélection des options de sortie*, page 115
- *Planification des rapports d'investigation*, page 138

La page **Rapports de présentation > File d'attente des tâches** présente la liste des tâches planifiées créées pour les rapports de présentation. La liste donne l'état de chaque tâche et les informations de base s'y rapportant telles que leur fréquence d'exécution. Depuis cette page, vous pouvez ajouter supprimer des tâches planifiées, suspendre temporairement une tâche, etc.

(Pour revoir les tâches planifiées pour les rapports d'investigation, consultez la section *Gestion des tâches de rapports d'investigation planifiés*, page 141.)

La liste fournit les informations suivantes pour chaque tâche.

Colonne	Description
Nom de tâche	Nom donné à la tâche lors de sa création.
État	L'état peut être : • ACTIVÉ indique que la tâche s'exécute en fonction du modèle de récurrence établi. • DÉSACTIVÉ indique que la tâche est inactive et ne s'exécute pas.
Récurrence	Modèle de récurrence (Une fois, Quotidien, Hebdomadaire, Mensuel) défini pour cette tâche.
Historique	Cliquez sur le lien **Détails** pour ouvrir la page Historique de tâches pour la tâche sélectionnée. Voir *Affichage de l'historique d'une tâche*, page 117.
Prochaine planification	Date et heure de la prochaine exécution
Propriétaire	Nom d'utilisateur de l'administrateur qui a planifié la tâche

Servez-vous des options de la page pour gérer les tâches. Certains boutons exigent que vous cochiez la case accolée au nom de chaque tâche à inclure.

Option	Description
Lien nom de la tâche	Ouvre la page Planificateur, qui vous permet de modifier la définition de la tâche. Voir *Planification des rapports de présentation*, page 110.
Ajouter une tâche	Ouvre la page Planificateur, qui vous permet de définir une nouvelle tâche. Voir *Planification des rapports de présentation*, page 110.
Supprimer	Supprime de la file d'attente toutes les tâches cochées dans la liste. Après avoir été supprimée, une tâche ne peut pas être restaurée. Pour interrompre temporairement l'exécution d'une tâche spécifique, utilisez le bouton **Désactiver**.
Exécuter maintenant	Lance immédiatement l'exécution des tâches cochées dans la liste. Il s'agit là d'un ajout aux exécutions planifiées régulièrement.

Option	Description
Activer	Réactive immédiatement les tâches cochées dans la liste. La tâche commence son exécution selon le planning établi.
Désactiver	Désactive l'exécution des tâches activées et cochées dans la liste. Servez-vous de cette option pour interrompre temporairement une tâche que vous souhaiterez peut-être restaurer ultérieurement.

Affichage de l'historique d'une tâche

Rubriques connexes :

- *Planification des rapports de présentation*, page 110
- *Affichage de la liste des tâches planifiées*, page 115

La page **Rapports de présentation > File d'attente de tâches > Historique des tâches** permet d'afficher des informations sur les tentatives récentes d'exécution de la tâche sélectionnée. La page énumère chaque rapport séparément, en fournissant les informations suivantes.

Colonne	Description
Nom du rapport	Titre imprimé sur le rapport
Date de début	Date et heure de début d'exécution du rapport
Date de fin	Date et heure de fin d'exécution du rapport
État	Indicateur de réussite ou d'échec du rapport
Message	Informations sur la tâche, indiquant par exemple si le rapport a bien été envoyé par courrier électronique.

Rapports d'investigation

Rubriques connexes :

- *Rapports résumés*, page 120
- *Rapports résumés multi-niveaux*, page 124
- *Rapports détaillés flexibles*, page 125
- *Rapports Détails de l'activité utilisateur*, page 129
- *Rapports standard*, page 134
- *Rapports d'investigation favoris*, page 136
- *Planification des rapports d'investigation*, page 138
- *Rapports Cas particuliers*, page 141
- *Sortie dans un fichier*, page 142
- *Connexion à la base de données et paramètres par défaut des rapports*, page 335

La page **Génération de rapports > Rapports d'investigation** permet d'analyser l'activité de filtrage Internet de façon interactive.

Au départ, la page Rapports d'investigation principale affiche un résumé de l'activité par classe de risques. Dans le rapport résumé, cliquez sur les liens et les éléments disponibles qui vous intéressent et examinez l'aperçu général de l'utilisation Internet dans votre organisation. Voir *Rapports résumés*, page 120.

Les rapports résumés multi-niveaux (voir *Rapports résumés multi-niveaux*, page 124) et les rapports détaillés flexibles (voir *Rapports détaillés flexibles*, page 125) vous permettent d'analyser les informations sous différentes perspectives.

D'autres fonctions d'affichage des rapports et de rapports d'investigation sont disponibles à partir des liens situés en haut de la page. Le tableau ci-dessous présente la liste des liens et des fonctions auxquelles ils permettent d'accéder. (Certains liens ne sont pas disponibles sur toutes les pages.)

Option	Action
Utilisateur par jour/mois	Affiche une boîte de dialogue qui vous permet de définir un rapport sur une activité spécifique de l'utilisateur, pour une journée ou un mois. Pour plus d'informations, consultez *Rapports Détails de l'activité utilisateur*, page 129.
Rapports standard	Affiche la liste des rapports prédéfinis qui vous permettent de consulter rapidement une combinaison spécifique de données. Voir *Rapports standard*, page 134.
Rapports favoris	Permet d'enregistrer le rapport en cours en tant que Favori et d'afficher la liste des Favoris que vous pouvez générer ou planifier. Voir *Rapports d'investigation favoris*, page 136.

Option	Action
File d'attente de tâches	Affiche la liste des tâches de rapports d'investigation planifiés. Voir *Planification des rapports d'investigation*, page 138.
Cas particuliers	Affiche les rapports d'utilisation Internet qui s'éloignent significativement de la moyenne. Voir *Rapports Cas particuliers*, page 141.
Options	Affiche une page qui permet de sélectionner une autre Base de données d'activité pour la génération de rapports. La page Options vous permet également de personnaliser certaines fonctions de création de rapport, par exemple la période initialement affichée dans les rapports résumés et les colonnes par défaut des rapports détaillés. Voir *Connexion à la base de données et paramètres par défaut des rapports*, page 335.
	Cliquez sur ce bouton, à droite des champs Rechercher, pour exporter le rapport actif dans une feuille de calcul compatible Microsoft Excel. Le système vous invite à ouvrir ou à enregistrer le fichier. Pour pouvoir ouvrir le fichier, Microsoft Excel 2003 ou une version ultérieure doit être installé. Voir *Sortie dans un fichier*, page 142.
	Cliquez sur ce bouton, à droite des champs Rechercher, pour exporter le rapport actif dans un fichier PDF compatible avec Adobe Reader. Le système vous invite à ouvrir ou à enregistrer le fichier. Pour pouvoir ouvrir le fichier, Adobe Reader version 7.0 ou ultérieure doit être installé. Voir *Sortie dans un fichier*, page 142.

N'oubliez pas que la génération de rapports est limitée aux informations enregistrées dans la Base de données d'activité (Log Database). Si vous désactivez la journalisation des utilisateurs, des adresses IP ou des catégories sélectionnées (voir *Configuration de Filtering Service pour la journalisation*, page 308), ces informations ne peuvent pas être incluses. De même, si vous désactivez la journalisation de certains protocoles (voir *Modification d'un filtre de protocoles*, page 52), les requêtes pour ces protocoles ne sont pas disponibles. Si vous voulez que le rapport présente à la fois le nom de domaine (www.domaine.com) et le chemin d'une page particulière dans le domaine (/produits/produitA), vous devez journaliser les adresses URL complètes (voir *Configuration de la journalisation des URL complètes*, page 326).

Les rapports d'investigation de Websense sont limités par le processeur et la mémoire disponible dans l'ordinateur sur lequel s'exécute Websense Manager, de même que certaines ressources réseau. L'exécution de certains rapports de grande taille peut se révéler très longue. Une option du message de progression permet d'enregistrer le rapport en tant que Favori de manière à pouvoir planifier son exécution à un autre moment. Voir *Planification des rapports d'investigation*, page 138.

Rapports résumés

Rubriques connexes :

- *Rapports résumés multi-niveaux*, page 124
- *Rapports détaillés flexibles*, page 125
- *Rapports Détails de l'activité utilisateur*, page 129
- *Rapports standard*, page 134
- *Rapports d'investigation favoris*, page 136
- *Planification des rapports d'investigation*, page 138
- *Rapports Cas particuliers*, page 141
- *Sortie dans un fichier*, page 142

Au départ, la page Rapports d'investigation affiche le rapport résumé de l'utilisation de tous les utilisateurs par classe de risques, présentant l'activité de la Base de données d'activité pour la journée. La mesure du graphique à barres initial est Accès (nombre de fois où le site a été demandé). Pour configurer la période que doit couvrir ce rapport résumé initial, consultez la section *Connexion à la base de données et paramètres par défaut des rapports*, page 335.

Modifiez rapidement les informations rapportées ou explorez les détails du rapport, en cliquant sur les différents liens et options disponibles sur la page.

1. Sélectionnez l'une des options suivantes dans la liste **Mesure**.

Option	Description
Accès	Nombre de fois où l'URL a été demandée. Selon la configuration de Log Server, il peut s'agir de véritables accès, qui conservent un enregistrement distinct pour chaque élément du site demandé, ou de visites, qui combinent les différents éléments du site dans un même enregistrement du journal. Voir *Configuration des fichiers cache du journal*, page 315.
Bande passante [ko]	Quantité de données, en kilo-octets, contenues dans la requête initiale de l'utilisateur et dans la réponse du site Web. Il s'agit du total combiné des valeurs Envoyé et Reçu. N'oubliez pas que certains produits d'intégration n'envoient pas ces informations à Websense. Les pare-feu Check Point FireWall-1 et Cisco PIX Firewall en sont deux exemples. Si votre intégration n'envoie pas ces informations, et que Websense Network Agent est installé, activez l'option **Journaliser les demandes HTTP** de la carte d'interface réseau appropriée pour activer la génération de rapports sur les informations de bande passante. Voir *Configuration des paramètres des cartes réseau*, page 349.
Envoyés [ko]	Nombre de kilo-octets envoyés dans la requête Internet. Cela représente la quantité de données transmises, pouvant correspondre à une simple demande d'URL, ou d'une soumission plus importante, par exemple si l'utilisateur s'enregistre auprès d'un site Web.

Option	Description
Reçus [ko]	Nombre de kilo-octets reçus en réponse à la requête. Cela comprend l'ensemble du texte, des graphiques et des scripts qui composent le site. Dans le cas des sites bloqués, le nombre de kilo-octets dépend du logiciel qui crée l'enregistrement du journal. Lorsque Websense Network Agent journalise les enregistrements, le nombre d'octets reçus pour un site bloqué correspond à la taille de la page de blocage de Websense. Si l'enregistrement de journal est créé par Websense Security Gateway en résultat d'une analyse en temps réel, les kilo-octets reçus représentent la taille de la page analysée. Pour plus d'informations sur l'analyse en temps réel, consultez *Analyse du contenu avec les options en temps réel*, page 145. Lorsqu'un autre produit d'intégration crée les enregistrements du journal, les kilo-octets reçus pour un site bloqué peuvent correspondre à zéro (0), à la taille de la page bloquée ou à la valeur obtenue du site demandé.
Temps de navigation	Évaluation du temps passé à naviguer sur le site. Voir *Temps de navigation sur Internet*, page 97.

2. Modifiez le regroupement principal du rapport en sélectionnant une option dans la liste **Utilisation d'Internet par** située au-dessus du rapport.

   Les options dépendent du contenu de la Base de données d'activité et de certaines caractéristiques du réseau. Par exemple, si la Base de données d'activité ne comprend qu'un seul groupe ou domaine, Groupes et Domaines n'apparaissent pas dans la liste. De même, lorsqu'il y a trop d'utilisateurs (plus de 5 000) ou de groupes (plus de 3 000), ces options ne s'affichent pas. (Certaines de ces limites peuvent être configurées. Voir *Options d'affichage et de sortie*, page 337.)

3. Cliquez sur un nom dans la colonne de gauche (ou sur la flèche accolée au nom) pour afficher la liste des options, par exemple par utilisateur, par domaine ou par action.

   Les options de la liste sont les mêmes que celles qui apparaissent sous Utilisation d'Internet par, personnalisées par rapport au contenu affiché.

   Remarque

   Certaines options telles qu'Utilisateur ou Groupe, s'affichent parfois en lettres rouges. Dans ce cas, la sélection de cette option peut entraîner la production d'un rapport très volumineux dont l'exécution sera très longue. Avant de sélectionner cette option, tentez de préciser davantage de détails.

4. Sélectionnez l'une de ces options pour générer un nouveau rapport résumé présentant les informations sélectionnées pour l'entrée associée.

   Par exemple, dans un rapport résumé Classe de risque, un clic sur Par utilisateur sous la classe de risque Responsabilité légale engagée génère un rapport sur l'activité de chaque utilisateur dans cette dernière classe de risque.

5. Cliquez sur une nouvelle entrée dans la colonne de gauche, puis sélectionnez une option pour afficher davantage de détails sur cet élément particulier.
6. Pour modifier l'ordre de tri du rapport, servez-vous des flèches placées à côté des en-têtes de colonne.
7. Contrôlez le rapport résumé à l'aide des options suivantes, placées au-dessus du graphique. Ensuite, explorez les détails associés en cliquant sur les éléments du nouveau rapport.

Option	Action
Chemin du rapport (Utilisateur > Jour)	À côté de la liste **Utilisation d'Internet par**, un chemin présente les sélections à l'origine du rapport actuel. Cliquez sur l'un des liens du chemin pour revenir à cette vue des données.
Afficher	Sélectionnez une période pour le rapport : Un jour, Une semaine, Un mois ou Tous. Le rapport s'actualise pour afficher les données de la période sélectionnée. Servez-vous des flèches adjacentes pour parcourir les données disponibles, une période (jour, semaine, mois) à la fois. Lorsque vous modifiez cette sélection, les champs **Afficher de** sont mis à jour pour refléter la période affichée. Si vous choisissez une date spécifique dans les champs Afficher de ou via la boîte de dialogue Favoris, le champ **Afficher** indique Personnalisé, à la place d'une période.
Afficher de... au...	Les dates de ces champs s'actualisent automatiquement pour refléter la période affichée lorsque vous modifiez le champ **Afficher**. Vous pouvez également entrer les dates exactes de début et de fin des rapports, ou cliquer sur l'icône du calendrier pour sélectionner les dates désirées. Cliquez sur la flèche droite adjacente pour actualiser le rapport après avoir sélectionné des dates.
Graphique en secteurs / Graphique à barres	Lorsque le graphique à barres est actif, cliquez sur **Graphique en secteurs** pour afficher le rapport résumé actuel sous forme de graphique à secteurs. Cliquez sur l'étiquette du secteur pour afficher les mêmes options que celles qui sont disponibles lorsque vous cliquez sur une entrée de la colonne gauche du graphique à barres. Lorsque le graphique en secteurs est actif, cliquez sur **Graphique à barres** pour afficher le rapport résumé actuel sous forme de graphique à barres.
Plein écran	Sélectionnez cette option pour afficher le rapport d'investigation actif dans une fenêtre distincte, sans les panneaux de navigation gauche et droit.

Option	Action
Anonyme /Noms	Cliquez sur **Anonyme** pour que les rapports présentent un numéro d'identification d'utilisateur attribué en interne chaque fois que le nom de l'utilisateur devrait s'afficher. Lorsque les noms sont masqués, cliquez sur **Noms** pour afficher les noms d'utilisateur dans ces emplacements. Dans certains cas, les noms d'utilisateur ne peuvent pas s'afficher. Pour plus d'informations, consultez *Configuration de Filtering Service pour la journalisation*, page 308. Si vous cliquez sur Anonyme et que vous passez ensuite à une autre vue des données, par exemple à une vue détaillée ou des cas particuliers, les noms d'utilisateur demeurent masqués dans le nouveau rapport. Pour revenir à la vue résumée avec les noms masqués, utilisez les liens placés en haut du rapport et non ceux de la bannière. Si certains administrateurs individuels ne doivent jamais accéder aux noms d'utilisateur dans le rapport, affectez-les à un rôle pour lequel les autorisations de création de rapport interdisent l'affichage des noms d'utilisateur dans les rapports d'investigation et l'accès aux rapports de présentation.
Rechercher	Sélectionnez un élément de rapport dans la liste, puis entrez une partie ou la totalité de la valeur de la recherche dans la zone de texte adjacente. Cliquez sur la flèche adjacente pour lancer la recherche et afficher les résultats. La saisie d'une adresse IP partielle, telle que 10.5., lance une recherche sur tous les sous-réseaux, de 10.5.0.0 à 10.5.255.255 dans cet exemple.

8. Ajoutez un sous-ensemble d'informations pour toutes les entrées ou pour les entrées sélectionnées dans la colonne de gauche en créant un rapport résumé multi-niveaux. Voir *Rapports résumés multi-niveaux*, page 124.
9. Créez un rapport tabulaire pour un élément spécifique de la colonne de gauche en cliquant sur le nombre adjacent ou dans la barre de mesure. Ce rapport détaillé peut être modifié en fonction de vos besoins spécifiques. Voir *Rapports détaillés flexibles*, page 125.

Rapports résumés multi-niveaux

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports résumés*, page 120
- *Rapports détaillés flexibles*, page 125
- *Rapports Détails de l'activité utilisateur*, page 129
- *Rapports standard*, page 134
- *Rapports d'investigation favoris*, page 136
- *Planification des rapports d'investigation*, page 138
- *Rapports Cas particuliers*, page 141
- *Sortie dans un fichier*, page 142

Les rapports résumés multi-niveaux présentent un second niveau d'informations qui complète les informations principales affichées. Par exemple, si l'affichage principal présente les classes de risques, vous pouvez définir un second niveau pour identifier les catégories les plus demandées dans chaque classe de risques. Dans un autre exemple, si le rapport principal présente les requêtes pour chaque catégorie, vous pouvez afficher les cinq premières catégories et les 10 utilisateurs à l'origine de la plupart des requêtes dans chaque catégorie.

Pour créer un rapport résumé multi-niveaux, servez-vous des paramètres situés immédiatement au-dessus du rapport résumé.

1. Dans la liste **Relever les**, choisissez un chiffre indiquant le nombre d'entrées principales (colonne de gauche) à utiliser dans le rapport. Le rapport résultant inclut les entrées principales avec les plus grandes valeurs. (Les dates les plus récentes s'affichent si l'entrée principale est Jour.)

   Vous pouvez également cocher la case accolée aux entrées individuelles désirées dans la colonne de gauche pour ne créer des rapports que pour ces entrées. Le champ **Relever les** affiche **Personnalisé**.
2. Dans la liste **par**, choisissez les informations secondaires à utiliser dans le rapport.
3. Dans le champ **Afficher**, choisissez le nombre de résultats secondaires à utiliser dans le rapport pour chaque entrée principale.
4. Cliquez sur **Afficher les résultats** pour générer le rapport résumé multi-niveaux.

   Le rapport résumé est mis à jour de manière à n'afficher que le nombre sélectionné d'entrées principales. La liste des entrées secondaires apparaît au-dessous de la barre de chaque entrée principale.
5. Pour modifier l'ordre de tri du rapport, servez-vous des flèches placées à côté des en-têtes de colonne.

Pour revenir à un rapport résumé sur un seul niveau, sélectionnez une autre option dans **Utilisation d'Internet par**. Vous pouvez également cliquer sur l'une des entrées principales ou secondaires et sélectionner une option pour générer un nouveau rapport d'investigation avec ces informations.

Rapports détaillés flexibles

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports résumés*, page 120
- *Rapports résumés multi-niveaux*, page 124
- *Rapports d'investigation favoris*, page 136
- *Planification des rapports d'investigation*, page 138
- *Rapports Cas particuliers*, page 141
- *Sortie dans un fichier*, page 142
- *Connexion à la base de données et paramètres par défaut des rapports*, page 335
- *Colonnes des rapports détaillés flexibles*, page 127

Les rapports détaillés donnent une vue tabulaire des informations de la Base de données d'activité. Accédez à un rapport en vue détaillée à partir de la page principale après avoir consulté un rapport résumé pour lequel vous souhaitez davantage de détails.

Vous pouvez demander une vue détaillée à partir de n'importe quelle ligne. Toutefois, lorsque vous demandez un rapport détaillé basé sur les accès, il est préférable de commencer par une ligne présentant moins de 100 000 accès. Lorsqu'une ligne contient plus de 100 000 accès, la valeur des accès s'affiche en rouge pour vous avertir que l'exécution d'un rapport détaillé peut être très lente.

Le rapport en vue détaillée est considéré comme *flexible* car il vous permet de concevoir votre propre rapport. Vous pouvez en effet ajouter ou supprimer des colonnes d'informations et modifier l'ordre des colonnes affichées. Les informations sont triées en fonction de l'ordre des colonnes. Vous pouvez même inverser l'ordre de tri de n'importe quelle colonne, croissant à décroissant ou vice versa.

Les rapports d'investigation de Websense sont limités par le processeur et la mémoire disponible dans l'ordinateur sur lequel s'exécute Websense Manager, de même que certaines ressources réseau. Les demandes de rapports très volumineux peuvent

provoquer une expiration du délai de connexion. Lorsque vous demandez un rapport volumineux, vous avez la possibilité de générer le rapport sans délai.

> **Important**
> Dans les listes déroulantes ou de valeurs, certaines options peuvent s'afficher en rouge. Cette couleur rouge signale que cette option peut entraîner un rapport très volumineux. Il est généralement plus efficace de tenter de préciser davantage de détails avant de sélectionner cette option.

1. Générez le rapport résumé ou multi-niveaux sur la page principale des rapports d'investigation. (Voir *Rapports résumés*, page 120 ou *Rapports résumés multi-niveaux*, page 124.)
2. Explorez les résultats afin de vous concentrer sur les informations qui vous intéressent directement.

   Lorsque vous générez un rapport sur les accès, il est préférable de naviguer jusqu'à une entrée présentant moins de 100 000 accès avant d'ouvrir le rapport en vue détaillée.
3. Cliquez sur le nombre ou la barre de la ligne que vous souhaitez explorer plus en détails. Pour inclure plusieurs lignes dans un rapport, cochez la case accolée à chaque ligne avant de cliquer sur le nombre ou sur la barre d'une ligne.

   Un message contextuel montre la progression du chargement du rapport détaillé.

   > **Remarque**
   > Si la création du rapport prend du temps, vous pouvez l'enregistrer sous forme de Favori en cliquant sur le lien du message de chargement et planifier une exécution ultérieure. Voir *Rapports d'investigation favoris*, page 136.

4. Vérifiez les informations du rapport initial.

   Les colonnes par défaut varient, selon si vous créez un rapport sur les accès, la bande passante ou le temps de navigation, et selon vos sélections dans la page Options. (Voir *Connexion à la base de données et paramètres par défaut des rapports*, page 335.)
5. Cliquez sur **Modifier le rapport** en haut de la page.

   La liste **Rapport en cours** de la boîte de dialogue Modifier le rapport présente les colonnes affichées dans le rapport détaillé en cours.
6. Sélectionnez un nom de colonne dans la liste **Colonnes disponibles** ou **Rapport en cours** et cliquez sur la flèche droite (>) ou gauche (<) pour déplacer cette colonne vers l'autre liste.

   Choisissez un maximum de 7 colonnes pour le rapport. La colonne présentant la mesure (accès, bande passante, temps de navigation) issue du rapport résumé initial s'affiche toujours le plus à droite. Sa position n'est pas modifiable.

   Consultez la section *Colonnes des rapports détaillés flexibles*, page 127 pour obtenir la liste des colonnes disponibles et leur description.

7. Sélectionnez un nom de colonne dans la liste **Rapport en cours** et utilisez les flèches vers le haut et vers le bas pour modifier l'ordre des colonnes.

   La première colonne de la liste Rapport en cours devient la colonne gauche du rapport.

8. Cliquez sur le lien **Résumé** ou **Détail** situé au-dessus du rapport pour passer d'un affichage à l'autre.

Option	Description
Résumé	Vous devez supprimer la colonne Temps pour afficher un rapport résumé. Les rapports résumés regroupent en une seule entrée tous les enregistrements qui partagent un élément commun. L'élément spécifique varie en fonction des informations utilisées dans le rapport. En général, la colonne située immédiatement à droite avant la mesure présente l'élément résumé.
Détail	L'option Détail présente chaque enregistrement dans une ligne distincte. La colonne Temps peut être affichée.

9. Cliquez sur **Appliquer** pour générer le rapport défini.
10. Servez-vous des options suivantes pour modifier le rapport affiché.
    - Utilisez les options **Afficher** situées au-dessus du rapport pour modifier la période utilisée dans le rapport.
    - Cliquez sur les flèches dirigées vers le haut ou vers le bas d'un en-tête de colonne pour inverser l'ordre de tri de cette colonne et des données associées.
    - Servez-vous des liens **Suivant** et **Précédent** situés au-dessus et au-dessous du rapport pour éventuellement afficher les autres pages du rapport. Par défaut, chaque page contient 100 lignes, que vous pouvez ajuster en fonction de vos besoins. Voir *Options d'affichage et de sortie*, page 337.
    - Cliquez sur l'URL pour ouvrir le site Web demandé dans une nouvelle fenêtre.
11. Cliquez sur **Rapports favoris** si vous souhaitez enregistrer le rapport de manière à pouvoir le générer de nouveau rapidement ou de façon périodique (voir *Enregistrement d'un rapport en tant que Favori*, page 136).

Colonnes des rapports détaillés flexibles

Rubriques connexes :

- *Rapports détaillés flexibles*, page 125
- *Rapports d'investigation favoris*, page 136
- *Planification des rapports d'investigation*, page 138

Le tableau ci-dessous présente les colonnes disponibles dans les rapports détaillés (voir *Rapports détaillés flexibles*, page 125).

Certaines colonnes ne sont pas toujours disponibles. Par exemple, si la colonne Utilisateur est affichée, la colonne Groupe n'est pas disponible. Si la colonne Catégorie est affichée, Classe de risque n'est pas disponible.

Nom de la colonne	Description
Utilisateur	Nom de l'utilisateur à l'origine de la requête. Les informations relatives à l'utilisateur doivent être disponibles dans la Base de données d'activité pour être incluses dans les rapports. Les informations relatives aux groupes ne sont pas disponibles dans les rapports basés sur les utilisateurs.
Jour	Date de création de la requête.
Nom hôte URL	Nom de domaine (également appelé nom d'hôte) du site demandé.
Domaine	Domaine du service d'annuaire du client à base d'annuaire (utilisateur ou groupe, domaine ou unité d'organisation) à l'origine de la requête.
Groupe	Nom du groupe auquel le demandeur appartient. Les noms des utilisateurs individuels ne sont pas donnés dans les rapports basés sur les groupes. Si l'utilisateur qui a demandé le site appartient à plusieurs groupes dans le service d'annuaire, le rapport affiche plusieurs groupes dans cette colonne.
Classe de risques	Classe de risque associée à la catégorie à laquelle le site demandé appartient. Si la catégorie appartient à plusieurs classes de risques, toutes les classes de risques concernées apparaissent dans la liste. Voir *Attribution de catégories aux classes de risque*, page 306.
Objet d'annuaire	Chemin d'accès au répertoire de l'utilisateur à l'origine de la requête, sans nom d'utilisateur. Cela donne généralement plusieurs lignes pour le même trafic car chaque utilisateur appartient à plusieurs chemins d'accès. Si vous utilisez un service d'annuaire non LDAP, cette colonne n'est pas disponible.
Disposition	Action exécutée par Websense en résultat de la requête, par exemple catégorie autorisée ou catégorie bloquée.
Serveur source	Adresse IP de l'ordinateur qui envoie la requête à Filtering Service. Il s'agit de l'ordinateur qui exécute le produit d'intégration ou Websense Network Agent.
Protocole	Protocole de la requête.
Groupe de protocoles	Groupe de la Base de données principale dans lequel se situe le protocole demandé.
IP source	Adresse IP de l'ordinateur à partir duquel la demande a été effectuée.
IP de destination	Adresse IP du site demandé.
URL complète	Nom de domaine et chemin d'accès du site demandé (exemple : http://www.mondomaine.com/produits/elementun/). Si vous ne journalisez pas les URL complètes, cette colonne est vide. Voir *Configuration de la journalisation des URL complètes*, page 326.
Mois	Mois du calendrier au cours duquel la demande a été effectuée.

Nom de la colonne	Description
Port	Port TCP/IP par lequel l'utilisateur a communiqué avec le site.
Bande passante	Quantité de données, en kilo-octets, contenues dans la requête initiale de l'utilisateur et dans la réponse du site Web. Il s'agit du total combiné des valeurs Envoyé et Reçu. N'oubliez pas que certains produits d'intégration n'envoient pas ces informations à Websense. Les pare-feu Check Point FireWall-1 et Cisco PIX Firewall en sont deux exemples. Si votre intégration n'envoie pas ces informations, et que Websense Network Agent est installé, activez l'option **Journaliser les demandes HTTP** de la carte d'interface réseau appropriée pour activer la génération de rapports sur les informations de bande passante. Voir *Configuration des paramètres des cartes réseau*, page 349.
Octets envoyés	Nombre d'octets envoyés dans la requête Internet. Cela représente la quantité de données transmises, pouvant correspondre à une simple demande d'URL, ou d'une soumission plus importante, par exemple si l'utilisateur s'enregistre auprès d'un site Web.
Octets reçus	Nombre d'octets reçus d'Internet en réponse à la requête. Cela comprend l'ensemble du texte, des graphiques et des scripts qui composent le site. Dans le cas des sites bloqués, le nombre d'octets dépend du logiciel qui crée l'enregistrement du journal. Lorsque Websense Network Agent journalise les enregistrements, le nombre d'octets reçus pour un site bloqué correspond à la taille de la page de blocage. Si l'enregistrement de journal est créé par Websense Security Gateway en résultat d'une analyse en temps réel, les octets reçus représentent la taille de la page analysée. Pour plus d'informations sur l'analyse en temps réel, consultez *Analyse du contenu avec les options en temps réel*, page 145. Lorsqu'un autre produit d'intégration crée les enregistrements du journal, les octets reçus pour un site bloqué peuvent correspondre à zéro (0), à la taille de la page bloquée ou à la valeur obtenue du site demandé.
Heure	Heure à laquelle le site a été demandé, au format HH:MM:SS, sur 24 heures.
Catégorie	Catégorie dans laquelle la requête a été filtrée. Cela peut être une catégorie de la Base de données principale Websense ou une catégorie personnalisée.

Rapports Détails de l'activité utilisateur

Rubriques connexes :

- *Rapports d'investigation*, page 118

Cliquez sur le lien **Utilisateur par jour/mois** pour générer un rapport Détails de l'activité d'un utilisateur. Ce rapport illustre graphiquement l'activité Internet de l'utilisateur pour une journée ou un mois complet.

Commencez par générer un rapport pour l'utilisateur spécifique pour un jour sélectionné. À partir de ce rapport, vous pouvez générer un rapport sur l'activité du même utilisateur pour un mois complet. Pour plus d'informations, consultez :

- *Détail de l'activité utilisateur par jour*, page 130
- *Activité utilisateur par mois*, page 131

Détail de l'activité utilisateur par jour

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports Détails de l'activité utilisateur*, page 129
- *Activité utilisateur par mois*, page 131

Le rapport Détail de l'activité utilisateur par jour présente une vue exhaustive de l'activité d'un utilisateur spécifique dans une journée.

1. Sélectionnez **Utilisateur par jour/mois** en haut de la page principale. La boîte de dialogue Activité utilisateur par jour apparaît.
2. Entrez un nom d'utilisateur ou une partie du nom dans le champ **Rechercher un utilisateur**, puis cliquez sur **Rechercher**.

   La recherche présente une liste contenant jusqu'à 100 noms d'utilisateur correspondants issus de la Base de données d'activité.
3. Faites une sélection dans la liste **Sélectionner un utilisateur**.
4. Dans le champ **Sélectionner le jour**, acceptez la dernière date d'activité affichée par défaut ou choisissez une autre date.

   Vous pouvez saisir la nouvelle date ou cliquer sur l'icône du calendrier pour en sélectionner une. La zone de sélection du calendrier indique la plage de dates couverte par la Base de données d'activité active.
5. Cliquez sur **Afficher l'activité quotidienne de l'utilisateur** pour obtenir un rapport détaillé de l'activité de cet utilisateur pour la date demandée.

   Le rapport initial présente la chronologie de l'activité de l'utilisateur par incréments de 5 minutes. Chaque requête est affichée sous forme d'icône, correspondant à une catégorie de la base de données principale Websense. Toutes les catégories personnalisées sont représentées par une seule icône. (La couleur des icônes correspond au regroupement des risques présentés dans les rapports Activité utilisateur par mois. Voir *Activité utilisateur par mois*, page 131.)

   Survolez une icône avec la souris pour afficher l'heure exacte, la catégorie et l'action de la requête associée.

Servez-vous des contrôles énumérés ci-dessous pour modifier l'affichage du rapport ou afficher la légende.

Option	Description
Jour précédent / Jour suivant	Affiche l'activité Internet de cet utilisateur pour le jour suivant ou précédent.
Vue tableau	Affiche la liste de chaque URL demandée, en précisant la date et l'heure de la requête, la catégorie et l'action effectuée (bloquée, autorisée ou autre).
Vue détaillée	Affiche la vue graphique initiale du rapport.
Regrouper les accès similaires / Afficher tous les accès	Combine sur une seule ligne toutes les requêtes survenues à moins de 10 secondes les unes des autres et présentant les mêmes domaine, catégorie et action. La vue résumée des informations est plus courte. Le seuil de temps standard est de 10 secondes. Pour modifier cette valeur, consultez la section *Options d'affichage et de sortie*, page 337. Lorsque vous cliquez sur le lien, ce dernier devient Afficher tous les accès, qui permet de restaurer la liste d'origine de chaque requête.
Afficher les catégories	Affiche la liste de chaque catégorie présente dans le rapport en cours, en indiquant à la fois le nom de la catégorie et l'icône qui la représente. Pour contrôler les catégories affichées dans le rapport, cochez les cases des catégories à inclure. Cliquez ensuite sur **Ok** pour mettre à jour le rapport avec vos sélections.

6. Cliquez sur **Activité utilisateur par mois**, au-dessus du rapport, pour afficher l'activité du même utilisateur pour le mois complet. Pour plus d'informations, consultez *Activité utilisateur par mois*, page 131.

Activité utilisateur par mois

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports Détails de l'activité utilisateur*, page 129
- *Détail de l'activité utilisateur par jour*, page 130
- *Correspondance des catégories*, page 132

Lorsque le rapport Détail de l'activité utilisateur par jour est ouvert, vous pouvez choisir de consulter l'activité mensuelle de cet utilisateur.

1. Ouvrez un rapport Détail de l'activité utilisateur par jour. Voir *Détail de l'activité utilisateur par jour*, page 130.
2. Cliquez sur **Activité utilisateur par mois** en haut.

Le nouveau rapport affiche une image de calendrier, chaque jour étant représenté par un petit bloc coloré correspondant à l'activité Internet de l'utilisateur pour cette journée. Les demandes de sites appartenant aux catégories personnalisées sont indiquées par des blocs gris.

3. Cliquez sur **Légende des catégories de la base de données** en haut et à gauche pour découvrir les correspondances entre les couleurs et les risques potentiels faibles ou élevés pour le site demandé.

   Les affectations de catégories sont fixes et ne peuvent pas être modifiées. Voir *Correspondance des catégories*, page 132.

4. Cliquez sur **Précédent** ou **Suivant** pour afficher l'activité Internet de cet utilisateur pour le mois suivant ou précédent.

Correspondance des catégories

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports Détails de l'activité utilisateur*, page 129
- *Activité utilisateur par mois*, page 131

La liste suivante identifie les catégories représentées par chacune des couleurs dans les rapports Activité utilisateur par jour et Activité utilisateur par mois.

N'oubliez pas que les noms des catégories dans la base de données principale peuvent changer. De plus, des catégories peuvent être ajoutées ou supprimées à tout moment.

Couleur	Catégories
Gris	Catégories personnalisées Trafic non HTTP
Bleu foncé	**Commerce et économie** et toutes ses sous-catégories **Enseignement** et toutes ses sous-catégories **Etat** **Informatique**, y compris les sous-catégories Moteurs de recherche et portails, et Hébergement de sites Web **Divers** sous-catégories Réseaux de diffusion de contenu, Contenu dynamique, Images (Médias), Serveurs d'images et Adresses IP privées **Productivité**/Publicités
Bleu clair	**Drogues**/Médicaments sur Ordonnance **Gouvernement** et sa sous-catégorie Armée **Informatique**/Sites de traduction automatique de pages Web **Divers**, catégorie parente uniquement **Actualités et médias**, catégorie parente uniquement **Événements spéciaux**

Couleur	Catégories
Vert jaune	**Avortement** et toutes ses sous-catégories **Section pour adultes**/ Éducation sexuelle **Bande passante**, y compris les sous-catégories Radio et TV Internet, Sauvegarde et stockage réseau personnels, et Médias en temps réel **Divertissement** et sa sous-catégorie MP3 **Jeux** **Gouvernement**/Organisations politiques **Informatique**/Sécurité informatique **Communication Internet**/Consultation en ligne de courrier électronique **Divers**/Serveurs de téléchargement de fichiers **Divers**/Erreurs réseau **Actualités et médias**/Journaux alternatifs **Productivité**, y compris les sous-catégories Messagerie instantanée, Tableaux d'affichage et forums électroniques, Courtage et commerce en ligne **Religion** et les sous-catégories Religions non traditionnelles, occultes et folklore et Religions traditionnelles **Sécurité**, catégorie parente uniquement **Achats** et toutes ses sous-catégories **Organisations sociales** et toutes ses sous-catégories **Société et styles de vie**, y compris les sous-catégories Homosexuels, lesbiennes et bisexuels, Hobbies, Sites Web personnels et Restaurants **Sports** et toutes ses sous-catégories **Voyage** **Définie par l'utilisateur** **Véhicules**

Couleur	Catégories
Orange	**Section pour adultes**/Nudité **Groupes activistes/Associations** **Bande passante**/Téléphonie Internet **Drogues** et les sous-catégories Abus de drogues, Marijuana et Compléments/Substances non réglementées **Technologies de l'information**/Antiblocage par proxy **Communication Internet** et la sous-catégorie Conversations en ligne **Recherche d'emplois** **Divers**/Non catégorisés **Productivité** sous-catégories Téléchargement de logiciels et de freewares et Sites rémunérateurs **Religion** **Société et style de vie** sous-catégories Alcool et tabac, et Petites annonces personnelles/Rendez-vous amoureux **Mauvais goût** **Armes**
Rouge	**Section pour adultes** et ses sous-catégories : Contenu pour adultes, Lingerie et Maillots de bain et Sexe **Largeur de bande**/Partage de fichiers peer-to-peer (P2P) **Jeux de hasard** **Illégal ou douteux** **Technologies de l'information**/Piratage **Militantisme, extrémisme** **Racisme, haine** **Sécurité** sous-catégories Enregistreurs de frappe, Sites Web dangereux, Phishing et Logiciels espion **Violence**

Rapports standard

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports d'investigation favoris*, page 136
- *Planification des rapports d'investigation*, page 138

Les rapports standard permettent d'afficher rapidement un ensemble particulier d'informations sans qu'il soit nécessaire d'investiguer plus avant.

1. Cliquez sur le lien **Rapports standard** de la page Rapports d'investigation principale.

2. Choisissez le rapport contenant les informations désirées. Les rapports suivants sont disponibles.

Niveaux d'activité les plus élevés
• Quels utilisateurs ont le plus d'accès ? • 10 principaux utilisateurs pour les 10 URL les plus visitées • 5 principaux utilisateurs dans les catégories Shopping, Divertissement et Sports • 5 principales URL pour les 5 catégories les plus visitées
Consommation la plus élevée de bande passante
• Quels groupes consomment le plus de bande passante ? • Groupes consommant le plus de bande passante pour la sous-catégorie Médias en temps réel • Rapport détaillé des URL sur les utilisateurs par perte de bande passante réseau • 10 principaux groupes pour les catégories de bande passante
Temps le plus long en ligne
• Utilisateurs ayant passé le plus de temps en ligne • Quels utilisateurs ont passé le plus de temps sur les sites pour les catégories de productivité ?
Les plus bloqués
• Quels utilisateurs ont été les plus bloqués ? • Quels sites ont été les plus bloqués ? • Rapport détaillé des URL sur les utilisateurs bloqués • 10 principales catégories bloquées
Risque de sécurité le plus élevé
• Catégories principales supposant un risque de sécurité • Principaux utilisateurs du protocole P2P • Principaux utilisateurs des sites pour les catégories de sécurité • URL pour les 10 principales machines avec des logiciels espion
Responsabilité légale
• Risque de responsabilité légale par catégorie • Principaux utilisateurs pour les catégories Section pour adultes

3. Consultez le rapport qui s'affiche.
4. Enregistrez le rapport sous forme de Rapport favori pour le réexécuter régulièrement. Voir *Rapports d'investigation favoris*, page 136.

Rapports d'investigation favoris

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Planification des rapports d'investigation*, page 138

Vous pouvez enregistrer la plupart des rapports d'investigation en tant que **Favoris**. Cela comprend les rapports que vous générez en naviguant jusqu'à des informations spécifiques, les rapports standard et les rapports détaillés que vous avez modifiés en fonction de vos besoins. Exécutez ensuite le rapport favori à tout moment, ou planifiez son exécution à des jours et des heures spécifiques.

Dans les organisations qui utilisent une administration déléguée, l'autorisation d'enregistrer et de planifier des Favoris est définie par le Super administrateur. Les administrateurs qui disposent de cette autorisation peuvent uniquement exécuter et planifier les favoris qu'ils ont enregistrés ; ils n'ont pas accès aux favoris enregistrés par d'autres administrateurs.

Pour plus d'informations sur l'utilisation des rapports favoris, consultez :

- *Enregistrement d'un rapport en tant que Favori*, page 136
- *Création ou suppression d'un rapport Favori*, page 137
- *Modification d'un rapport favori*, page 137

Enregistrement d'un rapport en tant que Favori

Rubriques connexes :

- *Rapports d'investigation favoris*, page 136
- *Modification d'un rapport favori*, page 137

Utilisez la procédure suivante pour enregistrer un rapport en tant que Favori.

1. Créez un rapport d'investigation avec le format et les informations désirés.
2. Cliquez sur **Rapports favoris**.
3. Acceptez ou modifiez le nom proposé par Websense Manager.

   Le nom peut contenir des lettres, des chiffres et des caractères de soulignement (_). Les espaces et les autres caractères spéciaux ne peuvent pas être utilisés.
4. Cliquez sur **Ajouter**.

   Le nom du rapport est ajouté dans la liste des favoris.
5. Sélectionnez un rapport dans cette liste, puis une option de gestion du rapport. Selon l'option choisie, consultez :
   - *Création ou suppression d'un rapport Favori*, page 137

- *Planification des rapports d'investigation*, page 138

Création ou suppression d'un rapport Favori

Rubriques connexes :

- *Rapports d'investigation favoris*, page 136
- *Modification d'un rapport favori*, page 137

Vous pouvez à tout moment générer un rapport favori ou en supprimer un devenu inutile.

1. Cliquez sur **Rapports favoris** pour afficher la liste des rapports enregistrés comme favoris.

   Remarque
   Si votre organisation utilise l'administration déléguée, cette liste ne comprend pas les rapports favoris enregistrés par les autres administrateurs.

2. Sélectionnez le rapport désiré dans la liste.

   Si le rapport désiré n'a pas été enregistré comme favori, consultez la section *Enregistrement d'un rapport en tant que Favori*, page 136.

3. Selon vos besoins :
   - Cliquez sur **Exécuter maintenant** pour générer et afficher le rapport sélectionné immédiatement.
   - Cliquez sur **Planification** pour planifier une exécution ultérieure ou périodique du rapport. Pour plus d'informations, consultez *Planification des rapports d'investigation*, page 138.
   - Cliquez sur **Supprimer** pour supprimer le rapport de la liste des favoris.

Modification d'un rapport favori

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports d'investigation favoris*, page 136

Vous pouvez aisément créer un rapport Favori similaire à un autre rapport favori existant, comme suit.

1. Cliquez sur **Rapports favoris** pour afficher la liste des rapports enregistrés comme favoris.

   Remarque
   Si votre organisation utilise l'administration déléguée, cette liste ne comprend pas les rapports favoris enregistrés par les autres administrateurs.

2. Sélectionnez et exécutez le rapport favori ressemblant le plus au nouveau rapport que vous souhaitez créer. (Voir *Création ou suppression d'un rapport Favori*, page 137.)
3. Modifiez le rapport affiché selon vos besoins.
4. Cliquez sur **Rapports favoris** pour enregistrer le rapport modifié en tant que favori sous un nouveau nom. (Voir *Enregistrement d'un rapport en tant que Favori*, page 136.)

Planification des rapports d'investigation

Rubriques connexes :

- *Rapports d'investigation favoris*, page 136
- *Enregistrement d'un rapport en tant que Favori*, page 136
- *Gestion des tâches de rapports d'investigation planifiés*, page 141

Vous devez enregistrer le rapport d'investigation en tant que favori pour qu'il puisse être planifié pour une exécution ultérieure ou régulière. Lorsque le travail de rapport planifié s'exécute, les rapports résultants sont envoyés par message électronique aux destinataires désignés. Lorsque vous créez des travaux planifiés, tenez compte de la taille et de la quantité de fichiers de rapport joints que peut gérer votre serveur de messagerie.

Les fichiers des rapports planifiés sont automatiquement enregistrés dans le répertoire suivant :

```
<chemin_installation>\webroot\Explorer\<nom>\
```

Le chemin d'installation par défaut est C:\Program Files\Websense. si le travail planifié n'a qu'un destinataire, <nom> correspond à la première partie de l'adresse

électronique (située avant le caractère @). Lorsqu'il existe plusieurs destinataires, les rapports sont enregistrés dans un répertoire appelé Autre.

> **Remarque**
>
> Les rapports enregistrés à partir d'un travail périodique utilisent chaque fois le même nom de fichier. Si vous souhaitez enregistrer les fichiers pour une période plus longue qu'un seul cycle, assurez-vous de modifier le nom du fichier ou de copier ce dernier dans un autre emplacement.
>
> Selon la taille et le nombre de rapports planifiés, ce répertoire peut devenir très volumineux. Assurez-vous de le vider régulièrement, en supprimant tous les fichiers inutiles.

1. Enregistrez un ou plusieurs rapports en tant que Favoris. (Voir *Enregistrement d'un rapport en tant que Favori*, page 136.)
2. Cliquez sur **Rapports favoris** pour afficher la liste des rapports enregistrés comme favoris.

   > **Remarque**
   >
   > Si votre organisation utilise des rôles d'administration déléguée, cette liste ne comprend pas les rapports favoris enregistrés par les autres administrateurs.

3. Mettez en surbrillance jusqu'à 5 rapports à exécuter dans le cadre du travail.
4. Cliquez sur **Planification** pour créer un travail de rapport planifié, puis saisissez les informations demandées dans la page Planifier le rapport.

   Il est préférable de planifier les tâches de rapport à des heures et des jours différents pour éviter une surcharge de la Base de données d'activité et de ralentir les performances de la journalisation et de la création interactive des rapports.

Champ	Description
Récurrence	Sélectionnez la fréquence (Une fois, Quotidien, Hebdomadaire, Mensuel) d'exécution du travail de rapport.
Date de début	Choisissez le jour de la semaine ou la date à laquelle le travail doit s'exécuter pour la première fois (ou pour la seule fois).
Heure d'exécution	Définissez l'heure d'exécution du travail.
Ecrire un message à	Utilisez le champ **Adresses de courrier électronique supplémentaires** pour ajouter les adresses appropriées dans cette liste. Mettez une ou plusieurs adresses électroniques en surbrillance pour recevoir les rapports du travail. (N'oubliez pas de désélectionner les adresses qui ne doivent pas recevoir les rapports.)

Champ	Description
Adresses de courrier électronique supplémentaires	Entrez une adresse électronique, puis cliquez sur **Ajouter** pour la placer dans la liste **Ecrire un message à**. La nouvelle adresse électronique est automatiquement surlignée avec les autres adresses électroniques sélectionnées.
Personnaliser l'objet et le corps du texte du courrier électronique	Cochez cette case pour personnaliser la ligne d'objet de votre notification électronique et le corps du message. Si cette case n'est pas activée, l'objet et le texte par défaut seront utilisés.
Objet du courrier électronique	Entrez le texte devant apparaître dans la ligne d'objet du message électronique lors de l'envoi des rapports planifiés. L'objet par défaut du message électronique est : Tâche de planification des rapports d'investigation
Texte du courrier électronique	Entrez le texte à ajouter dans le message électronique des rapports planifiés envoyés. Le message est identique à celui présenté ci-dessous, votre texte remplaçant le <TEXTE PERSONNALISÉ>. Le planificateur de rapports a généré le ou les fichiers joints le <date/heure>. <TEXTE PERSONNALISÉ> Pour afficher le ou les rapports générés, cliquez sur le ou les liens suivants. Remarque : le lien ne fonctionne pas si le destinataire n'a pas accès au serveur Web d'où provient le travail.
Planifier le nom de la tâche	Attribuez un nom unique au travail planifié. Le nom identifie ce travail dans la file d'attente des tâches. Voir *Gestion des tâches de rapports d'investigation planifiés*, page 141.
Format de sortie	Choisissez le format du fichier des rapports planifiés : **PDF** : Les fichiers PDF s'affichent dans Adobe Reader. **Excel** : Les fichiers XLS s'affichent dans Microsoft Excel.
Intervalle de dates	Définissez la plage de dates couverte par les rapports de ce travail. **Toutes les dates** : toutes les dates disponibles dans la Base de données d'activité. **Relatif** : choisissez une période (Jours, Semaines ou Mois) et la période spécifique à inclure (Ce(tte), Dernier(ère)(s), Deux dernier(ère)s, etc.). **Spécifique** : définissez les dates ou une plage de dates spécifiques pour les rapports de ce travail.

5. Cliquez sur **Suivant** pour ouvrir la page Confirmation de planification.
6. Cliquez sur **Enregistrer** pour enregistrer vos sélections et ouvrir la page File d'attente de tâches (voir *Gestion des tâches de rapports d'investigation planifiés*, page 141).

Gestion des tâches de rapports d'investigation planifiés

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Planification des rapports de présentation*, page 110

Lorsque vous créez un travail planifié pour des rapports d'investigation, la page **File d'attente de tâches** s'affiche et présente le nouveau travail et la liste des travaux planifiés existants. Vous pouvez également accéder cette page en cliquant sur le lien **File d'attente de tâches** de la page principale des rapports d'investigation.

> **Remarque**
> Si votre organisation utilise l'administration déléguée, cette page ne présentent pas les tâches planifiées par les autres administrateurs.

La section **Planifier le rapport détaillé** présente la liste des travaux planifiés dans l'ordre de leur création en indiquant le planning défini et l'état de chaque travail. Les options suivantes sont également disponibles.

Option	Description
Éditer	Présente le planning défini pour ce travail et vous permet de le modifier si nécessaire.
Supprimer	Supprime le travail et ajoute l'entrée dans la section Journal d'état en désignant le travail comme Supprimé.

La section **Journal d'état** présente la liste des travaux qui ont été modifiés, en indiquant l'heure de début planifiée du travail, l'heure de fin réelle et l'état.

Cliquez sur **Effacer le journal d'état** pour supprimer toutes les entrées de la section Journal d'état.

Rapports Cas particuliers

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Rapports résumés*, page 120

Un rapport Cas particuliers présente les utilisateurs dont l'activité Internet est la plus hors norme dans la base de données. Websense calcule l'activité moyenne de tous les utilisateurs par catégorie, par jour, par action (parfois appelée disposition) et par protocole. Il affiche ensuite l'activité des utilisateurs qui s'écartent le plus de cette

moyenne statistique. L'écart est calculé en tant qu'écart standard par rapport à la moyenne.

1. Dans la page principale des rapports d'investigation, créez un rapport résumé contenant les informations pour lesquelles vous souhaitez connaître les cas particuliers. Les sélections des rapports soulignées et présentées en bleu à côté du champ 'Utilisation d'Internet par' se reflètent dans le rapport Cas particuliers.

   Par exemple, pour afficher les cas particuliers par accès pour une catégorie spécifique, sélectionnez **Catégorie** dans la liste **Utilisation d'Internet par** et **Accès** en tant que **Mesure**.

   > **Remarque**
   > Les rapports de cas particuliers ne sont pas générés pour le temps de navigation. Si vous partez d'un rapport résumé présentant le temps de navigation, le rapport Cas particuliers est basé sur les accès.

2. Cliquez sur **Cas particuliers**.

   Les lignes sont triées par ordre décroissant, l'écart le plus important étant affichant en premier. Chaque ligne indique :

   - Le Total (accès ou bande passante) pour l'utilisateur, la catégorie, le protocole, le jour et l'action
   - La Moyenne (accès ou bande passante) pour tous les utilisateurs, cette catégorie, ce protocole, ce jour et cette action
   - Le décalage de l'utilisateur par rapport à la moyenne

3. Pour afficher l'activité dans le temps d'un utilisateur individuel dans cette catégorie, cliquez sur le nom de l'utilisateur.

   Par exemple, si l'activité d'un utilisateur est sensiblement élevée un certain jour, cliquez sur le nom de cet utilisateur pour afficher un rapport permettant de mieux comprendre son activité générale.

Sortie dans un fichier

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Impression des rapports d'investigation*, page 143

Après la création d'un rapport d'investigation, vous pouvez utiliser les boutons situés au-dessus du rapport pour l'enregistrer dans un fichier. Le bouton sur lequel vous cliquez détermine le format du fichier.

Option	Description
	Enregistre le rapport au format XLS. Si Microsoft Excel 2003 ou une version ultérieure est installée sur l'ordinateur à partir duquel vous accédez à Websense Manager, vous êtes invité(e) à afficher ou à enregistrer le rapport. Autrement, vous êtes invité(e) à sélectionner un répertoire et le nom de fichier du rapport enregistré. Servez-vous des options de Microsoft Excel pour imprimer, enregistrer ou envoyer le rapport par courrier électronique.
	Crée un rapport au format PDF. Si Adobe Reader v7.0 ou une version ultérieure est installée sur l'ordinateur à partir duquel vous accédez à Websense Manager, vous êtes invité(e) à afficher ou à enregistrer le rapport. Autrement, vous êtes invité(e) à sélectionner un répertoire et le nom de fichier du rapport enregistré. Servez-vous des options d'Adobe Reader pour imprimer, enregistrer ou envoyer le rapport par courrier électronique.

Impression des rapports d'investigation

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Sortie dans un fichier*, page 142

Pour imprimer les rapports d'investigation :

- Utilisez la fonction d'impression du navigateur Web lorsque le rapport est affiché.
- Créez un fichier PDF ou XLS, puis utilisez la fonction d'impression d'Adobe Reader ou de Microsoft Excel (voir *Sortie dans un fichier*, page 142).

Bien que les rapports d'Explorer aient été configurés pour s'imprimer depuis le navigateur, vous pouvez tester l'impression pour vérifier le résultat.

Les rapports Activité utilisateur par mois sont configurés pour une impression au format paysage. Tous les autres rapports sont configurés pour une impression en mode portrait.

Lorsque vous créez votre propre rapport (voir *Rapports détaillés flexibles*, page 125), la largeur des colonnes diffère selon les informations incluses. L'orientation de la page passe en mode paysage lorsque le rapport dépasse le format A4 (21,59 x 27,49 cm).

La largeur du contenu de la page est de 184 mm ou de 254 mm. Dans le cas du format A4, les marges sont légèrement plus étroites mais restent dans la zone imprimable. (La taille du papier par défaut est Lettre, ou 21,59 x 27,49 cm). Si vous utilisez du papier

A4, assurez-vous de modifier ce paramètre dans le fichier wse.ini. Voir *Options d'affichage et de sortie*, page 337.)

Rapports sur activité propre

Rubriques connexes :

- *Rapports d'investigation*, page 118
- *Configuration des préférences de génération de rapports*, page 308
- *Rapports sur activité propre*, page 339

Les rapports sur activité propre de Websense vous permettent d'évaluer vos propres activités Internet et de les ajuster, si nécessaire, pour vous rapprocher des directives de votre organisation. Ils respectent également la législation qui exige que les organisations autorisent les utilisateurs à savoir quels types d'informations les concernant sont collectées.

Si les rapports sur activité propre sont activés dans votre organisation, vous pouvez y accéder depuis votre navigateur :

1. Entrez l'URL fournie par votre administrateur Websense ou cliquez sur le lien Rapports sur activité propre de la page de connexion principale de Websense Manager pour accéder à la page de connexion des rapports sur activité propre.
2. Si le serveur **Policy Server** présente une liste déroulante, choisissez l'adresse IP du Policy Server qui journalise les informations de votre activité Internet.

   Au besoin, demandez l'aide de votre administrateur Websense.
3. Entrez le **Nom d'utilisateur** et le **Mot de passe** que vous utilisez pour vous connecter au réseau.
4. Cliquez sur **Se connecter**.

Websense Manager affiche un rapport d'investigation présentant votre activité Internet par classe de risques. Cliquez sur les différents liens et éléments de la page pour accéder aux différentes options d'affichage des informations stockées sur votre activité. Servez-vous du système d'**Aide** pour obtenir de l'assistance lorsque vous utilisez les rapports.

7 Analyse du contenu avec les options en temps réel

Rubriques connexes :

- *Options d'analyse*, page 147
- *Catégorisation du contenu et analyse des menaces*, page 148
- *Analyse des fichiers*, page 149
- *Découpage du contenu*, page 151
- *Création de rapports sur l'activité d'analyse en temps réel*, page 153

Le filtrage Websense filtre l'activité Internet en fonction de la stratégie active et des informations stockées dans la base de données principale. Si vous êtes abonné(e) à Websense Content Gateway ou à Websense Web Security Gateway, vous pouvez également analyser le contenu des sites Web et des fichiers en temps réel.

Selon votre abonnement, 2 options d'analyse en temps réel sont disponibles : la catégorisation du contenu et l'analyse en temps réel de la sécurité.

- La **catégorisation du contenu** permet de vérifier le contenu des URL qui ne sont pas réellement bloquées (en fonction de la stratégie active et de la catégorisation des URL dans la base de données principale Websense) et de renvoyer une catégorie à utiliser pour le filtrage.
- Si vous vous abonnez à Websense Web Security Gateway, 3 options d'**analyse de la sécurité en temps réel** sont disponibles.
  - L'**Analyse du contenu** recherche dans le contenu Web des menaces pour la sécurité, telles que le phishing, la redirection d'URL, les exploits Web et l'antiblocage par proxy.
  - L'**Analyse de fichier** examine le contenu des fichiers pour identifier une catégorie de menaces telle que des virus, des Chevaux de Troie ou des vers.
  - Le **Découpage du contenu** supprime du contenu actif dans les pages Web demandées.

Lorsque l'une de ces options est activée, seuls les sites qui ne sont **pas** déjà bloqués par la stratégie active et leur classement dans la base de données principale Websense sont analysés. Pour plus d'informations, consultez *Options d'analyse*, page 147.

> **Important**
>
> Les filtres d'accès limité et les URL non filtrées remplacent la catégorisation en temps réel.
>
> Si l'utilisateur demande un site présent dans un filtre d'accès limité actif (voir *Restriction des utilisateurs à une liste définie de sites Internet*, page 168) ou dans la liste des URL non filtrées (voir *Redéfinition du filtrage pour des sites spécifiques*, page 182), la requête est autorisée, même lorsqu'une analyse en temps réel est effectuée et que des menaces sont identifiées.

Pour tirer parti de ces fonctions de sécurité en temps réel, entrez une clé d'abonnement incluant la prise en charge de Websense Content Gateway ou de Websense Web Security Gateway en deux emplacements :

- Dans Websense Manager (sélectionnez **Paramètres > Compte**).
- Dans l'interface de gestion de Websense Content Gateway (sélectionnez l'onglet **Configurer > Mon Proxy > Abonnement > Gestion des abonnements**).

Il faudra quelques minutes aux deux produits pour télécharger les bases de données nécessaires, effectuer la synchronisation et afficher toutes les fonctions en temps réel dans les deux outils de gestion.

Option d'analyse en temps réel de Websense

Les options d'analyse en temps réel de Websense renforcent la sécurité du réseau. Servez-vous de ces options pour analyser le contenu Internet et l'affecter à une catégorie de filtrage. Le résultat de l'analyse en temps réel est envoyé à Filtering Service, qui filtre le site en fonction de l'action attribuée à son classement dans la stratégie active.

Téléchargement des bases de données

Les options d'analyse en temps réel s'appuient sur de petites bases de données installées en même temps que Websense Web Security Gateway, qui vérifie la présence de mise à jour de ces bases de données à intervalles réguliers. Les mises à jour de ces bases de données sont indépendantes des mises à jour de la base de données principale (y compris des mises à jour de la base de données en temps réel et des mises à jour de la sécurité en temps réel).

Chaque fois que vous utilisez la commande **./WCGAdmin start** pour démarrer Websense Security Gateway, un téléchargement des bases de données démarre. Si le téléchargement échoue, une nouvelle tentative intervient toutes les 15 minutes jusqu'à la réussite de l'opération.

L'intervalle par défaut de vérification de la présence de mises à jour des bases de données est de 15 minutes. Pour modifier cet intervalle, modifiez la valeur **PollInterval** dans le fichier **/opt/bin/downloadservice.ini** sur l'ordinateur Websense Content Gateway.

Après avoir modifié le fichier **downloadservice.ini**, arrêtez et redémarrez Websense Content Gateway à partir de la ligne de commande.

- Pour arrêter, entrez : **/opt/WCG/WCGAdmin stop**
- Pour redémarrer, entrez : **/opt/WCG/WCGAdmin start**

Options d'analyse

La page **Paramètres > Analyse en temps réel** permet d'activer et de configurer les options de l'analyse en temps réel. Les différentes options d'analyse sont détaillées dans les sections suivantes.

- *Catégorisation du contenu et analyse des menaces*, page 148
- *Analyse des fichiers*, page 149
- *Découpage du contenu*, page 151

Pour chaque option, deux choix sont disponibles :

- **Désactivé.** aucun blocage ou analyse en temps réel n'intervient. Cette option n'assure aucune sécurité supplémentaire.
- **Recommandé** ou **Activé.** Si votre site est configuré pour une analyse en temps réel, ce paramètre vous assure les meilleures performances. Les analyses sont effectuées en fonction de deux facteurs :
  - Des listes Toujours analyser et Ne jamais analyser de l'onglet **Paramètres > Analyse en temps réel > Exceptions** (voir *Affinage de l'analyse*, page 152).
  - De l'identification du site par Websense comme incluant du contenu dynamique. Les sites désignés comme comprenant du contenu dynamique sont analysés. Le marqueur qui identifie un site comme comprenant du contenu dynamique n'est pas configurable par l'utilisateur.

    Les sites de contenu dynamique qui apparaissent dans la liste Ne jamais analyser ne sont pas analysés.
- **Tous.** Toutes les pages Web demandées sont analysées. Les seules exceptions sont celles qui apparaissent dans la liste Ne jamais analyser.

Cette option assure une sécurité maximale, mais peut ralentir significativement les performances du système.

Avertissement

Les sites présents dans la liste Ne jamais analyser ne sont analysés en aucune circonstance. Si un site de la liste Ne jamais analyser est compromis, les options de l'analyse en temps réel n'analysent pas et ne détectent pas le code malveillant.

Catégorisation du contenu et analyse des menaces

Rubriques connexes :

- *Options d'analyse*, page 147
- *Analyse des fichiers*, page 149
- *Découpage du contenu*, page 151
- *Affinage de l'analyse*, page 152
- *Création de rapports sur l'activité d'analyse en temps réel*, page 153

Le contenu Web change rapidement. Les statistiques révèlent qu'une importante majorité du contenu Web est dynamique. En outre, Internet héberge de plus en plus de contenu généré par l'utilisateur, tel que celui des sites de réseautage personnel. Ces matériaux ne sont pas soumis aux directives de contenu et de style qui régissent les sites Web d'entreprise.

Lorsque la catégorisation du contenu est activée, les sites sélectionnés sont classés en temps réel et la catégorie qui en résulte est transmise au logiciel de filtrage Websense pour être bloquée ou autorisée en fonction de la stratégie active.

Important

Si vous prévoyez de créer des rapports sur l'activité de l'analyse en temps réel, activez la journalisation des URL complètes (voir *Configuration de la journalisation des URL complètes*, page 326), sinon les enregistrements du journal ne contiendront que le domaine (www.domaine.com) des sites catégorisés et les pages individuelles d'un site peuvent appartenir à des catégories différentes.

Si votre site utilise WebCatcher pour signaler les URL non catégorisées à Websense, Inc. (voir *Configuration de WebCatcher*, page 318), les URL catégorisées via la catégorisation du contenu sont transmises pour être ajoutées dans la base de données principale.

Si votre abonnement comprend Websense Security Gateway, vous pouvez également spécifier que les sites soient analysés par rapport aux menaces pour la sécurité.

La page **Paramètres > Analyse en temps réel > Options communes** permet de spécifier à quel moment l'analyse et la catégorisation du contenu doivent être utilisées.

1. Dans la section Catégorisation du contenu, sélectionnez **Désactivé** ou **Activé** (par défaut) pour déterminer si l'analyse est exécutée. Voir *Options d'analyse*, page 147.

   Une fois que la catégorie est déterminée, toutes les autres options d'analyse en temps réel configurées sont appliquées pour assurer une sécurité supplémentaire.
2. (*Websense Security Gateway*) Dans la section Analyse du contenu, sélectionnez **Désactivé** (par défaut), **Recommandé** ou **Tous** pour déterminer le niveau de l'analyse.
3. Procédez de l'une des manières suivantes :
   - Pour ajouter des sites dans les listes Ne jamais analyser ou Toujours analyser, sélectionnez l'onglet **Exceptions**. Voir *Affinage de l'analyse*, page 152.
   - Pour modifier les paramètres des autres options d'analyse en temps réel, continuez à la page **Options communes**. Voir *Analyse des fichiers*, page 149 et *Découpage du contenu*, page 151.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Les rapports de présentation peuvent fournir des détails sur les tentatives d'accès aux sites contenant des menaces. Pour plus d'informations sur l'exécution des rapports Websense, consultez la section *Rapports de présentation*, page 98.

Analyse des fichiers

Rubriques connexes :

- *Options d'analyse*, page 147
- *Catégorisation du contenu et analyse des menaces*, page 148
- *Découpage du contenu*, page 151
- *Affinage de l'analyse*, page 152
- *Création de rapports sur l'activité d'analyse en temps réel*, page 153

L'analyse des fichiers examine le contenu des fichiers exécutables entrants que les utilisateurs tentent de télécharger ou d'ouvrir à distance. Cette option de l'analyse en temps réel renvoie une catégorie au logiciel de filtrage Websense de sorte que le fichier soit autorisé ou bloqué de manière appropriée.

La meilleure pratique consiste à analyser tous les fichiers **exécutables** (par exemple les fichiers **.exe** et **.dll**). Vous pouvez également identifier d'autres types de fichiers à analyser et définir une taille maximale d'analyse.

> **Remarque**
> Seuls les fichiers des applications portables Windows 32 bits sont analysés.

La page **Paramètres > Analyse en temps réel > Options communes** permet de spécifier à quel moment l'analyse des fichiers doit être utilisée.

1. Dans la section Analyse des fichiers, sélectionnez **Off**, **Recommandé** (par défaut) ou **Tous** pour déterminer le niveau de l'analyse. Voir *Options d'analyse*, page 147.
2. Cliquez sur **Paramètres avancés**.
3. L'option **Analyser tous les types de fichiers ayant un contenu exécutable** est activée par défaut. Désactiver cette case à cocher si vous préférez définir des extensions de fichiers individuelles à analyser.
4. Pour spécifier d'autres types de fichiers à analyser, entrez l'extension du fichier (par exemple **ppt** ou **wmv**), puis cliquez sur **Ajouter**. L'extension du fichier ne peut contenir que des caractères alphanumériques, des caractères de soulignement (_) ou des tirets (-). N'incluez pas le point qui précède l'extension.

   Pour supprimer une extension de la liste des extensions de fichiers sélectionnées, sélectionnez-la, puis cliquez sur **Supprimer**.
5. Sous Options, entrez la taille maximale des fichiers à analyser (par défaut, 10 Mo). Sélectionnez **Personnaliser** pour entrer une taille allant jusqu'à 4 096 Mo (4 Go). Les fichiers dont la taille dépasse la taille spécifiée ne sont pas analysés.
6. Procédez de l'une des manières suivantes :
   - Pour ajouter des sites dans les listes Ne jamais analyser ou Toujours analyser, sélectionnez l'onglet **Exceptions**. Voir *Affinage de l'analyse*, page 152.
   - Pour modifier les paramètres des autres options de l'analyse en temps réel, passez à l'onglet **Options communes**. Voir *Catégorisation du contenu et analyse des menaces*, page 148 et *Découpage du contenu*, page 151.
7. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Plusieurs rapports de présentation fournissent des détails sur les tentatives de téléchargement de fichiers contenant des menaces. Pour plus d'informations sur l'exécution des rapports Websense, consultez la section *Rapports de présentation*, page 98.

Pour plus d'informations sur le blocage des fichiers en fonction du type et de la catégorie d'URL, consultez la section *Gestion du trafic en fonction du type de fichiers*, page 193.

Découpage du contenu

Rubriques connexes :

- *Options d'analyse*, page 147
- *Catégorisation du contenu et analyse des menaces*, page 148
- *Analyse des fichiers*, page 149
- *Affinage de l'analyse*, page 152
- *Création de rapports sur l'activité d'analyse en temps réel*, page 153

Les menaces pesant sur votre système peuvent être cachées dans le contenu actif envoyé par l'intermédiaire de pages Web. Faire en sorte qu'un tel contenu n'arrive jamais dans votre système est un moyen de préserver l'intégrité de votre réseau.

Les options d'analyse en temps réel de Websense permettent de spécifier que le contenu rédigé en certains langages de programmation (ActiveX, JavaScript ou VB Script) soit supprimé des pages Web entrantes. Lorsque le découpage du contenu est activé, l'ensemble du contenu écrit dans les langages de programmation spécifiés sont supprimés des sites désignés comme comprenant du contenu dynamique ou apparaissant dans la liste Toujours analyser (voir *Options d'analyse*, page 147).

Le découpage du contenu intervient seulement après la catégorisation du site par les options de l'analyse en temps réel et l'identification par Websense des stratégies devant s'appliquer.

Important

Les pages Web qui dépendent du contenu actif supprimé ne fonctionneront pas comme prévu. Pour autoriser un accès total aux sites comprenant du contenu actif, désactivez le découpage du contenu ou ajoutez les sites dans la liste Ne jamais analyser.

L'utilisateur qui demande une page de contenu actif ne reçoit pas de notification de suppression de contenu.

La page **Paramètres > Analyse en temps réel > Options communes** permet de spécifier à quel moment le contenu des sites de contenu dynamique doit être découpé.

1. Dans la section Découpage du contenu, sélectionnez les types de contenu actif devant être supprimés des pages Web entrantes.
2. Pour modifier les paramètres des autres options de l'analyse en temps réel, consultez les sections :
   - *Catégorisation du contenu et analyse des menaces*, page 148
   - *Analyse des fichiers*, page 149.

3. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour désactiver le découpage du contenu de l'un des langages sélectionnés, désactivez la case à cocher associée.

Affinage de l'analyse

Rubriques connexes :

- *Options d'analyse*, page 147
- *Catégorisation du contenu et analyse des menaces*, page 148
- *Analyse des fichiers*, page 149
- *Découpage du contenu*, page 151

Servez-vous des listes Toujours analyser et Ne jamais analyser pour personnaliser le comportement des options d'analyse Recommandé et Tous.

- Lorsqu'une option d'analyse en temps réel est définie sur Recommandé ou sur Activé, les sites de contenu dynamique et les sites de la liste Toujours analyser sont analysés (voir *Options d'analyse*, page 147). Les sites de la liste Ne jamais analyser sont ignorés.
- Lorsqu'une option d'analyse en temps réel est définie sur Tous, les sites de la liste Ne jamais analyser sont ignorés. Cette option peut améliorer les performances.

Utilisez la liste Ne jamais analyser avec précaution. Lorsqu'un site de cette liste est compromis, Websense Security Gateway ne l'analyse pas pour résoudre le problème de sécurité.

Pour renseigner et modifier les listes Toujours analyser et Ne jamais analyser, utilisez la page **Paramètres > Analyse en temps réel > Exceptions**.

Pour ajouter des sites dans la liste Toujours analyser ou Ne jamais analyser :

1. Entrez les noms des sites dans la zone **URL**.

   Entrez uniquement le nom d'hôte (par exemple, **cesite.com**). Il n'est pas nécessaire d'entrer l'URL complète. Veillez à entrer à la fois le domaine et l'extension ; **cesite.com** et **cesite.net** sont des entrées distinctes.

   Vous pouvez entrer plusieurs noms d'hôte à la fois.
2. Dans la colonne **Options**, sélectionnez les options d'analyse en temps réel devant s'appliquer à tous les sites saisis. Vous pouvez sélectionner une ou plusieurs options. Remarquez que **Risques de sécurité** ne fait référence qu'à l'analyse du contenu, pas à l'analyse des fichiers. L'analyse des fichiers n'est pas affectée par les listes Toujours analyser et Ne jamais analyser.

Pour appliquer des options différentes aux différents sites, entrez les sites séparément.

3. Sélectionnez **Ajouter à Toujours analyser** ou **Ajouter à Ne jamais analyser**.

   Un même site ne peut apparaître que dans l'une des deux listes. Par exemple, vous ne pouvez pas spécifier que le même site doit toujours être analysé pour la présence de menaces et jamais pour le découpage du contenu.

   - Pour changer un site de liste, commencez par le sélectionner, puis utilisez les flèches droite (>) et gauche (>) pour le déplacer vers une nouvelle liste.
   - Pour supprimer un site d'une liste, sélectionnez-le, puis cliquez sur **Supprimer**.

4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour modifier les options d'analyse associées à un site :

1. Sélectionnez le site dans la liste Toujours analyser ou Ne jamais analyser, puis cliquez sur **Éditer**.
2. Dans la zone Modifier les règles, sélectionnez de nouvelles options pour ce nom d'hôte :
   - **Aucune modification** conserve le paramètre actuel.
   - **Activé** indique que le contenu est analysé pour l'option spécifiée, par exemple pour la catégorisation de contenu.
   - **Dasactivé** indique qu'aucune analyse n'intervient pour l'option spécifiée. Lorsqu'une option est désactivée, les performances peuvent s'améliorer, mais la sécurité peut être compromise.
3. Lorsque vos sélections sont terminées, cliquez sur **OK** dans la zone Modifier les règles pour revenir dans l'onglet Exceptions.
4. Cliquez de nouveau sur **OK** pour mettre en cache vos modifications. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Création de rapports sur l'activité d'analyse en temps réel

Rubriques connexes :

- *Options d'analyse*, page 147
- *Catégorisation du contenu et analyse des menaces*, page 148
- *Analyse des fichiers*, page 149
- *Découpage du contenu*, page 151

Si votre abonnement comprend les fonctions d'analyse en temps réel, vous pouvez analyser les effets de ces fonctions avec les rapports de présentation et d'investigation.

La page Rapports de présentation propose un groupe de rapports appelés Risques de sécurité en temps réel. Ces rapports se concentrent de façon spécifique sur l'activité liée aux menaces. Comme pour tous les rapports de présentation, vous pouvez copier un rapport de menace de la sécurité et en modifier le filtre pour cibler les informations incluses lorsque vous créez un rapport à partir de cette copie.

Certains rapports de menaces de la sécurité comprennent une colonne ID de la menace. Vous pouvez cliquer sur l'identifiant de la menace pour ouvrir une page Websense Security Labs décrivant le type de menace identifié.

De plus, d'autres rapports de présentation contiennent des informations sur les activités d'analyse en temps réel et sur les activités de filtrage standard. Copiez un rapport prédéfini et modifiez son filtre pour créer un rapport propre aux activités d'analyse en temps réel.

Important

Pour vous assurer que les rapports sur l'activité d'analyse en temps réel soient significatifs, activez la journalisation des URL complètes (voir *Configuration de la journalisation des URL complètes*, page 326), sinon les rapports ne pourront afficher que le domaine (www.domaine.com) du site catégorisé, même si les pages individuelles d'un site appartiennent à des catégories différentes ou contiennent des menaces différentes.

Par exemple, le rapport Détails des URL complètes par catégorie, situé dans le groupe Activité Internet du Catalogue des rapports, fournit la liste détaillée de chaque URL consultée dans chaque catégorie. Pour créer un rapport spécifique à l'analyse en temps réel, copiez le rapport Détails des URL complètes par catégorie et modifiez son filtre. Dans l'onglet Actions, sélectionnez uniquement les actions autorisées et bloquées liées à l'analyse en temps réel. Dans l'onglet Options, modifiez le titre du catalogue des rapports et le nom du rapport de manière à l'identifier comme rapport d'analyse en temps réel. Par exemple, vous pouvez lui donner le nom et le titre Analyse en temps réel : Détails des URL complètes par catégorie.

Les rapports d'investigation permettent également d'obtenir un aperçu des activités d'analyse en temps réel.

1. Dans la liste déroulante **Utilisation d'Internet par**, sélectionnez Action.
2. Dans le rapport résultant, cliquez sur une action en temps réel, telle que Catégorie bloquée en temps réel, pour afficher la liste des options d'exploration.
3. Cliquez sur l'option d'exploration désirée, par exemple Catégorie ou Utilisateur.
4. Cliquez sur la valeur Accès ou sur la barre de l'une des lignes pour voir les détails associés.
5. Cliquez sur **Modifier le rapport**, en haut de la page, pour ajouter la colonne URL complète dans le rapport.

Pour plus d'informations sur l'utilisation des fonctions de rapports d'investigation, consultez la section *Rapports d'investigation*, page 118.

Journalisation de l'analyse en temps réel

Lorsque vous utilisez des options d'analyse en temps réel, sachez que la journalisation de l'activité de filtrage Web standard diffère de celle de l'activité d'analyse en temps réel.

Dans le cas du filtrage Web standard, plusieurs options permettent de réduire la taille de la base de données d'activité.

- Activez **visites** pour n'enregistrer dans le journal qu'un enregistrement pour chaque site Web demandé. Voir *Configuration des fichiers cache du journal*, page 315.
- Activez **consolidation** pour combiner dans un seul enregistrement de journal plusieurs requêtes comportant des éléments communs. Voir *Configuration des options de consolidation*, page 316.
- Désactivez **Enregistrement d'URL complète** pour ne journaliser que le nom de domaine (www.domaine.com) de chaque requête, et non le chemin d'accès conduisant à une page spécifique du domaine (/produits/produitA). Voir *Configuration de la journalisation des URL complètes*, page 326.
- Activez **Journalisation de catégories spécifiques** pour limiter la journalisation aux catégories sélectionnées essentielles pour votre organisation. Voir *Configuration de Filtering Service pour la journalisation*, page 308.

De leur côté, les fonctions d'analyse en temps réel ne sont liées que partiellement à ces paramètres. Lorsqu'un site est analysé en temps réel, deux enregistrements de journal distincts sont créés.

- Les **enregistrements de filtres Web** tirent parti des paramètres de réduction de taille éventuellement implémentés et sont disponibles pour tous les rapports de filtrage Web.
- Les **enregistrements d'analyse en temps réel** ignorent la plupart des paramètres de réduction de taille. Chaque accès distinct est journalisé, les requêtes de toutes les catégories sont journalisées et aucun enregistrement n'est consolidé. Un enregistrement d'analyse en temps réel est généré, que le site soit bloqué ou autorisé en résultat de l'analyse en temps réel. Seul le paramètre de journalisation des URL complètes est respecté pour les enregistrements d'analyse en temps réel.

Si vous avez activé des options de réduction de taille de la base de données d'activité, il est possible que les chiffres présentés dans les rapports d'analyse en temps ne correspondent **pas** aux chiffres présentés dans les rapports de filtrage standard, même lorsque ces rapports sont configurés pour les mêmes utilisateurs, périodes et catégories. Par exemple, si vous avez choisi de journaliser les visites et qu'un utilisateur demande un site analysé par les fonctions d'analyse en temps réel, cette requête prend la forme d'une seule visite dans les rapports de filtrage standard, mais peut se traduire par plusieurs accès dans les rapports d'analyse en temps réel.

Pour obtenir des données comparables pour le filtrage standard et l'analyse en temps réel, **désactivez** les paramètres de réduction de taille de la base de données d'activité. Comme il peut en résulter une base de données très volumineuse, assurez-vous que

l'ordinateur de la base de données d'activité dispose de suffisamment d'espace disque, de capacité de traitement et de mémoire.

Pour plus d'informations sur la configuration des paramètres de réduction de taille, consultez la section *Administration de la génération de rapports*, page 303. Pour plus d'informations sur la création des rapports, consultez les sections *Rapports de présentation*, page 98 et *Rapports d'investigation*, page 118.

8 Filtrage des clients distants

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *Configuration des paramètres de Remote Filtering*, page 164

La plupart des organisations ont des utilisateurs qui emmènent parfois leur ordinateur portable hors du réseau. Dans le cas des utilisateurs distants qui exécutent le système d'exploitation Microsoft Windows, vous pouvez filtrer les requêtes Internet en implémentant Websense Remote Filtering, une fonction en option disponible avec Websense Web Security et avec Websense Web Filter.

Remote Filtering surveille le trafic HTTP, SSL et FTP, en appliquant soit la stratégie affectée à l'utilisateur ou au groupe individuel, sur la stratégie Par défaut, selon la façon dont l'utilisateur se connecte à l'ordinateur distant. Remote Filtering n'effectue pas de filtrage sur la base des stratégies affectées aux ordinateurs ou aux plages réseau. Pour plus d'informations, consultez *Identification des utilisateurs distants*, page 161.

Le filtrage basé sur la bande passante n'est pas pris en charge pour les clients distants (voir *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191). La bande passante générée par le trafic distant n'est pas incluse dans les mesures et les rapports de bande passante.

Les requêtes FTP et SSL, telles que HTTPS, peuvent uniquement être bloquées ou autorisées. Par exemple, si un utilisateur distant demande un site FTP ou HTTPS d'une catégorie affectée à une action de temps contingenté ou de confirmation, le site est bloqué pour les clients du filtrage distant. Lorsque ces ordinateurs naviguent sur Internet depuis le réseau, les actions de filtrage de temps contingenté et de confirmation sont appliquées normalement.

Pour implémenter Remote Filtering, vous devez installer les composants suivants :

- Le serveur Remote Filtering doit être placé dans le pare-feu le plus extérieur et les ordinateurs distants doivent pouvoir communiquer avec lui. En général, il est installé dans une *zone démilitarisée* du réseau, ou zone DMZ, à l'extérieur du pare-feu qui protège le reste du réseau. Vous pouvez installer jusqu'à 3 serveurs Remote Filtering pour assurer des capacités de basculement.

- Le client Remote Filtering doit être installé sur chaque ordinateur exécutant le système d'exploitation Windows et utilisé hors du réseau.

  Remarques

  Suivez attentivement les recommandations du *Guide de déploiement* pour déployer ces composants. Pour des instructions sur leur installation, consultez le *Guide d'installation*.

  Si vous utilisez Websense en mode autonome (sans produit d'intégration), configurez Network Agent pour qu'il ne surveille **pas** le serveur Remote Filtering (voir *Configuration des paramètres globaux*, page 346).

Toutes les communications entre le client et le serveur Remote Filtering sont authentifiées et cryptées.

Fonctionnement de Remote Filtering

Rubriques connexes :

- *Au sein du réseau*, page 159
- *À l'extérieur du réseau*, page 160
- *Identification des utilisateurs distants*, page 161
- *Lorsque la communication du serveur échoue*, page 162
- *Réseau privé virtuel (VPN)*, page 163
- *Configuration des paramètres de Remote Filtering*, page 164

Chaque fois qu'un ordinateur distant envoie une requête HTTP, SSL ou FTP, son client Remote Filtering communique avec un serveur Remote Filtering. Le serveur Remote Filtering communique avec Websense Filtering Service pour identifier l'action à appliquer. Le serveur Remote Filtering répond ensuite au client Remote Filtering en autorisant le site ou en envoyant le message de blocage approprié.

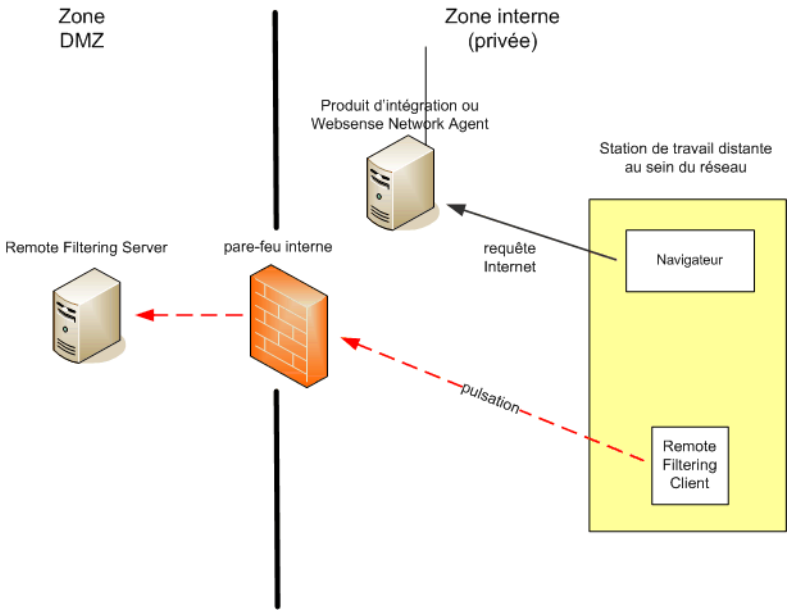
Lorsque le navigateur d'un ordinateur exécutant le client Remote Filtering envoie une requête via HTTP, SSL ou FTP, le client Remote Filtering doit déterminer s'il doit interroger le serveur Remote Filtering pour cette requête. Cette détermination est contrôlée par l'emplacement de l'ordinateur par rapport au réseau.

Au sein du réseau

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *À l'extérieur du réseau*, page 160
- *Identification des utilisateurs distants*, page 161
- *Lorsque la communication du serveur échoue*, page 162
- *Réseau privé virtuel (VPN)*, page 163
- *Configuration des paramètres de Remote Filtering*, page 164

Lorsqu'un ordinateur démarre *à l'intérieur* du réseau, le client Remote Filtering tente d'envoyer une **pulsation** au serveur Remote Filtering présent dans la zone DMZ. La pulsation fonctionne car le port de pulsation est ouvert sur le pare-feu interne.



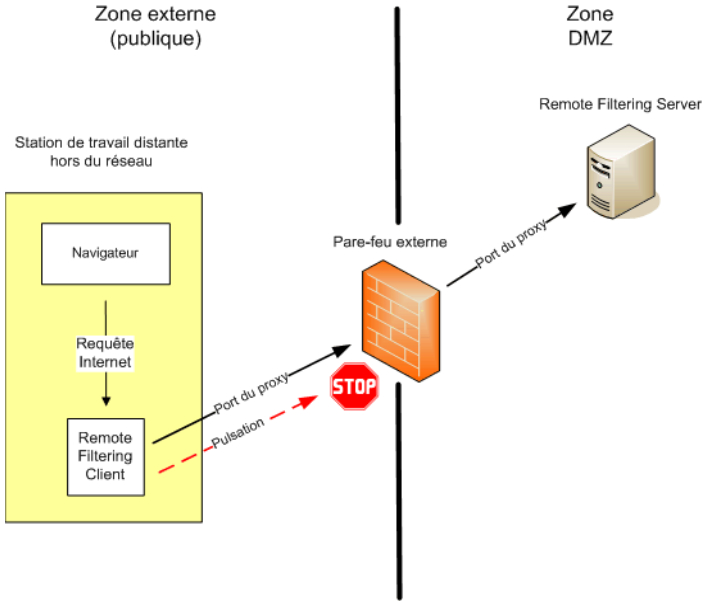
Dans ce cas, le client Remote Filtering devient passif et n'interroge pas le serveur Remote Filtering sur les requêtes Internet, mais transmet directement ces dernières aux produits d'intégration (par exemple Cisco Pix, Microsoft ISA Server) ou à Websense Network Agent. La requête est filtrée comme n'importe quelle autre requête interne.

À l'extérieur du réseau

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *Au sein du réseau*, page 159
- *Identification des utilisateurs distants*, page 161
- *Lorsque la communication du serveur échoue*, page 162
- *Réseau privé virtuel (VPN)*, page 163
- *Configuration des paramètres de Remote Filtering*, page 164

Lorsqu'un ordinateur démarre *hors* du réseau, le client Remote Filtering tente d'envoyer une pulsation au serveur Remote Filtering. La pulsation est un échec car le port de pulsation est bloqué au niveau du pare-feu externe.



Cet échec de pulsation invite le client Remote Filtering à interroger le serveur Remote Filtering de la zone DMZ sur chaque requête HTTP, SSL ou FTP envoyée par le port configuré (par défaut 80). Le serveur Remote Filtering transmet ensuite la requête de filtrage à Websense Filtering Service à l'intérieur du réseau. Filtering Service évalue la requête et envoie une réponse au serveur Remote Filtering. Cette réponse est ensuite envoyée à l'ordinateur distant. Si le site est bloqué, le client Remote Filtering reçoit la page de blocage appropriée, ensuite affichée à l'utilisateur.

Le client Remote Filtering retarde chaque requête filtrée jusqu'à ce qu'il reçoive une réponse du serveur Remote Filtering. Selon la réponse reçue, le client Remote Filtering autorise ensuite le site ou affiche la page de blocage.

Un fichier journal surveille les activités de Remote Filtering, par exemple les entrées et les sorties du réseau, les échecs d'ouverture ou de fermeture et les redémarrages du

client. Le client Remote Filtering crée le fichier journal lorsqu'il démarre pour la première fois. Vous pouvez contrôler la présence et la taille de ce fichier journal. Voir *Configuration des paramètres de Remote Filtering*, page 164.

Identification des utilisateurs distants

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *Au sein du réseau*, page 159
- *À l'extérieur du réseau*, page 160
- *Lorsque la communication du serveur échoue*, page 162
- *Réseau privé virtuel (VPN)*, page 163
- *Configuration des paramètres de Remote Filtering*, page 164

La façon dont un utilisateur se connecte à un ordinateur distant détermine la stratégie appliquée.

Lorsque l'utilisateur se connecte à l'aide des informations d'identification du domaine (informations de connexion de l'annuaire réseau), Websense Filtering Service peut résoudre le nom d'utilisateur et applique à l'ordinateur distant les stratégies appropriées, basées sur les utilisateurs et les groupes. L'activité Internet est en outre journalisée sous le nom d'utilisateur réseau.

Si l'utilisateur se connecte avec un compte d'utilisateur local sur l'ordinateur, Filtering Service ne peut pas résoudre le nom d'utilisateur et applique à la place la stratégie Par défaut. L'activité Internet est journalisée sous le nom d'utilisateur local. Remote Filtering n'effectue pas de filtrage sur la base des stratégies affectées aux ordinateurs ou aux plages réseau.

Remarque

Les utilisateurs distants sont toujours filtrés en fonction de leurs informations d'identification de connexion, selon la description donnée ici. Les paramètres d'authentification sélective ne s'appliquent pas à ces utilisateurs.

Lorsque la communication du serveur échoue

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *Au sein du réseau*, page 159
- *À l'extérieur du réseau*, page 160
- *Identification des utilisateurs distants*, page 161
- *Réseau privé virtuel (VPN)*, page 163
- *Configuration des paramètres de Remote Filtering*, page 164

Le filtrage intervient lorsqu'un client Remote Filtering, extérieur au réseau, réussit à communiquer avec le serveur Remote Filtering dans la zone DMZ du réseau. Toutefois, la communication échoue parfois.

L'action exécutée par le client Remote Filtering lorsqu'il ne peut pas contacter le serveur Remote Filtering est configurable. Par défaut, le client Remote Filtering utilise le paramètre **Échec d'ouverture**, qui autorise toutes les requêtes HTTP, SSL et FTP lorsque la communication ne peut pas être établie entre ces composants. Le client Remote Filtering continue d'essayer de contacter le serveur Remote Filtering. Dès que la communication est établie, la stratégie de filtrage appropriée est appliquée.

Lorsque le client Remote Filtering est configuré sur **Échec de fermeture**, une valeur de délai d'attente est appliquée (par défaut 15 minutes). Le compteur commence au démarrage de l'ordinateur distant. Le client Remote Filtering tente immédiatement de se connecter au serveur Remote Filtering et poursuit son cycle par l'intermédiaire des serveurs Remote Filtering disponibles jusqu'à ce qu'il réussisse.

Si l'utilisateur a accès à Internet au démarrage, le filtrage n'intervient pas (toutes les requêtes sont autorisées) jusqu'à ce que le client Remote Filtering se connecte au serveur Remote Filtering. Dès que la communication est établie, la stratégie de filtrage appropriée est appliquée.

Si le client Remote Filtering ne peut pas se connecter pendant la période d'expiration configurée, l'accès Internet est bloqué (échec de fermeture) jusqu'à ce que la connexion au serveur Remote Filtering soit établie.

Remarque

Si le serveur Remote Filtering ne peut pas se connecter à Websense Filtering Service pour une raison quelconque, une erreur est renvoyée au client Remote Filtering et le filtrage reste sur Échec d'ouverture.

Cette période d'expiration permet aux utilisateurs qui payent l'accès Internet en déplacement de démarrer l'ordinateur et de disposer d'une connexion sans être bloqués. Si l'utilisateur n'accède pas à Internet avant l'expiration du délai de 15 minutes, l'accès à Internet ne peut pas être établi au cours de cette session. Dans ce

cas, l'utilisateur doit redémarrer l'ordinateur pour commencer un nouvel intervalle de délai d'expiration.

Pour modifier le paramètre Échec d'ouverture/Échec de fermeture et la valeur du délai d'expiration, consultez la section *Configuration des paramètres de Remote Filtering*, page 164.

Réseau privé virtuel (VPN)

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *Au sein du réseau*, page 159
- *À l'extérieur du réseau*, page 160
- *Identification des utilisateurs distants*, page 161
- *Lorsque la communication du serveur échoue*, page 162
- *Configuration des paramètres de Remote Filtering*, page 164

Websense Remote Filtering prend en charge les connexions VPN, y compris les VPN autorisant le split-tunneling. Lorsqu'un ordinateur distant se connecte au réseau interne via un VPN (sans split-tunneling), le client Remote Filtering peut envoyer une pulsation au serveur Remote Filtering. Le client Remote Filtering devient alors passif et toutes les requêtes HTTP, SSL et FTP provenant de l'ordinateur distant sont filtrées par le produit d'intégration interne ou par Network Agent, comme les autres ordinateurs du réseau.

Si l'ordinateur distant se connecte au réseau interne via un client VPN autorisant le split-tunneling, le client Remote Filtering le détecte et n'envoie pas de pulsation au serveur Remote Filtering. Le client Remote Filtering part du principe qu'il fonctionne en externe et envoie les requêtes serveur Remote Filtering Server pour le filtrage.

Websense prend en charge le split-tunneling pour les clients VPN suivants :

- Checkpoint SecureClient
- Cisco
- Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL

Configuration des paramètres de Remote Filtering

Rubriques connexes :

- *Fonctionnement de Remote Filtering*, page 158
- *Au sein du réseau*, page 159
- *À l'extérieur du réseau*, page 160
- *Identification des utilisateurs distants*, page 161
- *Lorsque la communication du serveur échoue*, page 162
- *Réseau privé virtuel (VPN)*, page 163

Les Super administrateurs sans condition peuvent utiliser la page **Paramètres > Général > Remote Filtering** pour configurer les options qui affectent tous les clients Remote Filtering associés à cette installation.

Pour plus d'informations sur le fonctionnement de Remote Filtering, consultez la section *Fonctionnement de Remote Filtering*, page 158.

1. Cochez la case **Fermer en cas d'échec** pour bloquer tous les accès Internet des clients Remote Filtering lorsque leur ordinateur ne communique pas avec un serveur Remote Filtering.

   Cette option est désactivée par défaut, ce qui signifie que les utilisateurs distants ont un accès non filtré à Internet lorsque leur ordinateur ne peut pas communiquer avec le serveur Remote Filtering.

2. Si vous cochez la case Fermer en cas d'échec, utilisez le champ **Délai d'attente de fermer en cas d'échec** pour sélectionner un nombre de minutes allant jusqu'à 60 (par défaut 15), ou choisissez **Aucun délai d'attente**.

   Pendant la période du délai d'expiration, toutes les requêtes HTTP, SSL et FTP sont autorisées.

   Si le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering pendant l'intervalle de délai, l'accès Internet est bloqué (échec de fermeture).

   L'activation de l'option **Aucun délai d'attente** peut verrouiller un ordinateur distant avant que l'utilisateur ne puisse établir une connexion Internet depuis un hôtel ou un fournisseur payant. De plus, le client Remote Filtering tente continuellement de communiquer avec le serveur Remote Filtering.

   Avertissement

   Websense, Inc. ne recommande pas d'utiliser l'option **Aucun délai d'attente** ni de définir une période de délai trop basse.

3. Sélectionnez une **Taille maximum du fichier journal** (en méga-octets), allant jusqu'à 10. Choisissez **Aucun journal** pour désactiver la journalisation.

Cette option contrôle la taille et l'existence du fichier journal créé par l'ordinateur distant lorsqu'il est initialement déconnecté du serveur Remote Filtering. Ce fichier journal surveille les événements suivants :

- L'ordinateur quitte le réseau.
- L'ordinateur rejoint le réseau.
- Le client Remote Filtering redémarre.
- Une condition d'échec d'ouverture se produit.
- Une condition de fermeture en cas d'échec se produit.
- Le client Remote Filtering reçoit une mise à jour de stratégie.

L'ordinateur conserve les deux journaux les plus récents. Ces journaux peuvent être utilisés pour dépanner des problèmes de connexion ou d'autres problèmes liés à Remote Filtering.

9 Affinage des stratégies de filtrage

Dans sa configuration la plus simple, le filtrage de l'utilisation Internet ne requiert qu'une seule stratégie appliquant un filtre de catégories et un filtre de protocoles 24 heures sur 24 et 7 jours sur 7. Websense propose toutefois des outils qui vont bien au-delà de ce filtrage de base pour obtenir le niveau de granularité dont vous avez véritablement besoin pour gérer l'utilisation d'Internet dans votre entreprise. Vous pouvez :

- Créer des **filtres d'accès limité** pour bloquer l'accès à tous les sites à l'exception d'une liste de sites pour certains utilisateurs (voir *Restriction des utilisateurs à une liste définie de sites Internet*, page 168).
- Créer des **catégories personnalisées** permettant de redéfinir le filtrage des sites sélectionnés (voir *Fonctionnement des catégories*, page 175).
- **Recatégoriser les URL** pour déplacer des sites spécifiques de leur catégorie par défaut dans la base de données principale vers une autre catégorie définie par Websense ou personnalisée (voir *Recatégorisation d'URL*, page 184).
- Définir des **URL non filtrées** pour permettre aux utilisateurs d'accéder à des sites spécifiques, même lorsque ces sites sont affectés à une catégorie bloquée dans le filtre de catégories actif (voir *Définition d'URL non filtrées*, page 183).
- Implémenter des restrictions de **bande passante** qui empêchent les utilisateurs d'accéder à des catégories et des protocoles autrement autorisés lorsque l'utilisation de la bande passante atteint un seuil défini.
- Définir des **mots-clés** utilisés pour bloquer des sites appartenant à des catégories autrement autorisées lorsque le blocage des mots-clés est activé (voir *Filtrage par mots-clés*, page 180).
- Définir des **types de fichiers** permettant de bloquer le téléchargement de types de fichiers sélectionnés appartenant à des catégories autrement autorisées lorsque le blocage des types de fichiers est activé (voir *Gestion du trafic en fonction du type de fichiers*, page 193).

Restriction des utilisateurs à une liste définie de sites Internet

Rubriques connexes :

- *Filtres d'accès limité et priorités du filtrage*, page 168
- *Création d'un filtre d'accès limité*, page 169
- *Modification d'un filtre d'accès limité*, page 170

Les filtres d'accès limité constituent une méthode de filtrage Internet très précise. Chaque filtre d'accès limité est une liste de sites Web individuels. Comme les filtres de catégories, les filtres d'accès limité sont ajoutés à des stratégies et appliqués pendant une période définie. Lorsqu'un filtre d'accès limité est actif dans une stratégie, les utilisateurs affectés à cette stratégie ne peuvent visiter que les sites de la liste. Tous les autres sites sont bloqués.

Par exemple, si la stratégie Premier niveau impose un filtre d'accès limité incluant seulement certains sites de référence et d'enseignement, les étudiants régis par cette stratégie ne peuvent visiter que ces sites, et aucun autre.

Important

Lorsqu'un filtre d'accès limité est actif, Websense se contente de vérifier si le site demandé y apparaît. Aucune autre vérification n'est effectuée.

Cela signifie que si un site autorisé par le filtre est infecté par du code malveillant, les requêtes des utilisateurs pour ce site sont tout de même autorisées, quelle que soit la catégorisation du site dans la base de données principale ou dans l'analyse en temps réel.

Lorsqu'un filtre d'accès limité est actif, une page de blocage est renvoyée pour toute URL demandée non incluse dans ce filtre.

Websense peut prendre en charge jusqu'à 2 500 filtres d'accès limité contenant 25 000 URL au total.

Filtres d'accès limité et priorités du filtrage

Dans certains cas, plusieurs stratégies de filtrage peuvent s'appliquer à un même utilisateur. Cela se produit lorsqu'un utilisateur est membre de plusieurs groupes régis par des stratégies différentes. De plus, une URL peut apparaître dans un filtre d'accès limité et être définie comme URL non filtrée.

Lorsque plusieurs stratégies de groupe s'appliquent à un utilisateur, le paramètre **Utiliser le blocage le plus restrictif** (voir *Ordre du filtrage*, page 80) détermine comment l'utilisateur est filtré. Par défaut, ce paramètre est désactivé.

Websense identifie le paramètre de filtrage le moins restrictif au niveau du filtre. Lorsqu'un utilisateur est filtré par plusieurs stratégies, dont l'une d'entre elles applique un filtre d'accès limité, « moins restrictif » peut se révéler difficile à interpréter.

Lorsque l'option **Utiliser un blocage plus restrictif** est **OFF** :

- Si le filtre de catégorie **Bloquer tout** et un filtre d'accès limité peuvent s'appliquer, le filtre d'accès limité est toujours considéré comme le moins restrictif.
- Si un autre filtre de catégories et un filtre d'accès limité peuvent s'appliquer, le filtre de catégories est toujours considéré comme le moins restrictif.

  Cela signifie que, même lorsque le filtre d'accès limité autorise le site alors que le filtre de catégories le bloque, le site est bloqué.

Lorsque l'option **Utiliser un blocage plus restrictif** est **ON**, un filtre d'accès limité est considéré comme moins restrictif que tout autre filtre de catégories à l'exception de Bloquer tout.

Le tableau suivant résume les effets du paramètre **Utiliser un blocage plus restrictif** sur le filtrage lorsque plusieurs stratégies peuvent s'appliquer :

	***Utiliser un blocage plus restrictif* désactivé**	***Utiliser le blocage le plus restrictif* activé**
Filtre d'accès limité + Filtre de catégories **Bloquer tout**	Filtre d'accès limité (requête autorisée)	**Bloquer tout** (requête bloquée)
Filtre d'accès limité + Catégorie autorisée	Filtre de catégories (requête autorisée)	Filtre d'accès limité (requête autorisée)
Filtre d'accès limité + Catégorie bloquée	Filtre de catégories (requête bloquée)	Filtre d'accès limité (requête autorisée)
Filtre d'accès limité + Catégorie Temps contingenté/ Confirmer	Filtre de catégories (requête limitée par Temps contingenté/Confirmer)	Filtre d'accès limité (requête autorisée)
Filtre d'accès limité + URL non filtrée	URL non filtrée (requête autorisée)	Filtre d'accès limité (requête autorisée)

Création d'un filtre d'accès limité

Rubriques connexes :

- *Fonctionnement des filtres*, page 48
- *Restriction des utilisateurs à une liste définie de sites Internet*, page 168
- *Modification d'un filtre d'accès limité*, page 170

Utilisez la page **Ajouter un filtre d'accès limité** (accessible via la page **Filtres** ou **Modifier la stratégie**) pour donner à votre nouveau filtre un nom unique et une

description. Une fois le filtre créé, entrez une liste d'URL autorisées, affectez le filtre à une stratégie et appliquez cette dernière à des clients.

1. Entrez un **nom de filtre** unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Les noms de filtre peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez une brève **Description** du filtre. Cette description apparaît à côté du nom du filtre dans la section Filtres d'accès limité de la page Filtres et doit décrire l'objectif du filtre pour simplifier la gestion ultérieure des stratégies par les administrateurs.

   Les restrictions de caractères qui s'appliquent aux noms de filtre s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).
3. Pour voir et modifier le nouveau filtre, cliquez sur **OK**. Pour abandonner vos modifications et revenir à la page Filtres, cliquez sur **Annuler**.

Lorsque vous créez un nouveau filtre d'accès limité, il est ajouté dans la liste **Gestion des stratégies > Filtres > Filtres d'accès limité**. Cliquez sur le nom du filtre à modifier.

Pour finir de personnaliser le nouveau filtre, continuez avec la section *Modification d'un filtre d'accès limité*.

Modification d'un filtre d'accès limité

Rubriques connexes :

- *Restriction des utilisateurs à une liste définie de sites Internet*, page 168
- *Filtres d'accès limité et priorités du filtrage*, page 168
- *Création d'un filtre d'accès limité*, page 169
- *Modification d'une stratégie*, page 77

Un filtre d'accès limité est une liste de sites Web (URL ou adresses IP) et d'expressions régulières utilisées pour identifier des sites spécifiques auxquels les

utilisateurs peuvent accéder. Lorsque le filtre est appliqué à des clients, ces derniers ne peuvent visiter aucun autre site que ceux de la liste.

> **Important**
>
> Lorsqu'un filtre d'accès limité est actif, Websense se contente de vérifier si le site demandé y apparaît. Aucune autre vérification n'est effectuée.
>
> Cela signifie que si un site autorisé par le filtre est infecté par du code malveillant, les requêtes des utilisateurs pour ce site sont tout de même autorisées, quelle que soit la catégorisation du site dans la base de données principale ou dans l'analyse en temps réel.

La page **Gestion des stratégies > Filtres > Modifier le filtre d'accès limité** permet de modifier un filtre d'accès limité existant. Vous pouvez modifier le nom et la description du filtre, voir la liste des stratégies qui l'appliquent et gérer les sites inclus dans le filtre.

Lorsque vous modifiez un filtre d'accès limité, les modifications apportées affectent toutes les stratégies qui appliquent le filtre.

1. Vérifiez le nom et la description du filtre. Pour modifier le nom du filtre, cliquez sur **Renommer** et entrez un nouveau nom. Le nom est mis à jour dans toutes les stratégies qui appliquent le filtre d'accès limité sélectionné.
2. Servez-vous du champ **Stratégies utilisant ce filtre** pour connaître le nombre de stratégies qui emploient actuellement ce filtre. Si une ou plusieurs stratégies appliquent le filtre, cliquez sur **Afficher les stratégies** pour en voir la liste.
3. Sous Ajouter ou supprimer des sites, entrez les URL et les adresses IP que vous souhaitez ajouter au filtre d'accès limité. Entrez une URL ou une adresse IP par ligne.

   Il n'est pas nécessaire d'inclure le préfixe HTTP://.

   Lorsqu'un site est filtré en fonction de sa catégorie dans la base de données principale, Websense établit la correspondance entre l'URL et son adresse IP équivalente. Ce n'est pas le cas pour les filtres d'accès limité. Pour autoriser l'URL et l'adresse IP d'un site, ajoutez les deux dans le filtre.
4. Cliquez sur la flèche droite (>) pour déplacer les URL et les adresses IP vers la liste des sites autorisés.
5. En plus d'ajouter des sites individuels au filtre d'accès limité, vous pouvez ajouter des expressions régulières qui correspondent à plusieurs sites. Pour créer des expressions régulières, cliquez sur **Avancé**.
   - Entrez une expression régulière par ligne, puis cliquez sur la flèche droite pour déplacer les expressions vers la liste des sites autorisés.
   - Pour vérifier qu'une expression régulière correspond aux sites prévus, cliquez sur **Test**.
   - Pour plus d'informations sur l'utilisation d'expressions régulières pour le filtrage, consultez la section *Utilisation d'expressions régulières*, page 196.

6. Vérifiez les URL, les adresses IP et les expressions régulières dans la liste **Sites autorisés**.
   - Pour modifier un site ou une expression, sélectionnez-le et cliquez sur **Éditer**.
   - Pour supprimer un site ou une expression de la liste, sélectionnez-le et cliquez sur **Supprimer**.
7. Après avoir modifié le filtre, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Filtres. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout de sites depuis la page Modifier la stratégie

Rubriques connexes :

- *Restriction des utilisateurs à une liste définie de sites Internet*, page 168
- *Filtres d'accès limité et priorités du filtrage*, page 168
- *Création d'un filtre d'accès limité*, page 169
- *Modification d'une stratégie*, page 77

La page **Stratégies > Modifier la stratégie > Ajouter des sites** permet d'ajouter des sites à un filtre d'accès limité.

Entrez une URL ou une adresse IP par ligne. Si vous ne spécifiez pas de protocole, Websense ajoute automatiquement le préfixe **HTTP://**.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier la stratégie. Cliquez également sur **OK** dans la page Modifier la stratégie pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Les modifications apportées à un filtre d'accès limité affectent toutes les stratégies qui imposent ce filtre.

Copie de filtres et de stratégies vers des rôles

Rubriques connexes :

- *Création d'un filtre de catégories*, page 49
- *Création d'un filtre de protocoles*, page 51
- *Création d'un filtre d'accès limité*, page 169
- *Création d'une stratégie*, page 76

Les Super administrateurs peuvent utiliser les pages **Filtres > Copier des filtres dans le rôle** et **Stratégies > Copier des stratégies dans le rôle** pour copier un ou plusieurs filtres ou stratégies vers un rôle d'administration déléguée. Une fois que le filtre ou la stratégie a été copié(e), les administrateurs délégués peuvent les utiliser pour filtrer leurs clients gérés.

- Dans le rôle cible, la mention « (Copié) » est ajoutée à la fin du nom du filtre ou de la stratégie. Un nombre est également ajouté si le même filtre ou la même stratégie est copié(e) plusieurs fois.
- Les administrateurs délégués peuvent renommer ou modifier les filtres ou les stratégies qui ont été copiés dans leur rôle.
- Les filtres de catégories copiés dans un rôle d'administration déléguée définissent l'action de filtrage sur Autoriser pour les catégories personnalisées créées dans ce rôle. Il est préférable que les administrateurs délégués actualisent les filtres de catégories copiés afin de définir l'action désirée pour les catégories personnalisées propres à leur rôle.
- Les modifications apportées par un administrateur délégué à un filtre ou une stratégie copié(e) dans son rôle par un Super administrateur n'affectent pas le filtre ou la stratégie original(e) du Super administrateur, ni les autres rôles qui ont reçu une copie du filtre ou de la stratégie.
- Les restrictions de verrouillage de filtres n'affectent pas le filtre ou la stratégie du Super administrateur, mais affectent la copie du filtre ou de la stratégie de l'administrateur délégué.
- Les administrateurs délégués étant régis par les restrictions de verrouillage des filtres, le filtre de catégories Autoriser tout et les filtres de protocoles ne peuvent pas être copiés dans un rôle d'administration déléguée.

Pour copier un filtre ou une stratégie :

1. Dans la page Copier des filtres dans le rôle ou Copier des stratégies dans le rôle, assurez-vous que les stratégies ou les filtres appropriés s'affichent dans la liste en haut de la page.
2. Utilisez la liste déroulante **Sélectionner un rôle** pour choisir un rôle de destination.
3. Cliquez sur **OK**.

   Une fenêtre contextuelle signale que les stratégies ou les filtres sélectionné(e)s sont copié(e)s. Le processus de copie peut prendre un certain temps.

   Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Lorsque le processus de copie est terminé, les stratégies ou les filtres copié(e)s seront à la disposition des administrateurs délégués dans le rôle sélectionné lors de leur prochaine connexion à Websense Manager. Si un administrateur délégué est connecté au rôle pendant que les filtres ou les stratégies sont copié(e)s, il ne voit pas les nouveaux filtres ni les nouvelles stratégies avant de s'être déconnecté et reconnecté.

Construction de composants de filtres

La page **Gestion des stratégies > Composants de filtre** propose des outils qui permettent d'affiner et de personnaliser la façon dont Websense applique les stratégies d'accès à Internet de votre organisation. Les quatre boutons de l'écran sont associés aux tâches suivantes :

Modifier les catégories	• Recatégoriser une URL, (voir *Redéfinition du filtrage pour des sites spécifiques*, page 182). Par exemple, si votre stratégie de filtrage Internet bloque la catégorie Shopping mais que vous souhaitez autoriser l'accès à certains sites de partenaires ou de fournisseurs, vous pouvez déplacer ces sites vers une catégorie autorisée telle que Commerce et économie. • Définir ou modifier des catégories personnalisées (voir *Création d'une catégorie personnalisée*, page 178). Créez des sous-catégories supplémentaires dans les catégories parentes définies par Websense ou dans la catégorie parente Définie par l'utilisateur, puis affectez des URL aux nouvelles catégories. • Affecter des mots-clés à une catégorie (voir *Filtrage par mots-clés*, page 180). Pour recatégoriser et bloquer l'accès aux sites dont l'URL contient une chaîne spécifique, définissez d'abord des mots-clés, puis activez le blocage par mots-clés dans un filtre de catégorie. • Créer des expressions régulières (voir *Utilisation d'expressions régulières*, page 196) ou des modèles pouvant correspondre à plusieurs URL et les affecter à une catégorie.
Modifier les protocoles	Définir ou modifier des définitions de protocole personnalisées (voir *Création d'un protocole personnalisé*, page 189 et *Modification des protocoles personnalisés*, page 186). Par exemple, si certains membres de votre organisation utilisent un outil de messagerie personnalisé, vous pouvez créer une définition de protocole personnalisée autorisant l'utilisation de cet outil tout en bloquant les autres protocoles de messagerie instantanée ou de conversation.
Types de fichiers	Créer ou modifier les définitions de types de fichiers utilisées pour bloquer des types de fichiers spécifiques appartenant à des catégories sinon autorisées (voir *Gestion du trafic en fonction du type de fichiers*, page 193).
URL non filtrées	Définir des sites spécifiques pour autoriser tous les clients, même lorsqu'ils appartiennent à une catégorie bloquée (voir *Définition d'URL non filtrées*, page 183). Notez que l'ajout d'une URL dans cette liste ne remplace pas le filtre de catégories Bloquer tout ni les filtres d'accès limité.

Fonctionnement des catégories

Rubriques connexes :

- *Modification des catégories et de leurs attributs*, page 175
- *Création d'une catégorie personnalisée*, page 178
- *Filtrage par mots-clés*, page 180
- *Redéfinition du filtrage pour des sites spécifiques*, page 182

Websense fournit plusieurs méthodes pour filtrer les sites qui ne sont pas dans la base de données principale et pour modifier la façon dont les sites individuels de cette base de données sont filtrés.

- Pour un filtrage et des rapports plus précis, créez des **catégories personnalisées**.
- Servez-vous des **URL recatégorisées** pour définir les catégories des sites non classés ou pour modifier la catégorie des sites apparaissant dans la base de données principale.
- Définissez des **mots-clés** pour recatégoriser tous les sites dont l'URL contient une certaine chaîne.

Modification des catégories et de leurs attributs

Rubriques connexes :

- *Création d'une catégorie personnalisée*, page 178
- *Vérification de tous les attributs des catégories personnalisées*, page 177
- *Modification du filtrage global des catégories*, page 177
- *Filtrage par mots-clés*, page 180
- *Redéfinition du filtrage pour des sites spécifiques*, page 182

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories** permet de créer et de modifier des catégories personnalisées, des URL recatégorisées et des mots-clés.

Les catégories existantes, définies par Websense et personnalisées, sont énumérées dans la partie gauche du panneau de contenu. Pour voir les paramètres personnalisés actuellement associés à une catégorie, ou pour créer de nouvelles définitions personnalisées, commencez par sélectionner une catégorie dans la liste.

Pour voir la liste de tous les éléments (URL personnalisées, mots-clés et expressions régulières) associés à toutes les catégories, cliquez sur **Afficher l'ensemble des URL/ mots-clés personnalisés** dans la barre d'outils située en haut de la page. Pour plus

d'informations, consultez *Vérification de tous les attributs des catégories personnalisées*, page 177.

- Pour créer une nouvelle catégorie, cliquez sur **Ajouter**, puis passez à la section *Création d'une catégorie personnalisée*, page 178 pour d'autres instructions.

  Pour supprimer une catégorie personnalisée existante, sélectionnez-la, puis cliquez sur **Supprimer**. Vous ne pouvez pas supprimer les catégories définies par Websense.
- Pour modifier le nom ou la description d'une catégorie personnalisée, sélectionnez la catégorie, puis cliquez sur **Renommer** (voir *Modification du nom d'une catégorie personnalisée*, page 178).
- Pour modifier l'action de filtrage associée à une catégorie dans tous les filtres de catégories, cliquez sur **Remplacer l'action** (voir *Modification du filtrage global des catégories*, page 177).
- La liste **URL recatégorisées** présente les sites recatégorisés (URL et adresses IP) affectés à cette catégorie.
  - Pour ajouter un site dans la liste, cliquez sur **Ajouter des URL**. Consultez la section *Recatégorisation d'URL*, page 184 pour plus d'instructions.
  - Pour modifier une catégorie recatégorisée existante, sélectionnez l'URL ou l'adresse IP, puis cliquez sur **Éditer**.
- La liste **Mots-clés** présente les mots-clés associés à cette catégorie.
  - Pour définir un mot-clé associé à la catégorie sélectionnée, cliquez sur **Ajouter des mots-clés**. Consultez la section *Filtrage par mots-clés*, page 180 pour plus d'instructions.
  - Pour modifier la définition d'un mot-clé existant, sélectionnez le mot-clé, puis cliquez sur **Éditer**.
- Outre les URL et les mots-clés, vous pouvez définir des **Expressions régulières** pour la catégorie. Chaque expression régulière est un modèle utilisé pour associer plusieurs sites à la catégorie.

  Pour voir ou créer des expressions régulières pour la catégorie, cliquez sur **Avancé**.
  - Pour définir une expression régulière, cliquez sur Ajouter des expressions (voir *Utilisation d'expressions régulières*, page 196).
  - Pour modifier une expression régulière existante, sélectionnez l'expression, puis cliquez sur **Éditer**.
- Pour supprimer une URL, une expression régulière ou un mot clé recatégorisé(e), sélectionnez l'élément, puis cliquez sur **Supprimer**.

Lorsque vos modifications sont terminées dans la page Modifier les catégories, cliquez sur **OK** pour mettre en cache les modifications et revenir à la page Composants de filtre. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Vérification de tous les attributs des catégories personnalisées

La page **Composants de filtre > Modifier les catégories > Afficher l'ensemble des URL/mots-clés personnalisés** permet de revoir les définitions personnalisées d'URL, de mots-clés et d'expressions régulières. Vous pouvez également supprimer les définitions qui ne sont plus nécessaires.

La page présente trois tableaux similaires, un pour chaque attribut de catégorie : URL personnalisées, mots-clés ou expressions régulières. Dans chaque tableau, l'attribut est affiché à côté du nom de la catégorie à laquelle il est associé.

Pour supprimer un attribut de catégorie, cochez la case appropriée, puis cliquez sur **Supprimer**.

Pour revenir à la page Modifier les catégories, cliquez sur **Fermer**. Si vous supprimez des éléments dans la page Afficher l'ensemble des URL/mots-clés personnalisés, cliquez sur **OK** dans la page Modifier les catégories pour mettre les modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Modification du filtrage global des catégories

La page **Composants de filtre > Modifier les catégories > Remplacer l'action** permet de modifier l'action appliquée à une catégorie dans tous les filtres de catégories existants. Elle permet également de déterminer l'action appliquée par défaut à la catégorie dans les nouveaux filtres.

Bien que cette modification remplace l'action appliquée à la catégorie dans tous les filtres existants, les administrateurs peuvent ensuite modifier ces filtres pour appliquer une action différente.

Avant de modifier les paramètres de filtrage appliqués à une catégorie, vérifiez que le nom de la catégorie appropriée s'affiche à côté de **Catégorie sélectionnée**. Vous pouvez ensuite :

1. Choisir une nouvelle **Action** (Autoriser, Bloquer, Confirmer ou Contingent). Pour plus d'informations, consultez *Actions de filtrage*, page 44.

   Par défaut, l'option **Ne pas modifier les paramètres actuels** est sélectionnée pour toutes les options de la page.
2. Spécifiez si vous souhaitez ou non **Bloquer des mots-clés**. Pour plus d'informations, consultez *Filtrage par mots-clés*, page 180.
3. Spécifiez ensuite si vous souhaitez ou non **Bloquer des types de fichiers** et personnaliser les paramètres du blocage. Pour plus d'informations, consultez *Gestion du trafic en fonction du type de fichiers*, page 193.

4. Sous **Filtrage avancé**, spécifiez si vous souhaitez ou non utiliser Bandwidth Optimizer pour gérer l'accès aux sites HTTP et personnaliser les paramètres de blocage. Pour plus d'informations, consultez *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.

   Important
   Les modifications apportées ici affectent tous les filtres de catégories existants à l'exception des filtres **Bloquer tout** et **Autoriser tout**.

5. Cliquez sur **OK** pour revenir à la page Modifier les catégories (voir *Modification des catégories et de leurs attributs*, page 175). Pour mettre en cache vos modifications, cliquez sur **OK** dans la page Modifier les catégories.

Modification du nom d'une catégorie personnalisée

La page **Composants de filtre > Modifier les catégories > Renommer la catégorie** permet de modifier le nom et la description associés à une catégorie personnalisée.

- Utilisez le champ **Nom du filtre** pour modifier le nom de la catégorie. Le nouveau nom doit être unique et ne doit pas dépasser 50 caractères.

  Le nom ne doit pas inclure les caractères suivants :

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- Utilisez le champ **Description** pour modifier la description de la catégorie. La description ne doit pas dépasser 255 caractères.

  Les restrictions de caractères qui s'appliquent aux noms de filtre s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier les catégories. Pour mettre en cache vos modifications, cliquez sur **OK** dans la page Modifier les catégories.

Création d'une catégorie personnalisée

Rubriques connexes :

- *Modification des catégories et de leurs attributs*, page 175
- *Filtrage par mots-clés*, page 180
- *Redéfinition du filtrage pour des sites spécifiques*, page 182

En plus des catégories définies par Websense et présentes dans la base de données principale (plus de 90), vous pouvez définir vos propres **catégories personnalisées** pour obtenir un filtrage et des rapports plus précis. Créez par exemple des catégories personnalisées telles que :

- **Voyage d'affaires**, pour regrouper des sites d'agences de voyage approuvées que les employés peuvent utiliser pour acheter leurs billets d'avion, louer une voiture et réserver un hôtel.
- **Matériaux de référence**, pour regrouper les sites d'encyclopédies et de dictionnaires en ligne considérés comme appropriés pour les élèves des écoles primaires.
- **Développement professionnel**, pour regrouper les sites de formation et d'autres ressources que les employés sont encouragés à utiliser pour développer leurs compétences.

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories > Ajouter une catégorie** permet d'ajouter des catégories personnalisées à toute catégorie parente. Vous pouvez créer jusqu'à 100 catégories personnalisées.

1. Entrez un **Nom de catégorie** descriptif et unique. Le nom ne doit pas inclure les caractères suivants :

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

2. Entrez la **Description** de la nouvelle catégorie.

   Les restrictions de caractères qui s'appliquent aux noms de filtre s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).

3. Sélectionnez une catégorie parente dans la liste **Ajouter à**. Par défaut, l'option **Toutes les catégories** est sélectionnée.
4. Entrez les sites (URL ou adresses IP) à ajouter à cette catégorie. Pour plus d'informations, consultez *Recatégorisation d'URL*, page 184.

   Vous pourrez également modifier cette liste après la création de la catégorie.
5. Entrez les mots-clés que vous souhaitez associer à cette catégorie. Pour plus d'informations, consultez *Filtrage par mots-clés*, page 180.

   Vous pourrez également modifier cette liste après la création de la catégorie.
6. Définissez une **Action** de filtrage par défaut à appliquer à cette catégorie dans tous les filtres de catégories existants. Vous pourrez ensuite modifier cette action dans les filtres individuels.

   > **Remarque**
   > Les filtres de catégories copiés dans un rôle d'administration déléguée définissent l'action de filtrage sur Autoriser pour les catégories personnalisées créées dans ce rôle. Il est préférable que les administrateurs délégués actualisent les filtres de catégories copiés afin de définir l'action désirée pour les catégories personnalisées propres à leur rôle.

7. Activez éventuellement les actions de **Filtrage avancé** (blocage par mots-clés, par types de fichiers ou par bande passante) devant être appliquées à cette catégorie dans tous les filtres de catégories existants.

8. Lorsque vos modifications sont terminées, cliquez sur **OK** pour mettre les modifications en cache et revenir à la page Modifier les catégories. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

La nouvelle catégorie est ajoutée dans la liste des catégories et les informations d'URL personnalisées et de mots-clés de la catégorie s'affichent.

Filtrage par mots-clés

Rubriques connexes :

- *Recatégorisation d'URL*, page 184
- *Configuration des paramètres de filtrage de Websense*, page 56
- *Création d'un filtre de catégories*, page 49
- *Modification d'un filtre de catégories*, page 50
- *Fonctionnement des catégories*, page 175

Les mots-clés sont associés à des catégories, puis utilisés pour assurer une protection contre les sites qui n'ont pas été explicitement ajoutés dans la base de données principale ni définis comme URL personnalisée. L'activation du blocage par mots-clés comprend trois étapes :

1. Activez le blocage par mots-clés au niveau global (voir *Configuration des paramètres de filtrage de Websense*, page 56).
2. Définissez les mots-clés associés à une catégorie (voir *Définition des mots-clés*, page 181).
3. Activez le blocage par mots-clés pour la catégorie dans le filtre de catégories actif (voir *Modification d'un filtre de catégories*, page 50).

Lorsque des mots-clés ont été définis et le blocage par mots-clés activé pour une catégorie spécifique, Websense bloque tout site dont l'URL contient un mot-clé associé et journalise le site comme appartenant à la catégorie spécifiée. Le site est bloqué même si d'autres URL de la catégorie sont autorisées.

Par exemple, si la catégorie Sports est autorisée dans un filtre de catégories actif mais que vous souhaitez bloquer l'accès aux sites traitant du basket-ball, vous pouvez associer le mot-clé « nba » à la catégorie Sports et activer le blocage par mots-clés. Les URL suivantes sont alors bloquées et journalisées comme appartenant à la catégorie Sports :

- sports.espn.go.com/**nba**/
- moder**nba**kery.com
- moder**nba**biesandchildren.com
- fashio**nba**r.com

Définissez les mots-clés avec précaution afin d'éviter tout blocage non intentionnel.

> **Important**
> Si vous utilisez Websense Web Security, évitez d'associer des mots-clés à l'une des sous-catégories de la protection étendue. Le blocage par mots-clés ne s'applique pas à ces catégories.

Lorsqu'une requête est bloquée par un mot-clé, la page de blocage Websense reçue par l'utilisateur le signale.

Définition des mots-clés

Rubriques connexes :

- *Modification d'un filtre de catégories*, page 50
- *Fonctionnement des catégories*, page 175
- *Filtrage par mots-clés*, page 180
- *Utilisation d'expressions régulières*, page 196

Un mot-clé est une chaîne de caractères (par exemple un mot, une phrase ou un acronyme) pouvant se trouver dans une URL. Affectez des mots-clés à une catégorie, puis activez le blocage par mots-clés dans un filtre de catégories.

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories > Ajouter des mots-clés** permet d'associer des mots-clés à des catégories. Pour modifier la définition d'un mot-clé, utilisez la page **Modifier les mots-clés**.

Définissez les mots-clés avec précaution afin d'éviter tout blocage non intentionnel. Par exemple, si vous utilisez le mot clé « sex » pour bloquer l'accès aux sites réservés aux adultes, vous pouvez également bloquer les requêtes des moteurs de recherche pour des termes comme Sextuplé ou Ville d'Essex, et des sites comme m**sex**change.org (Informatique), vega**sex**perience.com (Voyage) et sci.esa.int/mar**sex**press (Institutions Scolaires).

Entrez un mot-clé par ligne.

- N'insérez pas d'espaces dans les mots-clés. Les chaînes URL et CGI ne contiennent jamais d'espace entre les mots.
- Insérez une barre oblique inversée (\) avant les caractères spéciaux tels que :

  ```
  . , # ? * +
  ```

  Si vous n'insérez pas le caractère barre oblique inversée, Websense ignore le caractère spécial.
- Si vous utilisez Websense Web Security, évitez d'associer des mots-clés à l'une des sous-catégories de la protection étendue. Le blocage par mots-clés ne s'applique pas à ces catégories.

Lorsque les ajouts ou les modifications sont terminé(e)s, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Modifier les catégories. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour que le blocage par mots-clés soit imposé, vous devez également :

1. Activer le blocage par mots-clés via la page **Paramètres > Filtrage** (voir *Configuration des paramètres de filtrage de Websense*, page 56).
2. Activer le blocage par mots-clés dans un ou plusieurs filtres de catégories actifs (voir *Modification d'un filtre de catégories*, page 50).

Redéfinition du filtrage pour des sites spécifiques

Rubriques connexes :

- *Création d'une catégorie personnalisée*, page 178
- *Filtrage par mots-clés*, page 180
- *Définition d'URL non filtrées*, page 183
- *Recatégorisation d'URL*, page 184

Les URL personnalisées vous permettent d'effectuer les opérations suivantes :

- Affiner le filtrage des sites qui n'apparaissent pas dans la base de données principale Websense. Par défaut, l'action appliquée à la catégorie **Divers\Non catégorisé** est utilisée pour filtrer ces sites.
- Filtrer les sites autrement qu'en fonction de leur catégorie dans la base de données principale.

Websense recherche d'abord les définitions d'URL personnalisées pour un site avant de consulter la base de données principale. Il filtre donc le site en fonction de la catégorie affectée à l'URL personnalisée.

Il existe deux types d'URL personnalisées : non filtrées et recatégorisées.

- Les URL non filtrées sont autorisées pour tous les utilisateurs non gérés par le filtre Bloquer tout ou un filtre d'accès limité (voir *Définition d'URL non filtrées*, page 183).
- Les URL recatégorisées ont été déplacées de leur catégorie par défaut dans la base de données principale vers une autre catégorie définie par Websense ou personnalisée (voir *Recatégorisation d'URL*, page 184).

  Une URL recatégorisée n'est pas bloquée par défaut. Elle est filtrée en fonction de l'action appliquée à sa nouvelle catégorie dans chaque filtre de catégories actif.

Lorsqu'un site est filtré en fonction de sa catégorie dans la base de données principale, Websense établit la correspondance entre l'URL et son adresse IP équivalente. Ce n'est pas le cas pour les URL personnalisées. Pour modifier le filtrage d'un site, définissez à la fois son URL et son adresse IP en tant qu'URL personnalisée.

Si un site est accessible par plusieurs URL, définissez chaque URL susceptible d'être utilisée pour accéder au site en tant qu'URL personnalisée pour vous assurer que le site est autorisé ou bloqué comme prévu.

Lorsqu'un site est déplacé vers un nouveau domaine et qu'une redirection HTTP renvoie les utilisateurs vers la nouvelle URL, cette dernière n'est pas automatiquement filtrée de la même façon que le site à l'origine de la redirection. Pour vous assurer que le site soit filtré de façon appropriée avec sa nouvelle adresse, créez une nouvelle URL personnalisée.

Définition d'URL non filtrées

Rubriques connexes :

- *Fonctionnement des catégories*, page 175
- *Redéfinition du filtrage pour des sites spécifiques*, page 182
- *Recatégorisation d'URL*, page 184

La page **Gestion des stratégies > Composants de filtre > URL non filtrées** permet de définir la liste des sites accessibles à tous les utilisateurs, à l'exception des sites gérés par le filtre de catégories Bloquer tout ou par un filtre d'accès limité.

La liste **Sites autorisés**, située dans la partie droite du panneau de contenu, répertorie les sites non filtrés (URL et adresses IP) et les expressions régulières que vous avez définies (voir *Utilisation d'expressions régulières*, page 196). Chaque site est associé à une catégorie.

- L'URL peut être associée à sa catégorie dans la base de données principale ou recatégorisée.
- Lorsqu'un utilisateur demande à accéder à l'URL non filtrée, la requête est journalisée en tant qu'URL personnalisée autorisée dans la catégorie dans laquelle elle a été affectée.

Pour ajouter une URL non filtrée :

1. Sous **Définissez les URL non filtrées**, entrez une URL ou une adresse IP par ligne, puis cliquez sur la flèche droite (>).

   Websense n'effectue pas la correspondance entre une URL personnalisée et son adresse IP équivalente. Pour autoriser à la fois l'URL et l'adresse IP d'un site, ajoutez-les toutes les deux dans la liste des URL non filtrées.
2. Pour ajouter des expressions régulières correspondant à plusieurs sites, cliquez sur **Avancé**. Entrez une expression régulière par ligne, puis cliquez sur la flèche droite pour déplacer les expressions vers la liste des URL non filtrées. Pour vérifier qu'une expression régulière correspond aux sites prévus, cliquez sur **Test**.

   Pour plus d'informations, consultez *Utilisation d'expressions régulières*, page 196.
3. Lorsque vous avez terminé, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Modifier les catégories. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour supprimer un site de la liste des URL non filtrées, sélectionnez l'URL, l'adresse IP ou l'expression régulière, puis cliquez sur **Supprimer**.

Recatégorisation d'URL

Rubriques connexes :

- *Fonctionnement des catégories*, page 175
- *Redéfinition du filtrage pour des sites spécifiques*, page 182
- *Définition d'URL non filtrées*, page 183

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories > Recatégoriser les URL** permet d'ajouter des sites individuels dans n'importe quelle catégorie. Pour modifier les sites recatégorisés existants, utilisez la page **Modifier des URL**.

Pour modifier la façon dont les sites individuels sont filtrés et journalisés, recatégorisez les URL. Lorsque vous ajoutez des sites recatégorisés :

- Entrez chaque URL ou adresse IP sur une ligne distincte.
- Incluez le protocole des sites non HTTP. Si vous ne précisez pas le protocole, Websense filtre le site en tant que site HTTP.

  Pour les sites HTTPS, incluez également le numéro de port (https://63.212.171.196:443/, https://www.onlinebanking.com:443/).
- Websense reconnaît les URL personnalisées exactement telles qu'elles ont été saisies. Si la catégorie Moteurs de recherche et portails est bloquée, mais que vous classez **www.yahoo.com** dans une catégorie autorisée, le site n'est autorisé que si les utilisateurs tapent l'adresse complète. Si l'utilisateur tape images.search.yahoo.com ou seulement yahoo.com, le site reste bloqué. Toutefois, si vous recatégorisez **yahoo.com**, tous les sites dont l'adresse contient yahoo.com sont autorisés.

Lorsque les ajouts ou les modifications sont terminé(e)s, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Modifier les catégories. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Après avoir enregistré les URL recatégorisées, utilisez l'outil **Catégorie d'URL** situé dans le panneau de raccourcis pour vérifier que le site est affecté à la catégorie appropriée. Voir *Utilisation de la boîte à outils pour vérifier le comportement du filtrage*, page 197.

Fonctionnement des protocoles

La base de données principale Websense contient les définitions de protocoles utilisées pour filtrer les protocoles Internet autres que HTTP, HTTPS et FTP. Ces

définitions comprennent les applications Internet et les méthodes de transfert de données, telles que celles utilisées pour la messagerie instantanée, la diffusion multimédia (streaming), le partage et le transfert de fichiers, la messagerie Internet et diverses autres opérations de base de données ou de réseau.

Ces définitions de protocoles peuvent même être utilisées pour filtrer les applications ou les protocoles qui contournent un pare-feu en créant un tunnel à travers les ports habituellement utilisés par le trafic HTTP. Les données de messagerie instantanée, par exemple, peuvent entrer dans un réseau dont le pare-feu bloque les protocoles de messagerie instantanée en créant un tunnel via les ports HTTP. Websense identifie précisément ces protocoles et les filtre en fonction des stratégies que vous configurez.

> **Remarque**
> L'agent Network Agent doit être installé pour que le filtrage à base de protocoles puisse s'effectuer.

Outre les définitions de protocole définies par Websense, vous pouvez définir des protocoles personnalisés pour le filtrage. Les définitions de protocoles personnalisées peuvent être basées sur les adresses IP ou sur les numéros de port, et peuvent être modifiées.

Pour bloquer le trafic passant par un port spécifique, associez le numéro de ce port à un protocole personnalisé, puis attribuez à ce dernier l'action par défaut **Bloquer**.

Pour utiliser des définitions de protocoles personnalisées, sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Protocoles**. Pour plus d'informations, consultez les sections *Modification des protocoles personnalisés*, page 186 et *Création d'un protocole personnalisé*, page 189.

Filtrage des protocoles

Rubriques connexes :

- *Fonctionnement des protocoles*, page 184
- *Modification des protocoles personnalisés*, page 186
- *Création d'un protocole personnalisé*, page 189
- *Ajout ou modification d'identificateurs de protocole*, page 187
- *Ajout à un protocole défini par Websense*, page 191

Lorsque l'agent Network Agent est installé, Websense peut bloquer le contenu Internet transmis via certains ports ou certaines adresses IP, ou marqué par des signatures particulières, quelle que soit la nature des données. Par défaut, le blocage d'un port

intercepte tout le contenu Internet entrant dans votre réseau par ce port, quelle qu'en soit la source.

> **Remarque**
> Il peut arriver que le trafic réseau interne envoyé par un port particulier ne soit pas bloqué, même lorsque le protocole qui utilise ce port l'est. Le protocole peut envoyer les données via un serveur interne plus vite que Network Agent ne peut capturer et traiter les données. Cela ne se produit pas avec les données provenant de l'extérieur du réseau.

Lorsqu'une demande de protocole intervient, Websense utilise la procédure suivante pour déterminer si elle doit être bloquée ou autorisée :

1. Il identifie le nom du protocole (ou de l'application Web).
2. Il identifie le protocole en fonction de l'adresse de destination demandée.
3. Il recherche des numéros de port ou des adresses IP associé(e)s dans les définitions de protocoles personnalisées.
4. Il recherche des numéros de port, des adresses IP ou des signatures associé(e)s dans les définitions de protocoles définies par Websense.

Si Websense ne trouve aucune de ces informations, l'ensemble du contenu associé au protocole est autorisé.

Modification des protocoles personnalisés

Rubriques connexes :

- *Fonctionnement des protocoles*, page 184
- *Création d'un protocole personnalisé*, page 189
- *Création d'un filtre de protocoles*
- *Modification d'un filtre de protocoles*
- *Fonctionnement des catégories*

La page **Gestion des stratégies > Composants de filtre > Modifier les protocoles** permet de créer et de modifier les définitions de protocoles personnalisées et de revoir les définitions de protocoles définies par Websense. Les définitions de protocoles définies par Websense ne sont pas modifiables.

La liste Protocoles comprend tous les protocoles personnalisés et définis par Websense. Cliquez sur un protocole ou sur un groupe de protocoles pour obtenir des informations sur l'élément sélectionné dans la partie droite du panneau de contenu.

Pour ajouter un nouveau protocole personnalisé, cliquez sur **Ajouter un protocole** et poursuivez l'opération avec la section *Création d'un protocole personnalisé*, page 189.

Pour modifier une définition de protocole :

1. Sélectionnez le protocole dans la liste Protocoles. La définition du protocole s'affiche à droite de la liste.
2. Cliquez sur **Remplacer l'action** pour modifier l'action de filtrage appliquée à ce protocole dans tous les filtres de protocoles (voir *Modification du filtrage global des protocoles*, page 188).
3. Cliquez sur **Ajouter un identificateur** pour définir d'autres identificateurs de protocole pour ce protocole (voir *Ajout ou modification d'identificateurs de protocole*, page 187).
4. Sélectionnez un identificateur dans la liste, puis cliquez sur **Éditer** pour modifier le **Port**, la **Plage d'adresses IP** ou la **Méthode de transport** défini(e) par cet identificateur.
5. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour supprimer une définition de protocole, sélectionnez un élément dans la liste Protocoles, puis cliquez sur **Supprimer**.

Ajout ou modification d'identificateurs de protocole

La page **Composants de filtre > Modifier les protocoles > Ajouter un identificateur de protocole** permet de définir d'autres identificateurs pour un protocole personnalisé existant. Pour modifier un identificateur défini précédemment, utilisez la page **Modifier l'identificateur de protocole**.

Avant de créer ou de modifier un identificateur, vérifiez que le nom du protocole approprié s'affiche à côté de **Protocole sélectionné**.

Lorsque vous utilisez des identificateurs de protocole, n'oubliez pas qu'un critère au moins (port, adresse IP ou méthode de transport) doit être unique pour chaque protocole.

1. Spécifiez les **Ports** inclus pour cet identificateur.
   - Si vous sélectionnez **Tous les ports**, ce critère se superpose à tous les autres ports ou adresses IP saisi(e)s dans les autres définitions de protocoles.
   - Les plages de ports ne sont pas considérées comme uniques lorsqu'elles se chevauchent. Par exemple, la plage de ports 80-6000 chevauche la plage 4000-9000.
   - Soyez prudent(e) lorsque vous définissez un protocole sur le port 80 ou 8080 car Network Agent écoute les requêtes Internet sur ces ports.

     Les protocoles personnalisés étant prioritaires sur les protocoles Websense, si vous définissez un protocole personnalisé à l'aide du port 80, tous les autres protocoles qui utilisent le port 80 sont filtrés et journalisés comme le protocole personnalisé.
2. Spécifiez les **Adresses IP** incluses dans cet identificateur.

- Si vous sélectionnez **Toutes les adresses IP externes**, ce critère se superpose à toutes les autres adresses IP saisies dans les autres définitions de protocoles.
- Les plages d'adresses IP ne sont pas considérées comme uniques lorsqu'elles se chevauchent.

3. Spécifiez la méthode de **Transport de protocole** incluse dans cet identificateur.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Modifier les protocoles. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Modification du nom d'un protocole personnalisé

La page **Composants de filtre > Modifier les protocoles > Renommer un protocole** permet de modifier le nom d'un protocole personnalisé ou de le déplacer vers un autre groupe de protocoles.

- Utilisez le champ **Nom** pour modifier le nom du protocole. Le nouveau nom ne doit pas dépasser 50 caractères.

  Le nom ne doit pas inclure les caractères suivants :

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- Pour déplacer le protocole vers un autre groupe, sélectionnez le nouveau groupe dans le champ **Dans le groupe**.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier les protocoles. Cliquez également sur **OK** dans la page Modifier les protocoles pour mettre vos modifications en cache.

Modification du filtrage global des protocoles

La page **Composants de filtre > Modifier les protocoles > Remplacer l'action** permet de modifier le filtrage d'un protocole dans tous les filtres de protocoles existants. Elle permet également de déterminer l'action appliquée par défaut au protocole dans les nouveaux filtres.

Bien que cette modification remplace l'action de filtrage appliquée dans tous les filtres de protocoles existants, les administrateurs peuvent ensuite modifier ces filtres pour appliquer une action différente.

1. Vérifiez que le nom du protocole approprié s'affiche à côté de **Protocole sélectionné**.
2. Sélectionnez une nouvelle **Action** (Autoriser ou Bloquer) à appliquer à ce protocole. Par défaut, l'option **Ne pas modifier l'action actuelle** est sélectionnée. Pour plus d'informations, consultez *Actions de filtrage*, page 44.
3. Définissez les nouvelles options de **Journalisation**. Le trafic des protocoles doit être journalisé pour apparaître dans les rapports et permettre les alertes d'utilisation de protocoles.

4. Précisez si **Bandwidth Optimizer** est utilisé pour gérer l'accès à ce protocole. Pour plus d'informations, consultez *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.

   Important
   Les modifications apportées ici affectent tous les filtres de protocoles existants à l'exception des filtres **Bloquer tout** et **Autoriser tout**.

5. Lorsque vous avez terminé, cliquez sur **OK** pour revenir à la page Modifier les protocoles (voir *Modification des protocoles personnalisés*, page 186). Cliquez également sur **OK** dans la page Modifier les protocoles pour mettre vos modifications en cache.

Création d'un protocole personnalisé

Rubriques connexes :

- *Fonctionnement des protocoles*, page 184
- *Filtrage des protocoles*, page 185
- *Modification des protocoles personnalisés*, page 186
- *Ajout à un protocole défini par Websense*, page 191

La page **Composants de filtre > Protocoles > Ajouter un protocole** permet de définir un nouveau protocole personnalisé.

1. Entrez le **Nom** du protocole.

   Le nom ne doit pas inclure les caractères suivants :

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Un protocole personnalisé peut porter le même nom qu'un protocole défini par Websense afin d'étendre le nombre d'adresses IP ou de ports associés au protocole original. Pour plus d'informations, consultez *Ajout à un protocole défini par Websense*, page 191.

2. Développez la liste déroulante **Ajouter un protocole à ce groupe** et sélectionnez un groupe de protocoles. Le nouveau protocole apparaît dans ce groupe pour tous les filtres et toutes les listes de protocoles.

3. Définissez un **Identificateur de protocole** unique (jeu de **ports**, **adresses IP** et **méthodes de transport**) pour ce groupe. Vous pouvez par la suite ajouter d'autres identificateurs depuis la page Modifier les protocoles.

   Pour créer des identificateurs de protocoles, suivez ces instructions :

   - Un critère au moins (port, adresse IP ou méthode de transport) doit être unique pour chaque définition de protocole.

- Si vous sélectionnez **Tous les ports** ou **Toutes les adresses IP externes**, ce critère se superpose à tout autre port ou adresse IP saisi(e) dans les autres définitions de protocoles.
- Les plages de ports ou d'adresses IP ne sont pas considérées comme uniques lorsqu'elles se chevauchent. Par exemple, la plage de ports 80-6000 chevauche la plage 4000-9000.

> **Remarque**
>
> Soyez prudent(e) lorsque vous définissez un protocole sur le port 80 ou 8080 car Network Agent écoute les requêtes Internet sur ces ports.
>
> Les protocoles personnalisés étant prioritaires sur les protocoles Websense, si vous définissez un protocole personnalisé à l'aide du port 80, tous les autres protocoles qui utilisent le port 80 sont filtrés et journalisés comme le protocole personnalisé.

Le tableau suivant présente des exemples de définitions de protocole valides et non valides :

Port	Adresse IP	Méthode de transport	Combinaison acceptée ?
70	N'IMPORTE LAQUELLE	TCP	Oui - le numéro de port rend chaque identificateur de protocole unique.
90	N'IMPORTE LAQUELLE	TCP	

Port	Adresse IP	Méthode de transport	Combinaison acceptée ?
70	N'IMPORTE LAQUELLE	TCP	Non - les adresses IP ne sont pas uniques. L'adresse 10.2.1.201 fait partie de l'ensemble N'IMPORTE LAQUELLE.
70	10.2.1.201	TCP	

Port	Adresse IP	Méthode de transport	Combinaison acceptée ?
70	10.2.3.212	TCP	Oui - les adresses IP sont uniques.
70	10.2.1.201	TCP	

4. Sous Action par défaut, définissez l'action par défaut (**Autoriser** ou **Bloquer**) devant s'appliquer à ce protocole dans tous les filtres de protocoles actifs :
   - Indiquez si le trafic qui utilise ce protocole doit être **journalisé**. Le trafic des protocoles doit être journalisé pour apparaître dans les rapports et permettre les alertes d'utilisation de protocoles.

- Indiquez si l'accès à ce protocole doit être régulé par **Bandwidth Optimizer** (voir *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191).

5. Lorsque vous avez terminé, cliquez sur **OK** pour revenir à la page Modifier les protocoles. La nouvelle définition de protocole apparaît dans la liste Protocoles.
6. Cliquez de nouveau sur **OK** pour mettre en cache vos modifications. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout à un protocole défini par Websense

Vous ne pouvez pas ajouter directement un numéro de port ou une adresse IP dans un protocole défini par Websense. Vous pouvez cependant créer un protocole personnalisé portant le même nom que le protocole défini par Websense, puis ajouter des ports ou des adresses IP à sa définition.

Lorsqu'un protocole personnalisé et un protocole défini par Websense portent le même nom, Websense surveille le trafic de protocoles au niveau des adresses IP et des ports spécifiés dans les définitions des deux protocoles.

Dans les rapports, les noms de protocoles personnalisés sont précédés de « C_ ». Par exemple, si vous créez un protocole personnalisé pour SQL_NET et spécifiez des numéros de port supplémentaires, les rapports affichent C_SQL_NET lorsque le protocole utilise les numéros de port du protocole personnalisé.

Utilisation de Bandwidth Optimizer pour gérer la bande passante

Rubriques connexes :

- *Fonctionnement des catégories*, page 175
- *Fonctionnement des protocoles*, page 184
- *Configuration des limites par défaut de Bandwidth Optimizer*, page 192

Lorsque vous créez un filtre de catégories ou de protocoles, vous pouvez choisir de limiter l'accès à une catégorie ou à un protocole en fonction de l'utilisation de la bande passante.

- Bloquez l'accès aux catégories ou aux protocoles en fonction de l'utilisation totale de la bande passante du réseau.
- Bloquez l'accès aux catégories en fonction de la bande passante totale utilisée par le trafic HTTP.
- Bloquez l'accès à un protocole spécifique en fonction de la bande passante utilisée par ce protocole.

Par exemple :

- Bloquez le protocole AOL Instant Messager (AIM) lorsque l'utilisation totale de la bande passante du réseau dépasse 50 % de la bande passante disponible, ou lorsque l'utilisation actuelle de la bande passante pour AIM dépasse 10 % de la bande passante totale du réseau.
- Bloquez la catégorie Sports lorsque l'utilisation totale de la bande passante du réseau atteint 75 %, ou lorsque la bande passante utilisée par l'ensemble du trafic HTTP atteint 60 % de la bande passante disponible.

L'utilisation de la bande passante des protocoles comprend le trafic passant par tous les ports, adresses IP ou signatures défini(e)s pour le protocole. Cela signifie que, lorsqu'un protocole ou une application Internet utilise plusieurs ports pour le transfert des données, le trafic traversant tous les ports inclus dans la définition du protocole est compté dans l'utilisation totale de la bande passante de ce protocole. Par contre, lorsqu'une application Web utilise un port non inclus dans la définition du protocole, le trafic passant par ce port n'est pas inclus dans les mesures d'utilisation de la bande passante.

Websense enregistre la bande passante utilisée par les protocoles filtrés de type TCP et UDP.

Websense, Inc. actualise régulièrement les définitions des protocoles Websense pour assurer la précision des mesures de bande passante.

Network Agent envoie les données de bande passante du réseau à Filtering Service à intervalles prédéfinis. Websense surveille ainsi plus précisément l'utilisation de la bande passante et reçoit des mesures plus proches de la moyenne.

Lorsque les options de filtrage par bande passante sont actives, Websense commence le filtrage de bande passante 10 minutes après la configuration initiale et 10 minutes après chaque redémarrage de Websense Policy Server. Ce délai assure une mesure précise des données de bande passante et de l'utilisation de ces données dans le filtrage.

Lorsqu'une requête est bloquée par des limites de bande passante, la page de blocage Websense affiche cette information dans le champ **Raison**. Pour plus d'informations, consultez *Pages de blocage*, page 85.

Configuration des limites par défaut de Bandwidth Optimizer

Rubriques connexes :

- *Modification d'un filtre de catégories*, page 50
- *Modification d'un filtre de protocoles*, page 52
- *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191

Avant de définir les paramètres de bande passante dans des stratégies, vérifiez les seuils de bande passante par défaut qui déclenchent les paramètres de filtrage de la bande passante. Les valeurs définies par Websense sont :

- Bande passante par défaut du réseau : **50%**
- Bande passante par défaut par protocole : **20%**

Les valeurs de bande passante par défaut sont stockées par Policy Server et imposées par toutes les instances associées de Network Agent. Si vous utilisez plusieurs serveurs Policy Server, les modifications apportées aux valeurs de bande passante par défaut sur un Policy Server n'affectent pas les autres Policy Server.

Pour modifier les valeurs de bande passante par défaut :

1. Dans Websense Manager, sélectionnez **Paramètres > Filtrage**.
2. Entrez les seuils d'utilisation de bande passante déclenchant le filtrage de la bande passante lorsque ce type de filtrage est activé.
   - Lorsqu'une catégorie ou un protocole est bloqué(e) en fonction du trafic sur l'ensemble du réseau, **Bande passante par défaut pour le réseau** définit le seuil de filtrage par défaut.
   - Lorsqu'une catégorie ou un protocole est bloqué(e) en fonction du trafic lié au protocole, **Bande passante par défaut par protocole** définit le seuil de filtrage par défaut.

   Vous pouvez remplacer les valeurs de seuil par défaut pour chaque catégorie ou protocole dans tous les filtres de protocoles ou de catégories.
3. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Toutes les modifications apportées aux valeurs par défaut ont un effet potentiel sur les filtres de catégories ou de protocoles qui imposent les restrictions de Bandwidth Optimizer.

- Pour gérer l'utilisation de la bande passante associée à un protocole particulier, modifiez le ou les filtres de protocoles actifs.
- Pour gérer l'utilisation de la bande passante associée à une catégorie d'URL particulière, modifiez le ou les filtres de catégories appropriés.

  Lorsque vous filtrez des catégories en fonction de l'utilisation de la bande passante HTTP, Websense mesure l'utilisation totale de la bande passante HTTP sur tous les sports spécifiés en tant que ports HTTP pour Websense.

Gestion du trafic en fonction du type de fichiers

Lorsque vous créez un filtre de catégories, vous pouvez définir un filtrage en fonction des extensions de fichier, en limitant l'accès à des types de fichier particulier des sites de certaines catégories. Par exemple, vous pouvez autoriser l'accès à la catégorie Sports, tout en bloquant l'accès aux fichiers vidéo de cette catégorie.

Websense propose plusieurs types de fichiers prédéfinis ou de regroupements d'extensions de fichier utilisés dans un but similaire. Ces définitions de types de

fichiers sont stockées dans la base de données principale et peuvent être modifiées lors du processus de mise à jour de cette base de données.

Vous pouvez implémenter un filtrage à l'aide de types de fichiers prédéfinis, modifier les définitions des types de fichiers existantes ou créer de nouveaux types de fichiers. Vous ne pouvez cependant pas supprimer les types de fichiers définis par Websense ni les extensions de fichiers associées à ces derniers.

Lorsqu'un utilisateur demande un site, Websense commence par identifier la catégorie de ce site, puis recherche les extensions de fichier filtrées.

> **Remarque**
> Pour implémenter un filtrage complet des supports Internet vidéo et audio, combinez un filtrage basé sur les protocoles avec un filtrage des types de fichiers. Dans ce cas, le filtrage de protocoles traite les supports en temps réel, pendant que le filtrage de types de fichiers traite les fichiers pouvant être téléchargés et lus.

Lorsqu'un utilisateur tente d'accéder à un fichier dont l'extension est bloquée, le champ **Raison** de la page de blocage Websense indique que le type de fichier a été bloqué. Pour plus d'informations, consultez *Pages de blocage*, page 85.

> **Remarque**
> La page de blocage standard ne s'affiche pas lorsqu'une image GIF ou JPEG bloquée se compose d'une partie seulement de page autorisée, mais la zone de l'image s'affiche vide. Cela permet d'éviter l'affichage d'une petite partie de page de blocage en plusieurs emplacements d'une page sinon autorisée.

Les définitions de types de fichiers peuvent contenir aussi peu d'extensions de fichier que nécessaire pour le filtrage. Les types de fichiers définis par Websense, par exemple, comprennent les extensions suivantes :

Audio	Fichiers compressés		Exécutables	Vidéo	
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra
.mid	.bhx	.tgz		.m1v	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx

Audio	Fichiers compressés		Exécutables	Vidéo	
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

Toutes les extensions de fichiers associées à un type de fichier défini par Websense peuvent être ajoutées à un type de fichier personnalisé. L'extension de fichier est ensuite filtrée et journalisée en fonction des paramètres associés au type de fichier personnalisé.

Pour afficher les définitions de types de fichiers existantes, modifier des types de fichiers ou créer des types de fichiers personnalisés, sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Types de fichiers**. Pour plus d'informations, consultez *Fonctionnement des types de fichiers*, page 195.

Fonctionnement des types de fichiers

Rubriques connexes :

- *Gestion du trafic en fonction du type de fichiers*, page 193
- *Modification d'un filtre de catégories*, page 50
- *Filtrage d'un site*, page 81

La page **Gestion des stratégies > Composants de filtre > Modifier les types de fichiers** permet de créer et de gérer jusqu'à 32 **types de fichiers**. Les types de fichiers sont des groupes d'extensions de fichiers pouvant être explicitement bloquées dans les filtres de catégories (voir *Gestion du trafic en fonction du type de fichiers*, page 193).

- Cliquez sur un type de fichiers pour voir les extensions qui lui sont associées.
- Pour ajouter des extensions au type de fichiers sélectionné, cliquez sur **Ajouter des extensions**, puis passez à la section *Ajout d'extensions de fichier à un type de fichiers*, page 196 pour d'autres instructions.
- Pour créer un nouveau type de fichiers, cliquez sur **Ajouter un type de fichier**, puis passez à la section *Ajout de types de fichiers personnalisés*, page 196 pour d'autres instructions.
- Pour supprimer une extension ou un type de fichiers personnalisé, sélectionnez un élément, puis cliquez sur **Supprimer**.

  Vous ne pouvez pas supprimer les types de fichiers définis par Websense ni les extensions de fichiers associées à ces derniers.

  Vous pouvez cependant ajouter les extensions de fichiers associées à un type de fichiers défini par Websense à un type de fichiers personnalisé. L'extension de fichier est ensuite filtrée et journalisée en fonction des paramètres associés au type

de fichier personnalisé. Vous ne pouvez pas ajouter la même extension à plusieurs types de fichiers personnalisés.

Lorsque vos modifications sont terminées, cliquez sur **OK**. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout de types de fichiers personnalisés

La page **Composants > Modifier les types de fichiers > Ajouter un type de fichier** permet de définir des types de fichiers personnalisés.

1. Entrez un **Nom de type de fichier** unique.

   Vous pouvez créer un type de fichiers personnalisé portant le même nom qu'un type de fichiers défini par Websense pour ajouter d'autres extensions de fichiers au type de fichiers existant.
2. Entrez les extensions de fichier, une par ligne, dans la liste **Extensions de fichier**. Il n'est pas nécessaire d'ajouter le point (« . ») avant chaque extension.
3. Cliquez sur **OK** pour revenir à la page Modifier les types de fichiers. Le nouveau type de fichier apparaît dans la liste Types de fichier.
4. Lorsque vos modifications sont terminées, cliquez sur **OK** dans la page Modifier les types de fichiers. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout d'extensions de fichier à un type de fichiers

La page **Composants de filtre > Modifier les types de fichiers > Ajouter des extensions de fichier** permet d'ajouter des extensions de fichier au type de fichiers sélectionné.

1. Vérifiez que le nom du type de fichiers approprié s'affiche à côté de **Type de fichier sélectionné**.
2. Entrez les extensions de fichier, une par ligne, dans la liste **Extensions de fichier**. Il n'est pas nécessaire d'ajouter le point (« . ») avant chaque extension.
3. Cliquez sur **OK** pour revenir à la page Modifier les types de fichiers. Les nouvelles extensions de fichier apparaissent dans la liste Personnaliser des extensions de fichiers.
4. Lorsque vos modifications sont terminées, cliquez sur **OK** dans la page Modifier les types de fichiers. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Utilisation d'expressions régulières

Une **expression régulière** est un modèle utilisé pour remplacer plusieurs chaînes ou groupes de caractères. Vous pouvez utiliser des expressions régulières dans des filtres d'accès limité ou pour définir des mots-clés ou des URL personnalisées. Websense

s'efforce ensuite de trouver une correspondance au modèle général plutôt qu'à un seul mot-clé ou à une seule URL spécifique.

Prenons l'exemple de cette simple expression régulière :

```
domaine.(com|org|net)
```

Ce modèle d'expression correspond aux URL :

- domaine.com
- domaine.org
- domaine.net

Les expressions régulières doivent être utilisées avec précaution. Elles fournissent un puissant outil de filtrage mais peuvent facilement autoriser ou bloquer l'accès à des sites non prévus. De même, les expressions régulières mal construites peuvent entraîner un filtrage excessif.

Important

L'utilisation d'expressions régulières comme critères de filtrage peut accroître la surcharge du processeur. Selon les tests, 100 expressions régulières augmentent de 20 % l'utilisation moyenne du processeur sur l'ordinateur Filtering Service.

Websense prend en charge la syntaxe des expressions régulières Perl, à quelques exceptions près. Une partie de la syntaxe non prise en charge n'est pas utile pour les correspondances de chaînes détectées dans une URL.

La syntaxe des expressions régulières non prise en charge comprend :

```
(?<=pattern)string
\N{name}
(?(condition)pat1)
(?(condition)pat1|pat2)
(?{code})
(?<!pattern)string
(?imsx-imsx)
\pP
\PP
??{code})
```

Pour plus d'informations sur les expressions régulières, consultez les sites :

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

Utilisation de la boîte à outils pour vérifier le comportement du filtrage

Le panneau de raccourcis droit de Websense Manager comprend une **Boîte à outils** qui vous permet de vérifier rapidement la configuration de votre filtrage.

Cliquez sur le nom d'un outil pour y accéder. Cliquez de nouveau sur le nom pour afficher la liste des outils. Pour plus d'informations sur l'utilisation d'un outil, consultez :

- *Catégorie d'URL*, page 198
- *Vérifier la stratégie*, page 198
- *Tester le filtrage*, page 199
- *Accès à l'URL*, page 199
- *Analyser l'utilisateur*, page 199

Vous pouvez également cliquer sur **Portail de support** pour accéder au site Web du support technique de Websense dans un nouvel onglet ou une nouvelle fenêtre du navigateur. Le Portail de support vous permet d'utiliser la base de connaissances pour accéder à des didacticiels, des conseils, des articles et de la documentation.

Catégorie d'URL

Pour savoir comment un site est actuellement classé :

1. Cliquez sur **Catégorie d'URL** dans la boîte à outils.
2. Entrez une URL ou une adresse IP.
3. Cliquez sur **Aller**.

La catégorie actuelle du site s'affiche dans une fenêtre contextuelle. Si votre organisation a recatégorisé l'URL, la nouvelle catégorie est affichée.

La catégorisation du site peut varier selon la version de la base de données principale utilisée (y compris des mises à jour en temps réel).

Vérifier la stratégie

Servez-vous de cet outil pour identifier les stratégies s'appliquant à un client spécifique. Les résultats ne concernent que l'heure et la date en cours.

1. Cliquez sur **Vérifier la stratégie** dans la boîte à outils.
2. Pour identifier un répertoire ou un client ordinateur, entrez :
   - Un nom d'utilisateur complet

     Pour localiser l'utilisateur dans l'annuaire, cliquez sur **Rechercher un utilisateur** (voir *Identification d'un utilisateur pour vérifier la stratégie ou tester le filtrage*, page 200).
   - Une adresse IP
3. Cliquez sur **Aller**.

Le nom d'une ou plusieurs stratégies s'affiche dans une fenêtre contextuelle. Plusieurs stratégies s'affichent lorsque aucune d'elles n'a été affectée à l'utilisateur alors que des stratégies ont été affectées à plusieurs groupes, domaines ou unités d'organisation dont l'utilisateur est membre.

Même lorsque plusieurs stratégies apparaissent, une seule s'applique à l'utilisateur à un moment donné (voir *Ordre du filtrage*, page 80).

Tester le filtrage

Pour savoir ce qu'il se passe lorsqu'un client spécifique demande un site particulier :

1. Cliquez sur **Tester le filtrage** dans la boîte à outils.
2. Pour identifier un répertoire ou un client ordinateur, entrez :
   - Un nom d'utilisateur complet

     Pour localiser l'utilisateur dans l'annuaire, cliquez sur **Rechercher un utilisateur** (voir *Identification d'un utilisateur pour vérifier la stratégie ou tester le filtrage*, page 200).
   - Une adresse IP
3. Entrez l'URL ou l'Adresse IP du site à vérifier.
4. Cliquez sur **Aller**.

La catégorie du site, l'action appliquée à la catégorie et la raison de l'action apparaissent dans une fenêtre contextuelle.

Accès à l'URL

Pour savoir si des utilisateurs ont tenté d'accéder à un site au cours des deux dernières semaines, date du jour comprise :

1. Cliquez sur **Accès à l'URL** dans la boîte à outils.
2. Entrez une partie ou la totalité de l'URL ou de l'adresse IP du site à vérifier.
3. Cliquez sur **Aller**.

Un rapport d'investigation montre si des utilisateurs ont accédé au site et, dans l'affirmative, à quel moment.

Vous pouvez utiliser cet outil après réception d'une alerte de sécurité afin de voir si votre organisation a été exposée au phishing ou à des sites infectés par des virus.

Analyser l'utilisateur

Pour découvrir l'historique de l'activité Internet d'un utilisateur au cours des deux dernières semaines, date du jour non comprise :

1. Cliquez sur **Analyser l'utilisateur** dans la boîte à outils.
2. Entrez une partie ou la totalité d'un nom d'utilisateur ou d'une adresse IP d'ordinateur.
3. Cliquez sur **Aller**.

L'historique de l'utilisation du client apparaît dans un rapport d'investigation.

Identification d'un utilisateur pour vérifier la stratégie ou tester le filtrage

Utilisez la page **Rechercher un utilisateur** pour identifier un client utilisateur (répertoire) pour l'outil Vérifier la stratégie ou Tester le filtrage.

La page s'ouvre avec l'option **Utilisateur** sélectionnée. Développez le dossier **Entrées de l'annuaire** pour parcourir l'annuaire, ou cliquez sur **Rechercher**. La fonction de recherche n'est disponible que si vous utilisez un service d'annuaire de type LDAP.

Pour rechercher un utilisateur dans l'annuaire :

1. Entrez une partie ou la totalité du **Nom** de l'utilisateur.
2. Développez l'arborescence **Entrées de l'annuaire** et localisez un contexte de recherche.

   Pour définir le contexte, vous devez cliquer sur un dossier (DC, OU ou CN). Le champ situé sous l'arborescence est alors renseigné.
3. Cliquez sur **Rechercher**. Les entrées correspondant à votre terme de recherche apparaissent sous **Résultats de la recherche**.
4. Cliquez sur un nom d'utilisateur pour sélectionner un utilisateur ou sur **Rechercher encore** pour entrer un nouveau terme de recherche ou un nouveau contexte.

   Pour parcourir à nouveau l'annuaire, cliquez sur **Annuler la recherche**.
5. Lorsque le nom d'utilisateur complet approprié s'affiche dans le champ **Utilisateur**, cliquez sur **Aller**.

Si vous utilisez l'outil Tester le filtrage, assurez-vous qu'une URL ou une adresse IP s'affiche dans le champ **URL** avant de cliquer sur **Aller**.

Pour identifier un client ordinateur plutôt qu'un utilisateur, cliquez sur **Adresse IP**.

10 Identification des utilisateurs

Pour appliquer des stratégies à des utilisateurs et des groupes, Websense doit pouvoir identifier l'utilisateur à l'origine d'une requête, en fonction de l'adresse IP d'origine. Plusieurs méthodes d'identification sont disponibles :

- Une application ou un périphérique d'intégration identifie et authentifie les utilisateurs, puis transmet les informations de cet utilisateur à Websense. Pour plus d'informations, consultez le *Guide d'installation*.
- Un agent d'identification transparente Websense fonctionne en arrière-plan pour communiquer avec un service d'annuaire et identifier les utilisateurs (voir *Identification transparente*).
- Websense demande aux utilisateurs leurs identifiants réseau, en les invitant à se connecter et lorsqu'ils ouvrent un navigateur Web (voir *Authentification manuelle*, page 203).

Identification transparente

Rubriques connexes :

- *Authentification manuelle*, page 203
- *Configuration des méthodes d'identification des utilisateurs*, page 204

En général, **l'identification transparente** décrit la méthode utilisée par Websense pour identifier les utilisateurs de votre service d'annuaire sans leur demander d'informations de connexion. Cela comprend l'intégration dans Websense d'un périphérique ou d'une application fournissant les informations des utilisateurs à utiliser pour le filtrage, ou l'utilisation des agents d'identification transparente de Websense en option.

- Websense *DC Agent*, page 213 est utilisé avec un service d'annuaire de type Windows. L'agent interroge régulièrement les contrôleurs de domaine sur les sessions de connexion des utilisateurs et les ordinateurs client pour vérifier l'état des connexions. Il s'exécute sur un serveur Windows et peut être installé dans n'importe quel domaine du réseau.

- Websense *Logon Agent*, page 216 identifie les utilisateurs lorsqu'ils se connectent à des domaines Windows. L'agent s'exécute sur un serveur Linux ou Windows, mais son application de connexion associée s'exécute uniquement sur des ordinateurs Windows.
- Websense *RADIUS Agent*, page 219 peut être combiné aux services d'annuaire de type Windows ou LDAP. L'agent fonctionne avec un serveur et un client RADIUS pour identifier les utilisateurs qui se connectent à partir d'emplacements distants.
- Websense *eDirectory Agent*, page 224 est utilisé avec Novell eDirectory. L'agent utilise l'authentification Novell eDirectory pour mapper les utilisateurs avec les adresses IP.

Pour plus d'informations sur l'installation de chaque agent, consultez le *Guide d'installation*. L'agent peut être utilisé seul ou dans certaines combinaisons (voir *Configuration de plusieurs agents*, page 230).

Remarques

Si vous utilisez un dispositif NetCache intégré, il doit envoyer les noms d'utilisateur à Websense au format WinNT, LDAP ou RADIUS pour que l'identification transparente fonctionne.

Si vous utilisez un serveur proxy et un agent d'identification transparente, il est préférable d'utiliser l'authentification anonyme dans votre serveur proxy.

Les paramètres généraux d'identification des utilisateurs et les agents d'identification transparente spécifiques sont configurés dans Websense Manager. Cliquez sur l'onglet **Paramètres** dans le panneau de navigation, puis sur **Identification des utilisateurs**.

Reportez-vous à la section *Configuration des méthodes d'identification des utilisateurs*, page 204 pour obtenir des instructions détaillées sur la configuration.

Il arrive parfois que Websense ne puisse pas obtenir les informations des utilisateurs d'un agent d'identification transparente. Cela peut se produire lorsque plusieurs utilisateurs emploient le même ordinateur, si l'utilisateur est un utilisateur invité ou anonyme ou encore pour d'autres raisons. Dans ce cas, vous pouvez inviter l'utilisateur à se connecter par l'intermédiaire du navigateur (voir *Authentification manuelle*, page 203).

Identification transparente des utilisateurs distants

Dans certaines configurations, Websense peut identifier de manière transparente les utilisateurs qui se connectent à votre réseau à partir d'emplacements distants :

- Si vous avez déployé le serveur Websense Remote Filtering et le client Remote Filtering, Websense peut identifier les utilisateurs distants qui se connectent à un domaine mis en cache à l'aide d'un compte de domaine. Pour plus d'informations, consultez *Filtrage des clients distants*, page 157.

- Si vous avez déployé DC Agent, et que les utilisateurs distants se connectent directement à des domaines Windows nommés de votre réseau, DC Agent peut les identifier (voir *DC Agent*, page 213).
- Si vous utilisez un serveur RADIUS pour authentifier les utilisateurs qui se connectent à partir d'emplacements distants, RADIUS Agent peut les identifier de façon transparente de sorte que vous puissiez appliquer des stratégies de filtrage en fonction des utilisateurs ou des groupes (voir *RADIUS Agent*, page 219).

Authentification manuelle

Rubriques connexes :

- *Identification transparente*, page 201
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206
- *Authentification manuelle sécurisée*, page 209
- *Configuration des méthodes d'identification des utilisateurs*, page 204

L'identification transparente n'est pas toujours disponible ou souhaitable dans tous les environnements. Lorsque les organisations n'utilisent pas l'identification transparente, ou lorsque celle-ci n'est pas disponible, vous pouvez tout de même effectuer le filtrage en fonction des stratégies basées sur les utilisateurs et les groupes grâce à l'**authentification manuelle**.

L'authentification manuelle invite les utilisateurs à saisir un nom d'utilisateur et un mot de passe lors de leur première connexion à Internet via un navigateur. Websense confirme ensuite le mot de passe avec le service d'annuaire pris en charge, puis récupère les informations de stratégies liées à cet utilisateur.

Vous pouvez configurer Websense pour activer l'authentification manuelle chaque fois que l'identification transparente n'est pas disponible (voir *Configuration des méthodes d'identification des utilisateurs*, page 204), ou créer une liste d'ordinateurs spécifiques en définissant des paramètres d'authentification personnalisés qui invitent les utilisateurs à se connecter lorsqu'ils ouvrent un navigateur (voir *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206).

Lorsque l'authentification manuelle est activée, l'utilisateur peut recevoir une erreur HTTP et ne pas réussir à accéder à Internet si :

- Il a saisi à trois reprises un mot de passe incorrect. Cela se produit lorsque le nom d'utilisateur ou le mot de passe n'est pas valide.
- Il clique sur **Annuler** pour contourner la demande d'authentification.

Lorsque l'authentification manuelle est activée, les utilisateurs qui ne peuvent pas s'identifier se voient refuser l'accès à Internet.

Configuration des méthodes d'identification des utilisateurs

Rubriques connexes :

- *Identification transparente*, page 201
- *Authentification manuelle*, page 203
- *Travail avec des utilisateurs et des groupes*, page 62

La page **Paramètres > Identification utilisateur** permet de définir le moment et la façon dont Websense tente d'identifier les utilisateurs du réseau pour appliquer les stratégies destinées aux groupes et aux utilisateurs.

- Configurez Policy Server pour qu'il communique avec les agents d'identification transparente.
- Vérifiez et actualisez les paramètres des agents d'identification transparente.
- Définissez une règle globale déterminant la réponse de Websense lorsque les utilisateurs ne peuvent pas être identifiés par un agent d'identification transparente ou par un périphérique d'intégration.
- Identifiez les ordinateurs de votre réseau auxquels les règles globales d'identification des utilisateurs ne s'appliquent pas, et précisez si et comment leurs utilisateurs doivent être authentifiés.

Si vous utilisez des agents d'identification transparente de Websense, ils sont répertoriés sous **Agents d'identification transparente** :

- **Serveur** présente l'adresse IP ou le nom de l'ordinateur qui héberge l'agent d'identification transparente.
- **Port** présente le port utilisé par Websense pour communiquer avec l'agent.
- **Type** indique si l'instance spécifiée est un DC Agent, Logon Agent, RADIUS Agent, ou eDirectory Agent. (Consultez la section *Identification transparente*, page 201 pour la présentation de chaque type d'agent.)

Pour ajouter un agent, sélectionnez le type d'agent dans la liste déroulante **Ajouter agent**. Cliquez sur l'un des liens suivants pour obtenir des instructions sur la configuration :

- *Configuration de DC Agent*, page 214
- *Configuration de Logon Agent*, page 217
- *Configuration de RADIUS Agent*, page 222
- *Configuration d'eDirectory Agent*, page 226

Pour supprimer une instance d'agent, cochez la case accolée aux informations de l'agent dans la liste, puis cliquez sur **Supprimer**.

Sous **Options d'authentification supplémentaires**, définissez la réponse par défaut de Websense lorsque les utilisateurs ne sont pas identifiés de manière transparente (par un agent ou par un périphérique d'intégration) :

- Cliquez sur **Appliquer la stratégie d'ordinateur ou de réseau** pour ignorer les stratégies basées sur les utilisateurs et les groupes au profit des stratégies basées sur les ordinateurs et le réseau ou de la stratégie Par défaut.
- Cliquez sur **Inviter l'utilisateur à fournir des informations de connexion** pour obliger les utilisateurs à fournir leurs identifiants de connexion lorsqu'ils ouvrent un navigateur. Les stratégies destinées aux utilisateurs et aux groupes peuvent ensuite être appliquées (voir *Authentification manuelle*, page 203).
- Définissez le **Contexte** de domaine par défaut que Websense doit utiliser chaque fois qu'un utilisateur est invité à saisir ses identifiants de connexion. Il s'agit du domaine dans lequel les identifiants de connexion des utilisateurs sont valides.

  Si vous utilisez la liste Exceptions pour définir les ordinateurs sur lesquels les utilisateurs sont invités à saisir des informations de connexion, vous devez fournir un contexte de domaine par défaut, même si la règle globale consiste à appliquer une stratégie basée sur les ordinateurs ou le réseau.

Après avoir défini la règle générale qui détermine le moment et la façon dont les utilisateurs sont identifiés par Websense, vous pouvez créer des exceptions à cette règle.

Par exemple, si vous utilisez un agent d'identification transparente ou un produit d'intégration pour identifier les utilisateurs et que vous avez activé l'authentification manuelle pour inviter les utilisateurs à saisir leurs informations d'identification lorsqu'ils ne peuvent pas être identifiés de manière transparente, vous pouvez identifier des ordinateurs spécifiques sur lesquels :

- Les utilisateurs qui ne peuvent pas être identifiés ne sont jamais invités à saisir leurs informations d'identification. En d'autres termes, lorsque l'identification transparente échoue, l'authentification manuelle n'est pas proposée et la stratégie du réseau ou de l'ordinateur, ou la stratégie Par défaut, s'applique.
- Les informations des utilisateurs sont toujours ignorées, même lorsqu'elles sont disponibles, et les utilisateurs sont toujours invités à saisir leurs identifiants.
- Les informations des utilisateurs sont toujours ignorées, même lorsqu'elles sont disponibles, et les utilisateurs ne sont jamais invités à saisir leurs identifiants (la stratégie de l'ordinateur ou du réseau, ou la stratégie Par défaut, est toujours appliquée).

Pour créer une exception, cliquez sur **Exceptions**, puis consultez la section *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206.

Lorsque vos modifications sont terminées dans cette page, cliquez sur **OK** pour les enregistrer. Pour abandonner les modifications, cliquez sur **Annuler**.

Définition de règles d'authentification pour des ordinateurs spécifiques

Rubriques connexes :

- *Configuration des méthodes d'identification des utilisateurs*, page 204
- *Authentification manuelle*, page 203
- *Authentification manuelle sécurisée*, page 209

L'authentification sélective vous permet de déterminer si les utilisateurs qui demandent un accès à Internet à partir d'un ordinateur client spécifique (identifié par son adresse IP) sont invités à saisir leurs identifiants de connexion via le navigateur. Cette option peut être utilisée pour :

- Établir des règles d'authentification différentes pour un ordinateur situé dans une borne publique que celles des employés de l'organisation fournissant la borne de connexion.
- Garantir que les utilisateurs d'un ordinateur de salle d'examen situé dans un bureau médical sont toujours identifiés avant d'accéder à Internet.

Les ordinateurs auxquels s'appliquent des paramètres particuliers d'identification sont répertoriés dans la page **Paramètres > Identification utilisateur**. Cliquez sur **Exceptions** pour définir des paramètres d'identification spécifiques pour certains ordinateurs de votre réseau ou pour voir si des paramètres particuliers ont été définis pour un ordinateur spécifique.

Pour ajouter un ordinateur à la liste, cliquez sur **Ajouter**, puis passez à la section *Définition d'exceptions dans les paramètres d'identification des utilisateurs*, page 206 pour d'autres instructions.

Lorsque vous avez terminé d'ajouter des ordinateurs ou des plages réseau à la liste, cliquez sur **OK**. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Définition d'exceptions dans les paramètres d'identification des utilisateurs

Rubriques connexes :

- *Identification transparente*, page 201
- *Authentification manuelle*, page 203
- *Configuration des méthodes d'identification des utilisateurs*, page 204

La page **Paramètres > Identification utilisateur > Ajouter des adresses IP** permet d'identifier les ordinateurs auxquels des règles d'identification spécifiques doivent s'appliquer.

1. Entrez une **Adresse IP** ou une **Plage d'adresses IP** permettant d'identifier les ordinateurs auxquels une méthode d'authentification spécifique doit s'appliquer, puis cliquez sur la flèche droite pour les ajouter dans la liste **Sélectionné**.

   Si les mêmes règles doivent s'appliquer à plusieurs ordinateurs, ajoutez-les tous dans la liste.
2. Sélectionnez une entrée dans la liste déroulante **Identification utilisateur** pour indiquer si Websense doit tenter d'identifier les utilisateurs de ces ordinateurs de manière transparente.
   - Sélectionnez **Essayer d'identifier l'utilisateur de façon transparente** pour récupérer les informations des utilisateurs auprès d'un agent d'identification transparente ou d'un périphérique d'intégration.
   - Sélectionnez **Ignorer les informations de l'utilisateur** pour ne pas utiliser de méthode transparente d'identification des utilisateurs.
3. Indiquez si les utilisateurs doivent être invités à saisir leurs identifiants de connexion via le navigateur. Ce paramètre s'applique lorsque les informations des utilisateurs ne sont pas disponibles, soit parce qu'une autre identification a échoué, soit parce que les informations des utilisateurs ont été ignorées.
   - Sélectionnez **Inviter l'utilisateur à fournir des informations de connexion** pour obliger les utilisateurs à fournir leurs identifiants de connexion.

     Si l'option **Essayer d'identifier l'utilisateur de façon transparente** est également sélectionnée, les utilisateurs reçoivent une invite du navigateur uniquement s'ils n'ont pas été identifiés de manière transparente.
   - Sélectionnez **Appliquer la stratégie d'ordinateur ou de réseau** pour que les utilisateurs ne soient jamais invités à fournir leurs identifiants de connexion.

     Si l'option **Essayer d'identifier l'utilisateur de façon transparente** est également sélectionnée, les utilisateurs dont les identifiants de connexion peuvent être vérifiés de façon transparente sont filtrés par la stratégie d'utilisateurs appropriée.
4. Cliquez sur **OK** pour revenir à la page Identification utilisateur.
5. Lorsque la mise à jour de la liste Exceptions est terminée, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Vérification des exceptions aux paramètres d'identification des utilisateurs

Rubriques connexes :

- *Identification transparente*, page 201
- *Authentification manuelle*, page 203
- *Configuration des méthodes d'identification des utilisateurs*, page 204

La page **Paramètres > Identification utilisateur > Modifier des adresses IP** permet de modifier les entrées de la liste Exceptions. Les modifications apportées dans cette page affectent tous les ordinateurs (identifiés par une adresse ou par une plage d'adresses IP) apparaissant dans la liste Sélectionné.

1. Sélectionnez une entrée dans la liste déroulante **Identification utilisateur** pour indiquer si Websense doit tenter d'identifier les utilisateurs de ces ordinateurs de manière transparente.
   - Sélectionnez **Essayer d'identifier l'utilisateur de façon transparente** pour récupérer les informations des utilisateurs auprès d'un agent d'identification transparente ou d'un périphérique d'intégration.
   - Sélectionnez **Ignorer les informations de l'utilisateur** pour ne pas utiliser de méthode transparente d'identification des utilisateurs.
2. Indiquez si les utilisateurs doivent être invités à saisir leurs identifiants de connexion via le navigateur. Ce paramètre s'applique lorsque les informations des utilisateurs ne sont pas disponibles, soit parce que l'identification transparente a échoué, soit parce qu'elle a été ignorée.
   - Sélectionnez **Inviter l'utilisateur à fournir des informations de connexion** pour obliger les utilisateurs à fournir leurs identifiants de connexion.

     Si l'option **Essayer d'identifier l'utilisateur de façon transparente** est également sélectionnée, les utilisateurs reçoivent une invite du navigateur uniquement s'ils n'ont pas été identifiés de manière transparente.
   - Sélectionnez **Appliquer la stratégie d'ordinateur ou de réseau** pour que les utilisateurs ne soient jamais invités à fournir leurs identifiants de connexion.

     Si l'option **Essayer d'identifier l'utilisateur de façon transparente** est également sélectionnée, les utilisateurs dont les identifiants de connexion peuvent être vérifiés de façon transparente sont filtrés par la stratégie d'utilisateurs appropriée.
3. Cliquez sur **OK** pour revenir à la page Identification utilisateur.
4. Lorsque la mise à jour de la liste Exceptions est terminée, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Authentification manuelle sécurisée

Rubriques connexes :

- *Configuration des méthodes d'identification des utilisateurs*, page 204
- *Authentification manuelle*, page 203
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206
- *Activation de l'authentification manuelle sécurisée*, page 211

L'authentification manuelle sécurisée de Websense utilise le cryptage SSL (Secure Sockets Layer) pour protéger les données d'authentification qui circulent entre les ordinateurs client et Websense. Un serveur SSL intégré à Filtering Service assure le cryptage des noms d'utilisateur et des mots de passe transmis entre les ordinateurs client et le service Filtering Service. Par défaut, l'authentification manuelle sécurisée est désactivée.

Remarque

L'authentification manuelle sécurisée ne peut pas être utilisée avec Remote Filtering. Le serveur Remote Filtering ne peut pas envoyer de pages de blocage aux clients s'il est associé à une instance de Filtering Service pour laquelle l'authentification manuelle sécurisée est activée.

Pour activer cette fonctionnalité, procédez comme suit :

1. Générez des certificats et des clés SSL, et stockez-les dans un emplacement accessible par Websense et Filtering Service (voir *Création de clés et de certificats*, page 210).
2. Activez l'authentification manuelle sécurisée (voir *Activation de l'authentification manuelle sécurisée*, page 211) et la communication sécurisée avec le service d'annuaire.
3. Importez les certificats dans le navigateur (voir *Acceptation du certificat dans le navigateur client*, page 212).

Création de clés et de certificats

Rubriques connexes :

- *Authentification manuelle*, page 203
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206
- *Authentification manuelle sécurisée*, page 209
- *Activation de l'authentification manuelle sécurisée*, page 211
- *Acceptation du certificat dans le navigateur client*, page 212

Un certificat se compose d'une clé publique, utilisée pour crypter les données, et d'une clé privée, utilisée pour les décrypter. Les certificats sont publiés par une Autorité de certification (CA). Vous pouvez générer un certificat à partir d'un serveur de certificats interne ou obtenir un certificat client auprès d'une autorité de certification tierce, telle que VeriSign.

L'autorité de certification qui publie le certificat client doit être approuvée par Websense. En général, cela est déterminé par un paramètre du navigateur.

- Vous trouverez les réponses aux questions courantes relatives aux clés privées, aux requêtes CSR et aux certificats à l'adresse httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts.
- Pour plus d'informations sur la création de votre propre clé privée, requête CSR et certificat, consultez le site www.akadia.com/services/ssh_test_certificate.html.

De nombreux outils vous permettent de générer un certificat auto-signé, dont OpenSSL Toolkit (disponible sur le site www.openssl.org).

Quelle que soit la méthode choisie pour générer le certificat, utilisez la procédure suivante.

1. Générez une clé privée (**server.key**).
2. Générez une requête de signature de certificat (CSR, Certificate Signing Request) avec la clé privée.

   Important

   Lorsque vous êtes invité(e) à saisir le NomCommun, entrez l'adresse IP de l'ordinateur Filtering Server. Si vous ignorez cette étape, les navigateurs client afficheront une erreur de certificat de sécurité.

3. Servez-vous de la requête CSR pour créer un certificat auto-signé (**server.crt**).
4. Enregistrez les fichiers **server.crt** et **server.key** dans un emplacement accessible à Websense et dans lequel Filtering Service peut les lire.

Activation de l'authentification manuelle sécurisée

Rubriques connexes :

- *Authentification manuelle*, page 203
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206
- *Authentification manuelle sécurisée*, page 209
- *Création de clés et de certificats*, page 210
- *Acceptation du certificat dans le navigateur client*, page 212

1. Arrêtez Websense Filtering Service (voir *Arrêt et démarrage des services Websense*, page 286).
2. Sur l'ordinateur Filtering Service, localisez le répertoire d'installation de Websense (par défaut, **C:\Program Files\Websense\bin** ou **/opt/Websense/bin/**).
3. Localisez le fichier **eimserver.ini** et sauvegardez-le dans un autre répertoire.
4. Ouvrez le fichier INI original dans un éditeur de texte.
5. Localisez la section **[WebsenseServer]** et ajoutez la ligne suivante :

   ```
   SSLManualAuth=on
   ```

6. Au-dessous de la ligne précédente, ajoutez :

   ```
   SSLCertFileLoc=[chemin]
   ```

   Remplacez **[chemin]** par le chemin d'accès complet du certificat SSL, en incluant le nom du fichier (par exemple, C:\secmanauth\server.crt).
7. Ajoutez également :

   ```
   SSLKeyFileLoc=[chemin]
   ```

   Remplacez **[chemin]** par le chemin d'accès complet de la clé SSL, en incluant le nom du fichier (par exemple, C:\secmanauth\server.key).
8. Enregistrez et fermez le fichier **eimserver.ini**.
9. Démarrez Websense Filtering Service.

Après le démarrage, Filtering Service écoute les requêtes sur le port HTTP sécurisé par défaut (**15872**).

La procédure précédente assure une communication sécurisée entre l'ordinateur client et Websense. Pour sécuriser également la communication entre Websense et le service d'annuaire, assurez-vous que l'option **Utiliser SSL** est également sélectionnée à la page **Paramètres > Services d'annuaire**. Pour plus d'informations, consultez la section *Paramètres de l'annuaire avancés*, page 65.

Acceptation du certificat dans le navigateur client

Rubriques connexes :

- *Authentification manuelle*, page 203
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 206
- *Authentification manuelle sécurisée*, page 209
- *Création de clés et de certificats*, page 210
- *Activation de l'authentification manuelle sécurisée*, page 211

Lors de votre première tentative d'accès à un site Web, le navigateur présente un avertissement sur le certificat de sécurité. Pour que ce message n'apparaisse plus ensuite, installez le certificat dans le magasin de certificats.

Microsoft Internet Explorer (Version 7)

1. Ouvrez le navigateur et accédez à un site Web.

   Un message d'avertissement s'affiche, signalant un problème avec le certificat de sécurité du site.
2. Cliquez sur **Continuer avec ce site Web (non conseillé)**.

   Si vous recevez une invite d'authentification, cliquez sur **Annuler**.
3. Cliquez sur la zone **Erreur de certificat** située à droite de la barre d'adresse (en haut de la fenêtre du navigateur), puis sur **Afficher les certificats**.
4. Dans l'onglet Général de la boîte de dialogue Certificat, cliquez sur **Installer le certificat**.
5. Sélectionnez **Sélectionner automatiquement le magasin de certificats selon le type de certificat** et cliquez sur **Suivant**.
6. Cliquez sur **Terminer**.
7. Lorsque vous êtes invité(e) à installer le certificat, cliquez sur **Oui**.

Les utilisateurs ne recevront plus d'avertissements de sécurité de certificat liés à Filtering Service sur cet ordinateur.

Mozilla Firefox (Version 2.x)

1. Ouvrez le navigateur et accédez à un site Web.

   Un message d'avertissement s'affiche.
2. Cliquez sur **Accepter le certificat définitivement**.
3. Entrez vos identifiants de connexion, si vous y êtes invité(e).
4. Sélectionnez **Outils > Options**, puis cliquez sur **Avancé**.
5. Sélectionnez l'onglet **Chiffrement** et cliquez sur **Afficher les certificats**.
6. Sélectionnez l'onglet **Sites Web** et vérifiez que le certificat apparaît bien dans la liste.

Les utilisateurs ne recevront plus d'avertissements de sécurité de certificat liés à Filtering Service sur cet ordinateur.

Mozilla Firefox (Version 3.x)

1. Ouvrez le navigateur et accédez à un site Web.

   Un message d'avertissement s'affiche.
2. Cliquez sur **Ou vous pouvez ajouter une exception**.
3. Cliquez sur **Ajouter une exception**.
4. Assurez-vous que l'option **Conserver définitivement cette exception** est bien activée, puis cliquez sur **Confirmer l'exception de sécurité**.

Les utilisateurs ne recevront plus d'avertissements de sécurité de certificat liés à Filtering Service sur cet ordinateur.

DC Agent

Rubriques connexes :

- *Identification transparente*, page 201
- *Configuration de DC Agent*, page 214
- *Configuration de paramètres différents pour une instance d'agent*, page 232

Websense DC Agent s'exécute sous Windows et détecte les utilisateurs du réseau Windows qui exécutent NetBIOS, WINS ou des services réseau DNS.

DC Agent et User Service rassemblent les données des utilisateurs du réseau et les envoient à Websense Filtering Service. Plusieurs variables déterminent la vitesse de transmission des données, dont la taille de votre réseau et le volume du trafic.

Pour activer l'identification transparente avec DC Agent :

1. Installez DC Agent. Pour plus d'informations, consultez la section *Installation séparée des composants Websense* du *Guide d'installation*.

   Remarque

   Exécutez DC Agent avec des droits d'administrateur de domaine. Le compte d'administrateur de domaine doit également être membre du groupe Administrateurs sur l'ordinateur DC Agent.

   Cette condition est obligatoire pour que DC Agent récupère les informations de connexion des utilisateurs à partir du contrôleur de domaine. Si vous ne pouvez pas installer DC Agent avec ces droits, configurez des droits d'administrateur pour ces services après l'installation. Pour plus d'informations, consultez *Websense n'applique pas les stratégies de groupe ou d'utilisateur*, page 367.

2. Configurez DC Agent pour qu'il communique avec les autres composants Websense et les contrôleurs de domaine de votre réseau (voir *Configuration de DC Agent*).
3. Utilisez Websense Manager pour ajouter des utilisateurs et des groupes à filtrer (voir *Ajout d'un client*, page 68).

Websense peut inviter les utilisateurs à s'identifier lorsque DC Agent ne peut pas les identifier de façon transparente. Pour plus d'informations, consultez *Authentification manuelle*, page 203.

Configuration de DC Agent

Rubriques connexes :

- *Identification transparente*
- *Authentification manuelle*
- *Configuration des méthodes d'identification des utilisateurs*
- *DC Agent*
- *Configuration de plusieurs agents*

La page **Paramètres > Identification utilisateur > DC Agent** permet de configurer une nouvelle instance de DC Agent et les paramètres globaux s'appliquant à toutes les instances de DC Agent.

Pour ajouter une nouvelle instance de DC Agent, fournissez d'abord les informations de base sur l'emplacement d'installation de l'agent et sur le mode de communication de Filtering Service avec cet agent. Ces paramètres peuvent être distincts pour chaque instance de l'agent.

1. Sous Configuration de base de l'agent, entrez l'adresse IP ou le nom du **Serveur** sur lequel l'agent est installé.

   Remarque

   Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.

   Les noms d'ordinateur contenant des caractères ASCII étendus peuvent ne pas être résolus de façon appropriée. Si vous utilisez une version non anglaise de Websense, entrez une adresse IP plutôt qu'un nom d'ordinateur.

2. Entrez le numéro de **Port** que DC Agent doit utiliser pour communiquer avec les autres composants de Websense. Le port par défaut est 30600.
3. Pour établir une connexion authentifiée entre Filtering Service et DC Agent, sélectionnez **Activer l'authentification**, puis entrez un **Mot de passe** de connexion.

Personnalisez ensuite la communication globale de DC Agent et les paramètres du dépannage, de l'interrogation du contrôleur de domaine et de l'interrogation des ordinateurs. Par défaut, les modifications apportées ici affectent toutes les instances de DC Agent. Les paramètres signalés par un astérisque (*) peuvent toutefois être remplacés dans le fichier de configuration d'un agent afin de personnaliser le comportement de cette instance (voir *Configuration de paramètres différents pour une instance d'agent*, page 232).

1. Sous Communication de DC Agent, entrez le **Port de communication** à utiliser pour les communications entre DC Agent et les autres composants de Websense. Le port par défaut est 30600.

   Sauf autorisation expresse du support technique de Websense, ne modifiez pas le paramètre **Port de diagnostic**. Le port par défaut est 30601.
2. Sous Interrogation du contrôleur de domaine, sélectionnez **Activer l'interrogation du contrôleur de domaine** pour autoriser DC Agent à interroger les contrôleurs de domaine sur les sessions de connexion des utilisateurs.

   Dans le fichier de configuration de l'agent, vous pouvez définir quels contrôleurs de domaine seront interrogés par chaque instance de DC Agent. Pour plus d'informations, consultez la section *Configuration de plusieurs agents*, page 230.
3. Utilisez le champ **Intervalle de requête** pour indiquer la fréquence (en secondes) selon laquelle DC Agent doit interroger les contrôleurs de domaine.

   Diminuer cet intervalle peut accroître la précision des captures de session de connexion, mais augmente également l'ensemble du trafic réseau. Augmenter cet intervalle allège le trafic réseau mais peut également retarder ou empêcher la capture de certaines sessions de connexion. L'intervalle par défaut est de 10 secondes.
4. Utilisez le champ **Délai d'attente de l'entrée utilisateur** pour définir la fréquence (en heures) selon laquelle DC Agent actualise les entrées des utilisateurs dans son mappage. Le délai par défaut est de 24 heures.

5. Sous Interrogation des ordinateurs, sélectionnez l'option **Activer l'interrogation des ordinateurs** pour que DC Agent interroge les ordinateurs sur les sessions de connexion des utilisateurs. Cela peut inclure des ordinateurs extérieurs aux domaines déjà interrogés par DC Agent.

   DC Agent utilise WMI (Windows Management Instruction) pour l'interrogation des ordinateurs. Si vous activez l'interrogation des ordinateurs, configurez le Pare-feu de Windows sur les ordinateurs client pour autoriser une communication sur le port **135**.

6. Entrez un **Intervalle de vérification des correspondances d'utilisateur** pour définir la fréquence selon laquelle DC Agent contacte les ordinateurs client pour vérifier quels utilisateurs sont connectés. L'intervalle par défaut est de 15 minutes.

   DC Agent compare les résultats de la requête et les paires nom d'utilisateur/adresse IP dans le mappage des utilisateurs qu'il envoie au service Filtering Service. Réduire cet intervalle peut accroître la précision des correspondances, mais augmente le trafic du réseau. Augmenter cet intervalle allège le trafic réseau mais peut également réduire la précision.

7. Entrez un **Délai d'attente de l'entrée utilisateur** pour définir la fréquence selon laquelle DC Agent actualise les entrées obtenues via l'interrogation des ordinateurs dans son mappage des utilisateurs. Le délai par défaut est de 1 heure.

   DC Agent retire toutes les entrées nom d'utilisateur/adresse IP postérieures à ce délai, et qu'il ne peut pas vérifier par rapport aux utilisateurs actuellement connectés. Augmenter cet intervalle peut réduire la précision du mappage des utilisateurs car les anciens noms d'utilisateur peuvent y demeurer pendant de longues périodes.

   > **Remarque**
   > Ne définissez pas un délai d'attente de l'entrée utilisateur plus court que l'intervalle de vérification des correspondances des utilisateurs car des noms d'utilisateur pourraient être retirés du mappage avant de pouvoir être vérifiés.

8. Cliquez sur **OK** pour enregistrer et implémenter immédiatement vos modifications.

Logon Agent

Rubriques connexes :

- *Identification transparente*, page 201
- *Configuration de Logon Agent*, page 217
- *Configuration de paramètres différents pour une instance d'agent*, page 232

Websense Logon Agent identifie les utilisateurs en temps réel, lorsqu'ils se connectent aux domaines. La possibilité de manquer une connexion d'utilisateur à cause d'un problème de délai de requête est ainsi éliminée.

Logon Agent (également appelé Serveur d'authentification) peut résider sur un ordinateur Windows ou Linux. Cet agent fonctionne avec Websense Logon Application (LogonApp.exe) sur les ordinateurs client Windows pour identifier les utilisateurs lorsqu'ils se connectent aux domaines Windows.

Dans la plupart des cas, l'utilisation de DC Agent ou Logon Agent suffit, mais vous pouvez les utiliser ensemble. Dans ce cas, Logon Agent est prioritaire sur DC Agent. DC Agent communique uniquement les sessions de connexion à Filtering Service si Logon Agent en a manqué une, ce qui est peu probable.

Installez Logon Agent, puis déployez Logon Application sur les ordinateurs client depuis un emplacement centralisé. Pour plus d'informations, consultez le *Guide d'installation*.

Après son installation, configurez l'agent pour qu'il communique avec les ordinateurs client et avec Websense Filtering Service (voir *Configuration de Logon Agent*).

Remarque

Si vous utilisez Windows Active Directory (mode natif) et que User Service est installé sur un ordinateur Linux, consultez la section *User Service sous Linux*, page 374 pour des instructions supplémentaires sur la configuration.

Configuration de Logon Agent

Rubriques connexes :

- *Identification transparente*, page 201
- *Authentification manuelle*, page 203
- *Configuration des méthodes d'identification des utilisateurs*, page 204
- *Logon Agent*, page 216
- *Configuration de plusieurs agents*, page 230

La page **Paramètres > Identification utilisateur > Logon Agent** permet de configurer une nouvelle instance de Logon Agent et les paramètres globaux s'appliquant à toutes les instances de Logon Agent.

Pour ajouter une nouvelle instance de Logon Agent :

1. Sous Configuration de base de l'agent, entrez l'adresse IP ou le nom du **Serveur** sur lequel l'agent est installé.

   > **Remarque**
   > Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.
   >
   > Les noms d'ordinateur contenant des caractères ASCII étendus peuvent ne pas être résolus de façon appropriée. Si vous utilisez une version non anglaise de Websense, entrez une adresse IP plutôt qu'un nom d'ordinateur.

2. Entrez le numéro de **Port** que Logon Agent doit utiliser pour communiquer avec les autres composants de Websense. Le port par défaut est 30602.
3. Pour établir une connexion authentifiée entre Filtering Service et Logon Agent, sélectionnez **Activer l'authentification** et entrez un **Mot de passe** de connexion.
4. Cliquez sur **OK** pour enregistrer vos modifications ou passez à la prochaine section de l'écran pour entrer d'autres informations de configuration.

Personnalisez ensuite les paramètres globaux de communication de Logon Agent. Par défaut, les modifications apportées ici affectent toutes les instances de Logon Agent.

1. Sous Communication de Logon Agent, entrez le **Port de communication** à utiliser pour les communications entre Logon Agent et les autres composants de Websense. Le port par défaut est 30602.
2. Sauf autorisation expresse du support technique de Websense, ne modifiez pas le paramètre **Port de diagnostic**. Le port par défaut est 30603.
3. Sous Communication de Logon Agent, définissez le **Port de connexion** que l'application de connexion utilise pour communiquer avec Logon Agent. Le port par défaut est 15880.
4. Entrez le **Nombre maximum de connexions** que chaque instance de Logon Agent autorise. La valeur par défaut est 200.

   Si votre réseau est très vaste, vous pouvez augmenter ce nombre. L'augmentation de cette valeur accroît le trafic réseau.
5. Cliquez sur **OK** pour enregistrer vos modifications ou passez à la prochaine section de l'écran pour entrer d'autres informations de configuration.

Pour configurer les paramètres par défaut qui déterminent comment la validité de l'entrée de l'utilisateur est détectée, vous devez commencer par déterminer si Logon Agent et l'application de connexion cliente fonctionneront en **mode persistant** ou en **mode non persistant** (par défaut).

Le mode non persistant est activé en incluant le paramètre /NOPERSIST au démarrage de **LogonApp.exe**. (Vous trouverez d'autres informations dans le fichier **LogonApp_ReadMe.txt**, inclus avec l'installation de Logon Agent.)

- En mode persistant, l'application de connexion contacte régulièrement Logon Agent pour communiquer les informations de connexion des utilisateurs.

Si vous utilisez le mode persistant, définissez un **Intervalle de requête** pour déterminer la fréquence de communication des informations de connexion par l'application de connexion.

> **Remarque**
> Si vous changez cette valeur, la modification ne prend pas effet avant la fin de l'intervalle précédemment défini. Par exemple, si vous remplacez un intervalle de 15 minutes par 5 minutes, l'intervalle de 15 minutes en cours doit s'écouler avant que l'interrogation ne commence toutes les 5 minutes.

- En mode non persistant, l'application de connexion n'envoie les informations de connexion des utilisateurs à Logon Agent qu'une fois par connexion.

  Si vous utilisez le mode non persistant, entrez un délai **Expiration des entrées utilisateur**. Lorsque ce délai est écoulé, l'entrée de l'utilisateur est retirée du mappage des utilisateurs.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour enregistrer vos paramètres.

RADIUS Agent

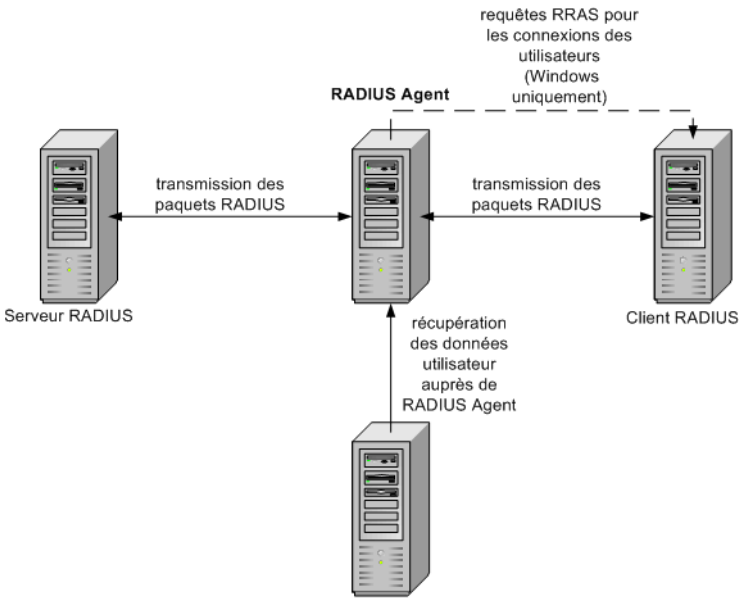
Rubriques connexes :

- *Identification transparente*, page 201
- *Traitement du trafic RADIUS*, page 220
- *Configuration de l'environnement RADIUS*, page 221
- *Configuration de RADIUS Agent*, page 222
- *Configuration du client RADIUS*, page 223
- *Configuration du serveur RADIUS*, page 224
- *Configuration de paramètres différents pour une instance d'agent*, page 232

Websense RADIUS Agent vous permet d'appliquer des stratégies d'utilisateurs et de groupes à l'aide de l'authentification fournie par un serveur RADIUS. RADIUS Agent autorise d'identification transparente des utilisateurs qui accèdent à votre réseau par une connexion distante, un VPN (Virtual Private Network), une ligne ADSL ou une autre connexion à distance (selon votre configuration).

RADIUS Agent fonctionne avec le serveur RADIUS et le client RADIUS de votre réseau pour traiter et surveiller le trafic du protocole RADIUS (Remote Access Dial-In User Service). Vous pouvez ainsi affecter des stratégies de filtrage particulières aux

utilisateurs ou aux groupes qui accèdent à votre réseau à distance, ainsi qu'aux utilisateurs locaux.



Lorsque vous installez RADIUS Agent, l'agent s'intègre aux composants de Websense existants. Toutefois, RADIUS Agent, votre serveur RADIUS et votre client RADIUS doivent être configurés de façon appropriée (voir *Configuration de RADIUS Agent*, page 222).

Traitement du trafic RADIUS

Websense RADIUS Agent joue le rôle d'un proxy qui transmet les messages RADIUS entre un client RADIUS et un serveur RADIUS (ou plusieurs clients et serveurs).

RADIUS Agent n'authentifie pas directement les utilisateurs mais identifie les utilisateurs distants et les associe à des adresses IP pour qu'un serveur RADIUS puisse les authentifier. Dans l'idéal, le serveur RADIUS transmet les demandes d'authentification à un service d'annuaire de type LDAP.

RADIUS Agent stocke les paires nom/adresse IP dans un mappage des utilisateurs. Si votre client RADIUS prend en charge les demandes de compte (ou le suivi des connexions des utilisateurs), et que la demande de compte est activée, RADIUS Agent obtient davantage d'informations sur les sessions de connexion des utilisateurs que dans les messages RADIUS qu'il reçoit.

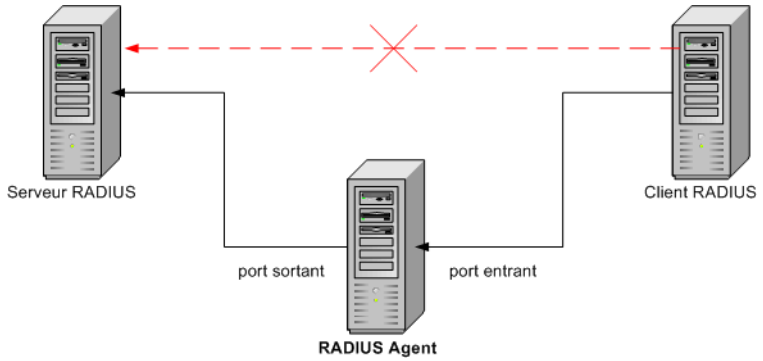
Lorsqu'il est correctement configuré, Websense RADIUS Agent capture et traite tous les paquets de protocoles RADIUS des types suivants :

- **Requêtes d'accès** : envoyées par un client RADIUS pour demander l'autorisation de tenter de se connecter au réseau.
- **Acceptations d'accès** : envoyées par un serveur RADIUS en réponse à un message Requête d'accès ; indique au client RADIUS que la tentative de connexion est autorisée et authentifiée.

- **Rejets d'accès** : envoyés par un serveur RADIUS en réponse à un message Requête d'accès ; indique au client RADIUS que la tentative de connexion est rejetée.
- **Requête d'arrêt** : envoyée par un client RADIUS pour dire au serveur RADIUS d'arrêter le suivi de l'activité des utilisateurs.

Configuration de l'environnement RADIUS

Websense RADIUS Agent joue le rôle de proxy entre un client et un serveur RADIUS. Le diagramme suivant illustre de façon simplifiée les différences entre l'utilisation de RADIUS Agent et une configuration RADIUS standard.



RADIUS Agent et le serveur RADIUS doivent être installés sur des ordinateurs distincts. L'agent et le serveur ne peuvent pas avoir la même adresse IP et doivent utiliser des ports différents.

Après l'installation de RADIUS Agent, configurez RADIUS Agent dans Websense Manager (voir *Configuration de RADIUS Agent*, page 222). Vous devez également :

- Configurer le client RADIUS (en général un serveur d'accès au réseau [NAS]) pour qu'il communique avec RADIUS Agent et non directement avec votre serveur RADIUS.
- Configurer le serveur RADIUS pour qu'il utilise RADIUS Agent comme proxy (consultez la documentation du serveur RADIUS). Si vous utilisez plusieurs serveurs RADIUS, configurez chacun d'eux séparément.

> **Remarque**
> Si vous utilisez Lucent RADIUS Server et RRAS, configurez le serveur RADIUS pour qu'il utilise le protocole PAP (Password Authentication Protocol) et le serveur RRAS pour qu'il n'accepte que les requêtes PAP. Pour plus d'informations, consultez la documentation relative aux produits.

Configuration de RADIUS Agent

Rubriques connexes :

- *Identification transparente*, page 201
- *Authentification manuelle*, page 203
- *Configuration des méthodes d'identification des utilisateurs*, page 204
- *RADIUS Agent*, page 219
- *Configuration de plusieurs agents*, page 230

La page **Paramètres > Identification utilisateur > RADIUS Agent** permet de configurer une nouvelle instance de RADIUS Agent et les paramètres globaux s'appliquant à toutes les instances de RADIUS Agent.

Pour ajouter une nouvelle instance de RADIUS Agent :

1. Sous Configuration de base de l'agent, entrez l'adresse IP ou le nom du **Serveur** sur lequel l'agent est installé.

   Remarque

   Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.

   Les noms d'ordinateur contenant des caractères ASCII étendus peuvent ne pas être résolus de façon appropriée. Si vous utilisez une version non anglaise de Websense, entrez une adresse IP plutôt qu'un nom d'ordinateur.

2. Entrez le numéro de **Port** que RADIUS Agent doit utiliser pour communiquer avec les autres composants de Websense. La valeur par défaut est 30800.
3. Pour établir une connexion authentifiée entre Filtering Service et RADIUS Agent, sélectionnez **Activer l'authentification** et entrez un **Mot de passe** de connexion.
4. Cliquez sur **OK** pour enregistrer vos modifications ou passez à la prochaine section de l'écran pour entrer d'autres informations de configuration.

Personnalisez ensuite les paramètres globaux de RADIUS Agent. Par défaut, les modifications apportées ici affectent toutes les instances de RADIUS Agent. Les paramètres signalés par un astérisque (*) peuvent toutefois être remplacés dans le fichier de configuration d'un agent afin de personnaliser le comportement de cette instance (voir *Configuration de paramètres différents pour une instance d'agent*, page 232).

1. Entrez le numéro de **Port de communication** que RADIUS Agent doit utiliser pour communiquer avec les autres composants de Websense. La valeur par défaut est 30800.
2. Sauf autorisation expresse du support technique de Websense, ne modifiez pas le paramètre **Port de diagnostic**. La valeur par défaut est 30801.

3. Sous Serveur RADIUS, entrez **IP ou nom du serveur RADIUS**. RADIUS Agent transmet les demandes d'authentification au serveur RADIUS et doit donc connaître l'identité de ce dernier.
4. Si Microsoft RRAS est utilisé, entrez l'adresse IP de la **Machine RRAS**. Websense interroge cet ordinateur sur les sessions de connexion des utilisateurs.
5. Entrez le **Délai d'attente de l'entrée utilisateur** pour définir la fréquence selon laquelle RADIUS Agent actualise son mappage des utilisateurs. L'intervalle idéal est généralement celui proposé par défaut (24 heures).
6. Utilisez les paramètres **Ports d'authentification** et **Ports de gestion des comptes** pour définir les ports utilisés par RADIUS Agent pour envoyer et recevoir les requêtes d'authentification et de demande de compte. Pour chaque type de communication, vous pouvez spécifier le port utilisé pour la communication entre :
   - RADIUS Agent et le serveur RADIUS
   - RADIUS Agent et le client RADIUS
7. Lorsque vous avez terminé, cliquez sur **OK** pour enregistrer immédiatement vos paramètres.

Configuration du client RADIUS

Votre client RADIUS doit être configuré pour transmettre les requêtes d'authentification et de demande de compte au serveur RADIUS via RADIUS Agent.

Modifiez la configuration de votre client RADIUS de sorte que :

- Le client RADIUS envoie les demandes d'authentification à l'ordinateur et au port sur lequel RADIUS Agent écoute les demandes d'authentification. Il s'agit du **Port d'authentification** spécifié lors de la configuration de RADIUS Agent.
- Le client RADIUS envoie les requêtes de demande de compte à l'ordinateur et au port sur lequel RADIUS Agent écoute les requêtes de demande de compte. Il s'agit du **Ports de gestion des comptes** spécifié lors de la configuration de RADIUS Agent.

La procédure exacte de configuration d'un client RADIUS dépend du type de client. Pour plus d'informations, consultez la documentation de votre client RADIUS.

Remarque

Le client RADIUS doit inclure les attributs **Nom d'utilisateur** et **Adresses IP de trames** dans les messages d'authentification et de demande de compte qu'il envoie. RADIUS Agent utilise les valeurs de ces attributs pour interpréter et stocker les paires nom/adresse IP. Si votre client RADIUS ne génère pas ces informations par défaut, configurez-le pour qu'il le fasse (consultez la documentation du client RADIUS).

Configuration du serveur RADIUS

Pour configurer correctement la communication entre Websense RADIUS Agent et votre serveur RADIUS :

- Ajoutez l'adresse IP de l'ordinateur RADIUS Agent dans la liste des clients de votre serveur RADIUS. Pour plus d'informations, consultez la documentation de votre serveur RADIUS.
- Définissez des secrets partagés entre le serveur RADIUS et tous les clients RADIUS qui utilisent l'agent pour communiquer avec le serveur RADIUS. Les secrets partagés sont généralement spécifiés en tant qu'options de sécurité de l'authentification.

  La configuration d'un secret partagé pour les clients RADIUS et le serveur RADIUS sécurise la transmission des messages RADIUS. En général, le secret partagé est une chaîne de texte commune. Pour plus d'informations, consultez la documentation de votre serveur RADIUS.

> **Remarque**
> Le serveur RADIUS doit inclure les attributs **Nom d'utilisateur** et **Adresses IP de trames** dans les messages d'authentification et de demande de compte. RADIUS Agent utilise les valeurs de ces attributs pour interpréter et stocker les paires nom/adresse IP. Si votre serveur RADIUS ne génère pas ces informations par défaut, configurez-le pour qu'il le fasse (consultez la documentation du serveur RADIUS).

eDirectory Agent

Rubriques connexes :

- *Identification transparente*, page 201
- *Configuration d'eDirectory Agent*, page 226
- *Configuration de paramètres différents pour une instance d'agent*, page 232

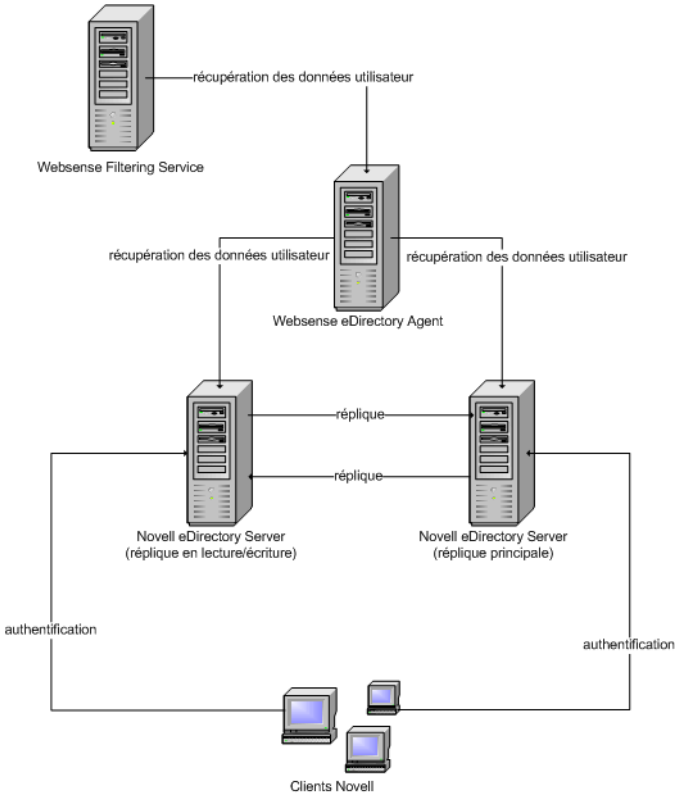
Websense eDirectory Agent fonctionne avec Novell eDirectory pour identifier les utilisateurs de manière transparente de sorte que Websense puisse les filtrer en fonction des stratégies affectées aux utilisateurs, aux groupes, aux domaines ou aux unités d'organisation.

eDirectory Agent collecte les informations de session de connexion des utilisateurs auprès de Novell eDirectory, qui authentifie les utilisateurs se connectant au réseau. L'agent associe ensuite chaque utilisateur authentifié à une adresse IP et enregistre les

paires nom d'utilisateur/adresse IP dans un mappage local des utilisateurs. eDirectory Agent transmet ensuite ces informations à Filtering Service.

> **Remarque**
>
> Plusieurs utilisateurs peuvent se connecter à un même serveur Novell eDirectory à partir d'un client Novell fonctionnant sous Windows. Dans ce cas, une même adresse IP est associée à plusieurs utilisateurs. Dans ce scénario, le mappage des utilisateurs d'eDirectory Agent ne conserve que la paire nom d'utilisateur/adresse IP du dernier utilisateur connecté à partir d'une adresse IP donnée.

Une même instance de Websense eDirectory Agent peut prendre en charge une instance principale de Novell eDirectory, plus n'importe quel nombre de répliques Novell eDirectory.



Considérations spéciales relatives à la configuration

- Si vous avez intégré Cisco Content Engine v5.3.1.5 ou version ultérieure à Websense :
  - Exécutez les services Websense suivants sur le même ordinateur que Cisco Content Engine :

Websense eDirectory Agent
Websense User Service
Websense Filtering Service
Websense Policy Server

- Assurez-vous que toutes les répliques Novell eDirectory ont été ajoutées dans le fichier **wsedir.ini** sur le même ordinateur.
- Supprimez le fichier **eDirAgent.bak**.

Exécutez les services Websense Reporting Tools sur un **autre** ordinateur que celui de Cisco Content Engine et de Websense.

- Websense prend en charge l'utilisation de NMAS avec eDirectory Agent. Pour utiliser eDirectory Agent avec NMAS activé, eDirectory Agent doit être installé sur un ordinateur qui exécute également Novell Client.

Configuration d'eDirectory Agent

Rubriques connexes :

- *Identification transparente*, page 201
- *Authentification manuelle*, page 203
- *Configuration des méthodes d'identification des utilisateurs*, page 204
- *eDirectory Agent*, page 224
- *Configuration d'eDirectory Agent pour l'utilisation de LDAP*, page 228
- *Configuration de plusieurs agents*, page 230

La page **Paramètres > Identification utilisateur > eDirectory Agent** permet de configurer une nouvelle instance d'eDirectory Agent et les paramètres globaux s'appliquant à toutes les instances d'eDirectory Agent.

Pour ajouter une nouvelle instance d'eDirectory Agent :

1. Sous Configuration de base de l'agent, entrez l'adresse IP ou le nom du **Serveur** sur lequel l'agent est installé.

   Remarque

   Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.

   Les noms d'ordinateur contenant des caractères ASCII étendus peuvent ne pas être résolus de façon appropriée. Si vous utilisez une version non anglaise de Websense, entrez une adresse IP plutôt qu'un nom d'ordinateur.

2. Entrez le numéro de **Port** qu'eDirectory Agent doit utiliser pour communiquer avec les autres composants de Websense. La valeur par défaut est 30700.

3. Pour établir une connexion authentifiée entre Filtering Service et eDirectory Agent, sélectionnez **Activer l'authentification** et entrez un **Mot de passe** de connexion.
4. Cliquez sur **OK** pour enregistrer vos modifications ou passez à la prochaine section de l'écran pour entrer d'autres informations de configuration.

Personnalisez ensuite les paramètres globaux de communication d'eDirectory Agent. Par défaut, les modifications apportées ici affectent toutes les instances d'eDirectory Agent. Les paramètres signalés par un astérisque (*) peuvent toutefois être remplacés dans le fichier de configuration d'un agent afin de personnaliser le comportement de cette instance (voir *Configuration de paramètres différents pour une instance d'agent*, page 232).

1. Entrez le numéro de **Port de communication** qu'eDirectory Agent doit utiliser pour communiquer avec les autres composants de Websense. La valeur par défaut est 30700.
2. Sauf autorisation expresse du support technique de Websense, ne modifiez pas le paramètre **Port de diagnostic**. La valeur par défaut est 30701.
3. Sous Serveur eDirectory, spécifiez la **Base de recherche** (contexte racine) qu'eDirectory Agent doit utiliser comme point de départ lorsqu'il recherche des informations d'utilisateurs dans l'annuaire.
4. Entrez les informations de compte d'administration qu'eDirectory Agent doit utiliser pour communiquer avec l'annuaire :
   a. Entrez le **Nom distinctif de l'administrateur** d'un compte d'administration Novell eDirectory.
   b. Entrez le **Mot de passe** utilisé par ce compte.
   c. Entrez un **Délai d'attente de l'entrée utilisateur** pour définir le délai de conservation des entrées dans le mappage des utilisateurs de l'agent.

      Cet intervalle doit être environ 30 % plus long qu'une session de connexion d'utilisateur typique. Il évite que des entrées d'utilisateur soient retirées du mappage avant que les utilisateurs n'aient terminé leur navigation.

      L'intervalle idéal est généralement celui proposé par défaut (24 heures).

      Remarque

      Dans certains environnements, au lieu d'utiliser le délai d'attente de l'entrée de l'utilisateur pour déterminer la fréquence selon laquelle eDirectory Agent actualise son mappage des utilisateurs, il peut être approprié de demander régulièrement à eDirectory Server les mises à jour des connexions des utilisateurs. Voir *Activation des requêtes complètes du serveur eDirectory*, page 229.

5. Ajoutez l'instance principale d'eDirectory Server et les répliques éventuelles dans la liste **Répliques eDirectory**. Pour ajouter une instance principale d'eDirectory Server dans la liste, cliquez sur **Ajouter** et suivez les instructions de la section *Ajout d'une réplique de serveur eDirectory*, page 228.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour enregistrer vos paramètres.

Ajout d'une réplique de serveur eDirectory

Une même instance de Websense eDirectory Agent peut prendre en charge une instance principale de Novell eDirectory, plus n'importe quel nombre de répliques Novell eDirectory s'exécutant sur des ordinateurs distincts.

eDirectory Agent doit pouvoir communiquer avec chaque ordinateur exécutant une réplique du service d'annuaire. L'agent obtient ainsi les informations de connexion les plus récentes aussi rapidement que possible et n'attend pas qu'une réplication d'eDirectory ne se produise.

Novell eDirectory réplique l'attribut qui identifie de façon unique les utilisateurs connectés toutes les 5 minutes. Malgré ce délai de réplication, eDirectory Agent récupère les nouvelles sessions de connexion dès qu'un utilisateur se connecte à une réplique eDirectory.

Pour configurer l'installation d'eDirectory Agent pour une communication avec eDirectory :

1. Dans l'écran Ajouter une réplique eDirectory, entrez l'adresse IP ou le nom du **Serveur** eDirectory (principal ou réplique).
2. Entrez le numéro de **Port** qu'eDirectory Agent utilise pour communiquer avec l'ordinateur eDirectory.
3. Cliquez sur **OK** pour revenir à la page eDirectory Agent. La nouvelle entrée apparaît dans la liste Répliques eDirectory.
4. Répétez éventuellement le processus pour d'autres serveurs eDirectory.
5. Cliquez sur **OK** pour mettre en cache vos modifications, puis cliquez sur **Enregistrer tout**.
6. Arrêtez et démarrez eDirectory Agent pour que l'agent puisse commencer à communiquer avec la nouvelle réplique. Reportez-vous à la section *Arrêt et démarrage des services Websense*, page 286 pour obtenir des instructions.

Configuration d'eDirectory Agent pour l'utilisation de LDAP

Websense eDirectory Agent peut utiliser le protocole NCP (Netware Core Protocol) ou LDAP (Lightweight Directory Access Protocol) pour obtenir les informations de connexion des utilisateurs auprès de Novell eDirectory. Par défaut, eDirectory Agent utilise NCP sous Windows. Sous Linux, eDirectory Agent doit utiliser LDAP.

Si vous exécutez eDirectory Agent sous Windows et si vous souhaitez que l'agent utilise LDAP pour interroger Novell eDirectory, définissez l'agent pour qu'il utilise LDAP au lieu de NCP. En général, NCP assure un mécanisme de requête plus efficace.

Pour qu'eDirectory Agent utilise LDAP sous Windows :

1. Assurez-vous de disposer d'au moins une réplique Novell eDirectory contenant tous les objets de l'annuaire pour surveiller et filtrer votre réseau.
2. Arrêtez le service Websense eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 286).
3. Localisez le répertoire d'installation d'eDirectory Agent (par défaut, **\Program Files\Websense\bin**), et ouvrez le fichier **wsedir.ini** dans un éditeur de texte.
4. Modifiez l'entrée **QueryMethod** comme suit :

   ```
   QueryMethod=0
   ```

   Ce paramètre indique à l'agent d'utiliser LDAP pour interroger Novell eDirectory. (La valeur par défaut est 1, pour NCP.)
5. Enregistrez et fermez le fichier.
6. Redémarrez le service Websense eDirectory Agent.

Activation des requêtes complètes du serveur eDirectory

Dans les petits réseaux, vous pouvez configurer Websense eDirectory Agent pour qu'il interroge le serveur eDirectory sur tous les utilisateurs connectés à intervalles réguliers. L'agent peut ainsi détecter les utilisateurs nouvellement connectés et les utilisateurs qui se sont déconnectés depuis la dernière requête, et mettre à jour son mappage local des utilisateurs de façon appropriée.

Important

Configurer eDirectory Agent pour qu'il utilise des requêtes complètes n'est pas conseillé sur les grands réseaux car le temps nécessaire pour renvoyer les résultats des requêtes dépend du nombre d'utilisateurs connectés. Plus le nombre d'utilisateurs connectés est important, plus les performances sont affectées.

Lorsque vous activez les requêtes complètes pour eDirectory Agent, le **délai d'attente de l'entrée de l'utilisateur** n'est pas utilisé car les utilisateurs qui se sont déconnectés sont identifiés par la requête. Par défaut, la requête intervient toutes les 30 secondes.

L'activation de cette fonction accroît le temps de traitement d'eDirectory Agent de deux manières :

- Du fait du temps nécessaire pour récupérer les noms des utilisateurs connectés à chaque nouvelle requête
- Du fait du temps nécessaire pour traiter les informations relatives aux noms d'utilisateurs, pour supprimer les entrées obsolètes du mappage local des utilisateurs et pour ajouter les nouvelles entrées en fonction de la dernière requête

eDirectory Agent examine le mappage local des utilisateurs dans son intégralité après chaque requête au lieu d'identifier uniquement les nouvelles connexions. Le temps requis par ce processus dépend du nombre d'utilisateurs renvoyés par chaque requête. Le processus peut donc affecter les délais de réponse d'eDirectory Agent et du serveur Novell eDirectory.

Pour activer les requêtes complètes :

1. Sur l'ordinateur eDirectory Agent, localisez le répertoire Websense **bin** (C:\Program Files\Websense\bin ou /opt/Websense/bin par défaut).
2. Localisez le fichier **wsedir.ini** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
3. Ouvrez le fichier **wsedir.ini** dans un éditeur de texte (tel que Notepad ou vi).
4. Localisez la section **[eDirAgent]**, puis l'entrée suivante :

   ```
   QueryMethod=<N>
   ```

   Prenez note de la valeur de QueryMethod pour le cas où vous souhaiteriez ensuite réinitialiser le paramètre par défaut.
5. Modifiez la valeur **QueryMethod** comme suit :
   - Si la valeur est 0 (communication avec l'annuaire via LDAP), remplacez-la par **2**.
   - Si la valeur est 1 (communication avec l'annuaire via NCP), remplacez-la par **3**.

   Remarque
   Si la modification de cette valeur de requête ralentit les performances du système, rétablissez la valeur précédente de l'entrée QueryMethod.
6. Si l'intervalle de requête par défaut (30 secondes) ne convient pas à votre environnement, modifiez la valeur de **PollInterval** de façon appropriée.

   Notez que l'intervalle est défini en **millisecondes**.
7. Enregistrez et fermez le fichier.
8. Redémarrez le service Websense eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 286).

Configuration de plusieurs agents

Rubriques connexes :

- *DC Agent*, page 213
- *Logon Agent*, page 216
- *RADIUS Agent*, page 219
- *eDirectory Agent*, page 224

Plusieurs agents d'identification transparente peuvent être combinés au sein du même réseau. Si la configuration de votre réseau requiert plusieurs agents, il est préférable d'installer chaque agent sur un ordinateur distinct. Dans certains cas, toutefois, vous pouvez configurer Websense pour qu'il fonctionne avec plusieurs agents sur un même ordinateur.

Les combinaisons suivantes d'agents d'identification transparente sont prises en charge :

Combinaison	Même ordinateur	Même réseau	Configuration requise
Plusieurs agents DC Agent	Non	Oui	Assurez-vous que toutes les instances de DC Agent puissent communiquer avec Filtering Service.
Plusieurs agents RADIUS Agent	Non	Oui	Configurez chaque instance pour qu'elle communique avec Filtering Service.
Plusieurs agents eDirectory Agent	Non	Oui	Configurez chaque instance pour qu'elle communique avec Filtering Service.
Plusieurs agents Logon Agent	Non	Oui	Configurez chaque instance pour qu'elle communique avec Filtering Service.
DC Agent + RADIUS Agent	Oui	Oui	Installez ces agents dans des répertoires distincts. Configurez chaque agent pour qu'il communique avec Filtering Service par un port de communication différent.
DC Agent + eDirectory Agent	Non	Non	Websense ne prend pas en charge les communications avec les deux services d'annuaire Windows et Novell dans le même déploiement. Les deux agents peuvent toutefois être installés, un seul étant actif.
DC Agent + Logon Agent	Oui	Oui	Configurez les deux agents pour qu'ils communiquent avec Filtering Service. Chaque agent utilisant par défaut un port unique, les conflits de ports ne posent pas de problème si ces ports ne sont pas modifiés.
eDirectory Agent + Logon Agent	Non	Non	Websense ne prend pas en charge les communications avec les deux services d'annuaire Windows et Novell dans le même déploiement. Les deux agents peuvent toutefois être installés, un seul étant actif.

Combinaison	Même ordinateur	Même réseau	Configuration requise
RADIUS Agent + eDirectory Agent	Oui	Oui	Configurez chaque agent pour qu'il communique avec Filtering Service par un port de communication différent.
DC Agent + Logon Agent + RADIUS Agent	Oui	Oui	Bien que cette combinaison ne soit que rarement nécessaire, elle est prise en charge. Installez chaque agent dans des répertoires distincts. Configurez tous les agents pour qu'ils communiquent avec Filtering Service par des ports de communication différents.

Configuration de paramètres différents pour une instance d'agent

Les paramètres de configuration d'un agent d'identification transparente de Websense Manager sont globaux et s'appliquent à toutes les instances de l'agent que vous avez installées. Toutefois, si plusieurs instances d'un agent s'exécutent, vous pouvez configurer une instance indépendamment des autres.

Les paramètres uniques que vous spécifiez pour une instance d'agent particulière remplacent les paramètres globaux de la boîte de dialogue Paramètres. Les paramètres remplaçables sont signalés par un astérisque (*).

1. Arrêtez le service de l'agent d'identification transparente (voir *Arrêt et démarrage des services Websense*, page 286).
2. Sur l'ordinateur dans lequel s'exécute l'instance de l'agent, localisez le répertoire d'installation de cet agent et ouvrez le fichier approprié dans un éditeur de texte :
   - pour DC Agent : **transid.ini**
   - pour Logon Agent : **authserver.ini**
   - pour eDirectory Agent : **wsedir.ini**
   - pour RADIUS Agent : **wsradius.ini**
3. Localisez le paramètre à modifier pour cette instance d'agent (voir *Paramètres du fichier INI*, page 233).

   Par exemple, vous pouvez activer une connexion authentifiée entre cette instance et les autres services Websense. Pour ce faire, entrez une valeur pour le paramètre **password** dans le fichier INI à:

   ```
   password=[xxxxxx]
   ```
4. Modifiez les autres valeurs selon vos besoins.
5. Enregistrez et fermez le fichier INI.
6. Si vous modifiez les paramètres de **DC Agent**, vous devez supprimer deux fichiers dans le répertoire Websense **bin** (C:\Program Files\Websense\bin, par défaut) :

a. Arrêtez les services Websense sur l'ordinateur DC Agent (voir *Arrêt et démarrage des services Websense*, page 286).

b. Supprimez les fichiers suivants :

```
Journal.dat
XidDcAgent.bak
```

Ces fichiers sont recréés lorsque vous démarrez le service Websense DC Agent.

c. Redémarrez les services Websense (y compris DC Agent) et passez à **l'étape 8**.

7. Redémarrez le service de l'agent d'identification transparente.
8. Actualisez les paramètres de l'agent dans Websense Manager :
   a. Sélectionnez **Paramètres >** Identification utilisateur.
   b. Sous **Agents d'identification transparente**, sélectionnez l'agent et cliquez sur **Éditer**.

> **Remarque**
> Si vous modifiez la valeur du **port** pour cette instance d'agent, supprimez l'agent, puis rajoutez-le. Sélectionnez d'abord l'entrée existante de l'agent et cliquez sur **Supprimer**, puis sur **Ajouter agent**.

   c. Vérifiez le **IP ou nom du serveur** et le **Port** utilisés par cette instance. Si vous avez spécifié un numéro de port unique dans le fichier INI, assurez-vous que votre entrée corresponde à cette valeur.
   d. Si vous avez spécifié un mot de passe d'authentification unique dans le fichier INI, assurez-vous que l'entrée **Mot de passe** affichée ici soit correcte.
   e. Cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Paramètres du fichier INI

Intitulé du champ Websense Manager	Nom du paramètre .ini	Description
Port de communication (*tous les agents*)	Port	Port par lequel l'agent communique avec les autres services Websense.
Port de diagnostic (*tous les agents*)	DiagServerPort	Port sur lequel l'outil de dépannage de l'agent écoute les données de l'agent.
Mot de passe (*tous les agents*)	password	Mot de passe utilisé par l'agent pour authentifier les connexions aux autres services Websense. Définissez un mot de passe pour activer l'authentification.
Intervalle de requête (*DC Agent*)	QueryInterval	Fréquence selon laquelle DC Agent interroge les contrôleurs de domaine.

Adresse IP ou nom du serveur Port (*eDirectory Agent*)	Server=IP:port	Adresse IP et numéro de port de l'ordinateur exécutant eDirectory Agent.
Base de recherche (*eDirectory Agent*)	SearchBase	Contexte racine du serveur Novell eDirectory.
Nom distinctif de l'administrateur (*eDirectory Agent*)	DN	Nom de l'administrateur du serveur Novell eDirectory.
Mot de passe (*eDirectory Agent*)	PW	Mot de passe de l'administrateur du serveur Novell eDirectory.
IP ou nom du serveur RADIUS	RADIUSHost	Adresse IP ou nom de votre serveur RADIUS.
RRAS machine IP (Windows uniquement) (*RADIUS Agent*)	RRASHost	Adresse IP de l'ordinateur exécutant RRAS. Websense interroge cet ordinateur sur les sessions de connexion des utilisateurs.
Ports d'authentification : entre RADIUS Agent et le serveur RADIUS	AuthOutPort	Port sur lequel le serveur RADIUS écoute les requêtes d'authentification.
Ports d'authentification : entre les clients RADIUS et RADIUS Agent	AuthInPort	Port sur lequel RADIUS Agent accepte les requêtes d'authentification.
Ports de demande de compte : entre RADIUS Agent et le serveur RADIUS	AccOutPort	Port sur lequel le serveur RADIUS écoute les requêtes de demande de compte RADIUS.
Ports de demande de compte : entre les clients RADIUS et RADIUS Agent	AccInPort	Port sur lequel RADIUS Agent accepte les requêtes de demande de compte.

Configuration d'un agent pour qu'il ignore certains noms d'utilisateur

Vous pouvez configurer un agent d'identification transparente pour qu'il ignore les noms de connexion non associés à de véritables utilisateurs. Cette fonction est souvent utilisée pour gérer la façon dont certains services Windows 200x et XP contactent les contrôleurs de domaine du réseau.

Par exemple, **utilisateur1** se connecte au réseau et est identifié par le contrôleur de domaine en tant que **ordinateurA/utilisateur1**. Cet utilisateur est filtré par une stratégie Websense affectée à **utilisateur1**. Si un service démarre sur l'ordinateur de l'utilisateur avec l'identité **ordinateurA/NomService** pour contacter le contrôleur de domaine, des problèmes de filtrage peuvent survenir. Websense traite **ordinateurA/NomService** comme un nouvel utilisateur auquel aucune stratégie n'a été attribuée et filtre cet utilisateur en fonction de la stratégie de l'ordinateur ou de la stratégie **Par défaut**.

Pour résoudre ce problème :

1. Arrêtez le service de l'gent (voir *Arrêt et démarrage des services Websense*, page 286).
2. Accédez au répertoire **\Websense\bin** et ouvrez le fichier **ignore.txt** dans un éditeur de texte.
3. Entrez chaque nom d'utilisateur sur une ligne distincte. N'utilisez pas de caractère générique comme « * ».

   ```
   maran01
   WindowsServiceName
   ```

   Websense ignore ces noms d'utilisateur, quel que soit l'ordinateur auquel ils sont associés.

   Pour indiquer à Websense d'ignorer un nom d'utilisateur dans un domaine spécifique, utilisez le format **nom d'utilisateur, domaine**.

   ```
   aperez, engineering1
   ```
4. Lorsque vous avez terminé, enregistrez et fermez le fichier.
5. Redémarrez le service de l'agent.

L'agent ignore les noms d'utilisateur spécifiés et Websense ne prend plus ces noms en compte dans le filtrage.

11 Administration déléguée

Rubriques connexes :

- *Présentation des rôles d'administration*, page 238
- *Présentation des administrateurs*, page 238
- *Mise en place des rôles d'administration*, page 243
- *Activation de l'accès à Websense Manager*, page 251
- *Utilisation de l'administration déléguée*, page 255
- *Accès à Websense Manager par plusieurs administrateurs*, page 266
- *Définition de restrictions de filtrage pour tous les rôles*, page 267

L'administration déléguée fournit des méthodes puissantes et flexibles pour gérer le filtrage Internet et créer des rapports pour des groupes de clients particuliers. Il s'agit d'un moyen efficace de partager les responsabilités de la gestion des accès Internet et de créer des gestionnaires individuels lorsque tous les utilisateurs sont situés en un emplacement central. Elle se révèle particulièrement efficace dans les grandes organisations réparties sur plusieurs emplacements et zones géographiques, puisqu'elle permet aux administrateurs locaux de gérer l'accès Internet et de créer des rapports sur l'activité de filtrage pour les utilisateurs depuis leur emplacement.

L'implémentation de l'administration déléguée implique de créer un rôle d'administration pour chaque groupe de clients devant être géré par les mêmes administrateurs. Les administrateurs individuels de chaque rôle peuvent être autorisés à gérer une stratégie ou à générer des rapports pour leurs clients, ou les deux. Voir *Mise en place des rôles d'administration*, page 243.

Le rôle Super administrateur est préinstallé et comprend l'administrateur par défaut : WebsenseAdministrator. Les super administrateurs ont accès à davantage de paramètres de stratégie et de configuration que les administrateurs des autres rôles. Voir *Super administrateurs*, page 239.

Présentation des rôles d'administration

Rubriques connexes :

- *Présentation des administrateurs*, page 238
- *Mise en place des rôles d'administration*, page 243

Un rôle d'administration est un ensemble de clients (utilisateurs, groupes, domaines, unités d'organisation, ordinateurs et plages réseau) gérés par un ou plusieurs administrateurs. Vous accordez aux administrateurs individuels des autorisations d'appliquer des stratégies aux clients du rôle, de générer des rapports, ou les deux.

Websense est installé avec un rôle de Super administrateur prédéfini. Il existe également un utilisateur par défaut, WebsenseAdministrator, membre automatique du rôle Super administrateur. Vous pouvez ajouter des administrateurs à ce rôle, mais vous ne pouvez pas supprimer l'administrateur par défaut.

Important

Vous ne pouvez pas supprimer le rôle de super administrateur prédéfini. L'utilisateur par défaut, WebsenseAdministrator, est un administrateur du rôle super administrateur mais il n'apparaît pas dans le rôle. Vous ne pouvez pas supprimer ni modifier les autorisations de l'administrateur WebsenseAdministrator.

Vous pouvez créer autant de rôles que nécessaire pour votre organisation. Par exemple, vous pouvez créer un rôle pour chaque département, en désignant le responsable de ce département comme administrateur et ses membres comme clients gérés. Dans une organisation distribuée géographiquement, vous pouvez créer un rôle pour chaque site géographique et attribuer tous les utilisateurs de ce site en tant que clients gérés de ce rôle. Un ou plusieurs individus de ce même site peuvent ensuite être nommés administrateurs.

Pour plus d'informations sur les options disponibles pour la définition des administrateurs, consultez la section *Présentation des administrateurs*, page 238.

Pour obtenir des instructions sur la création des rôles et la configuration des autorisations, consultez la section *Utilisation de l'administration déléguée*, page 255.

Présentation des administrateurs

Les administrateurs sont les personnes qui accèdent à Websense Manager pour gérer les stratégies ou générer des rapports sur un groupe de clients. Les autorisations spécifiques disponibles dépendent du type du rôle.

- Le Super administrateur est un rôle spécial prédéfini dans Websense Manager. Ce rôle assure davantage de flexibilité pour la définition des autorisations d'accès. Voir *Super administrateurs*, page 239.
- Les rôles d'administration déléguée doivent être créés par un Super administrateur. Les administrateurs de ces rôles disposent d'autorisations d'accès plus limitées. Voir *Administrateurs délégués*, page 241.

De plus, vous pouvez créer certains rôles d'administration déléguée limités à la création de rapports, en autorisant certaines personnes à générer des rapports sans leur attribuer des responsabilités de gestion des stratégies.

Vous pouvez attribuer des administrateurs à des rôles en utilisant leurs identifiants de connexion réseau ou vous pouvez créer des comptes spéciaux utilisés uniquement pour accéder à Websense Manager. Voir *Activation de l'accès à Websense Manager*, page 251.

Super administrateurs

Rubriques connexes :

- *Présentation des administrateurs*, page 238
- *Administrateurs délégués*, page 241
- *Administrateurs attribués à plusieurs rôles*, page 242

Le rôle Super administrateur est créé pendant l'installation. L'utilisateur par défaut, WebsenseAdministrator, est automatiquement attribué à ce rôle. De ce fait, lorsque vous vous connectez pour la première fois avec ce nom d'utilisateur et son mot de passe définis pendant l'installation, vous disposez d'un accès administrateur complet à tous les paramètres de stratégie, de création de rapports et de configuration dans Websense Manager.

Pour préserver l'accès complet de ce compte, WebsenseAdministrator n'apparaît pas dans la liste des administrateurs pour le rôle Super administrateur. Il ne peut pas être supprimé et ses autorisations ne sont pas modifiables.

Si nécessaire, vous pouvez ajouter des administrateurs au rôle de Super administrateur. Chaque administrateur peut se voir attribuer des autorisations comme suit :

- Les autorisations de **stratégie** permettent aux Super administrateurs de créer et de modifier les rôles d'administration déléguée et de copier des filtres et des stratégies dans ces rôles, selon les besoins. Ils peuvent également créer et modifier les composants du filtrage, les filtres et les stratégies, et appliquer des stratégies aux clients qui ne sont pas gérés par un autre rôle.

  En outre, les Super administrateurs qui disposent d'autorisations de stratégie peuvent consulter le journal d'audit et accéder aux options de configuration de Websense et à d'autres options, comme suit :

- Les autorisations **inconditionnelles** permettent au Super administrateur d'accéder à tous les paramètres de configuration système de l'installation Websense, par exemple aux paramètres de compte, de Policy Server et des serveurs Remote Filtering, aux options d'attribution de classe de risque et aux options de journalisation.

  Les Super administrateurs inconditionnels ont la possibilité de créer un Verrouillage du filtre qui bloque certaines catégories et certains protocoles pour tous les utilisateurs gérés par les rôles d'administration déléguée. Pour plus d'informations, consultez *Définition de restrictions de filtrage pour tous les rôles*, page 267.

  Les Super administrateurs inconditionnels peuvent modifier le rôle de super administrateur en ajoutant et en supprimant des administrateurs selon leurs besoins. Ils peuvent également supprimer des rôles d'administration déléguée ou supprimer des administrateurs ou des clients de ces rôles.

- Les autorisations **conditionnelles** permettent au Super administrateur d'accéder aux paramètres de téléchargement des bases de données, des services d'annuaire, d'identification des utilisateurs et de configuration de Network Agent. Les Super administrateurs conditionnels également autorisés à créer des rapports peuvent accéder aux paramètres de configuration des outils de rapports.

  Les Super administrateurs conditionnels peuvent ajouter des comptes utilisateur Websense mais pas les supprimer. Ils peuvent créer et modifier les rôles d'administration déléguée, mais pas supprimer les rôles, les administrateurs ou les clients gérés qui leur sont attribués. Ils ne peuvent pas non plus supprimer des administrateurs du rôle Super administrateur.

- Les autorisations de **génération de rapports** permettent au super administrateur d'accéder à toutes les fonctions de rapports et de générer des rapports sur tous les utilisateurs. Les Super administrateurs inconditionnels disposent automatiquement de l'autorisation de génération de rapports.

  Si un administrateur est uniquement autorisé à générer des rapports, les options Créer une stratégie, Recatégoriser une URL et Débloquer une URL de la liste Tâches communes ne sont pas disponibles. De plus, l'option Vérifier la stratégie ne s'affiche pas dans la Boîte à outils.

La création de plusieurs Super administrateurs inconditionnels permet de s'assurer qu'un autre administrateur peut accéder à tous les paramètres de stratégie et de configuration de Websense lorsque le Super administrateur principal n'est pas disponible.

N'oubliez pas que deux administrateurs ne peuvent pas se connecter en même temps pour gérer une stratégie pour le même rôle. Pour plus d'informations sur la prévention des conflits, consultez la section *Accès à Websense Manager par plusieurs administrateurs*, page 266.

Les privilèges uniques du rôle Super administrateur permettent à un administrateur du rôle d'accéder à tous les rôles. Pour changer de rôle après la connexion, sélectionnez-en un dans la liste déroulante **Rôle** de la bannière.

Après avoir changé de rôle, vos autorisations de stratégie se limitent à celles disponibles pour le rôle d'administration déléguée. Les filtres et les stratégies que vous créez ne sont disponibles qu'aux administrateurs de ce rôle et ne peuvent être appliqués qu'aux clients gérés par ce rôle. Voir *Administrateurs délégués*, page 241.

Les autorisations de génération de rapports sont cumulatives, c'est-à-dire que vous disposez des autorisations combinées de tous les rôles pour lesquels vous êtes administrateur. Les Super administrateurs inconditionnels disposent d'autorisations de génération de rapports complètes, quel que soit le rôle accédé.

Administrateurs délégués

Rubriques connexes :

- *Présentation des administrateurs*, page 238
- *Super administrateurs*, page 239
- *Administrateurs attribués à plusieurs rôles*, page 242

Les administrateurs délégués peuvent gérer les clients attribués un rôle spécifique. Attribuez à chaque administrateur des autorisations de stratégie, des autorisations de génération de rapports, ou les deux.

Les administrateurs délégués qui disposent d'autorisations de **stratégie** appliquent des stratégies aux clients attribués à leur rôle, déterminant ainsi l'accès Internet dont dispose chaque client. Dans le cadre de cette responsabilité, les administrateurs délégués peuvent créer, modifier et supprimer des stratégies et des filtres, soumis aux limites de Verrouillage du filtre établies par le Super administrateur. Voir *Définition de restrictions de filtrage pour tous les rôles*, page 267.

Remarque

Les administrateurs délégués exercent un contrôle important sur les activités Internet des clients qu'ils gèrent. Pour être certain que ce contrôle soit géré de façon responsable et selon les stratégies d'utilisation acceptées par l'organisation, les Super administrateurs peuvent utiliser la page Journal d'audit pour surveiller les modifications apportées par les administrateurs. Voir *Affichage et exportation du journal d'audit*, page 284.

Les administrateurs délégués ne peuvent pas supprimer la stratégie Par défaut.

Les administrateurs délégués peuvent modifier les composants de filtre, avec certaines restrictions. Pour plus d'informations, consultez *Création de stratégies et de filtres*, page 249.

Les administrateurs qui disposent d'autorisation de stratégie et qui se connectent à Websense Manager avec un compte utilisateur Websense peuvent également modifier leur propre mot de passe Websense. (Voir *Comptes utilisateur Websense*, page 253.)

Les options à la disposition des administrateurs délégués qui bénéficient d'autorisations de **génération de rapports** dépendent de la configuration du rôle. Il est possible qu'ils ne puissent générer de rapports que sur les clients gérés par leur rôle, ou qu'ils soient autorisés à générer des rapports sur tous les clients. Ils peuvent être autorisés à accéder à toutes les fonctions de rapports ou disposer d'un accès plus limité à la génération de rapports. Pour plus d'informations, consultez *Modification des rôles*, page 257.

Un administrateur qui ne dispose que d'autorisations de génération de rapports ne bénéficie que d'options limitées dans le panneau de raccourcis (Tâches communes et Boîte à outils).

Administrateurs attribués à plusieurs rôles

Rubriques connexes :

- *Présentation des administrateurs*, page 238
- *Super administrateurs*, page 239
- *Administrateurs délégués*, page 241

Selon les besoins de votre organisation, le même administrateur peut être attribué à plusieurs rôles. Les administrateurs attribués à plusieurs rôles doivent choisir un unique rôle à gérer lors de leur connexion.

Après la connexion, vos autorisations sont les suivantes :

- **Stratégie** : vous pouvez ajouter et modifier des filtres et des stratégies pour le rôle sélectionné lors de la connexion, et appliquer des stratégies aux clients gérés par ce rôle. La page Administration déléguée énumère tous les rôles qui vous sont attribués, ce qui vous permet de voir les clients gérés et les autorisations de génération de rapports de chaque rôle.
- **Génération de rapports** : vous disposez des autorisations de génération de rapports combinées de tous vos rôles. Supposons par exemple que trois rôles vous soient attribués, avec les autorisations de génération de rapports suivantes :
  - Rôle 1 : pas de génération de rapports
  - Rôle 2 : rapport sur les clients gérés uniquement, rapports d'investigation uniquement
  - Rôle 3 : rapport sur tous les clients, accès complet à toutes les fonctions de génération de rapports

  Dans ce cas, quel que soit le rôle choisi au moment de la connexion, vous êtes autorisé(e) à consulter des rapports dans les pages Aujourd'hui et Historique, et à générer des rapports sur tous les clients, à l'aide de toutes les fonctions de rapports.

  Si vous êtes connecté(e) pour la génération de rapports uniquement, le champ Rôle de la barre de la bannière précise si vous disposez d'une autorisation

Génération de rapports complète (rapport sur tous les clients) ou Génération de rapports limitée (rapport sur les clients gérés uniquement).

Mise en place des rôles d'administration

Rubriques connexes :

- *Présentation des rôles d'administration*, page 238
- *Notification des administrateurs*, page 245
- *Tâches des administrateurs délégués*, page 246

Pour mettre en place l'administration déléguée, le Super administrateur doit effectuer les tâches suivantes :

- Choisir comment les administrateurs se connecteront à Websense Manager. Voir *Activation de l'accès à Websense Manager*, page 251.
- Ajouter des rôles et les configurer. Voir *Utilisation de l'administration déléguée*, page 255.
- Informer les administrateurs de leurs responsabilités et de leurs options. Voir *Notification des administrateurs*, page 245.

Outre ces tâches obligatoires, d'autres tâches facultatives sont associées à l'administration déléguée.

Création du Verrouillage du filtre

Les Super administrateurs inconditionnels peuvent créer un Verrouillage du filtre, qui désigne certaines catégories et certains protocoles comme bloqués pour tous les clients gérés dans tous les rôles d'administration déléguée. Ces restrictions s'appliquent automatiquement à tous les filtres créés ou copiés dans un rôle d'administration déléguée et ne sont pas modifiables par l'administrateur délégué.

Remarque

Le Verrouillage du filtre ne s'applique pas aux clients gérés par le rôle Super administrateur.

Le Verrouillage du filtre peut également bloquer et verrouiller des types de fichiers et des mots-clés associés aux catégories sélectionnées et imposer la journalisation des protocoles sélectionnés. Voir *Création d'un verrouillage du filtre*, page 267.

Déplacement des clients

L'ajout d'un client dans la page Clients lorsque vous êtes connecté(e) en tant que Super administrateur attribue ce client au rôle Super administrateur. Ce client ne peut pas être ajouté à un rôle d'administration déléguée dans la page Modifier le rôle. Dans l'idéal, il est préférable d'ajouter directement les clients au rôle plutôt qu'en attribuant

une stratégie au sein du rôle Super administrateur. Toutefois, cela n'est pas toujours possible.

Pour transférer des clients du rôle Super administrateur vers un autre rôle, utilisez l'option **Déplacer vers le rôle** de la page Clients. Voir *Déplacements de clients vers des rôles*, page 70.

Dans le cadre du déplacement, la stratégie appliquée dans le rôle Super administrateur est copiée vers le rôle d'administration déléguée. Les filtres imposés par la stratégie sont également copiés. Au cours du processus de copie, les filtres sont mis à jour de manière à imposer les restrictions éventuelles du Verrouillage du filtre.

Dans le rôle cible, la mention « (Copié) » est ajoutée à la fin du nom du filtre ou de la stratégie. Les administrateurs de ce rôle peuvent identifier volontairement le nouvel élément et le mettre à jour de façon appropriée.

> **Remarque**
>
> Chaque fois qu'un filtre ou une stratégie est copié(e) vers le même rôle, la mention (Copié) reçoit un numéro incrémenté avec chaque nouvelle copie : (Copié 1), (Copié 2), etc. Chaque copie devient un filtre ou une stratégie distinct(e) au sein du rôle.
>
> Encouragez les administrateurs du rôle à renommer les filtres et les stratégies et à les modifier selon leurs besoins afin de simplifier la compréhension de leurs paramètres et de minimiser les doublons. Ces modifications peuvent simplifier la maintenance ultérieure.

Les filtres Autoriser tout du rôle Super administrateur permettent d'accéder à toutes les catégories ou à tous les protocoles, et ils ne sont pas modifiables. Pour préserver la capacité du Super administrateur à implémenter un Verrouillage du filtre, ces filtres ne peuvent pas être copiés vers un rôle d'administration déléguée.

Si le filtre attribué au client déplacé impose un filtre Autoriser tout, le client ne peut pas être déplacé jusqu'à ce que vous appliquiez une stratégie n'utilisant pas le filtre Autoriser tout.

Une fois le client déplacé vers le nouveau rôle, seul un administrateur de ce rôle peut en modifier la stratégie ou les filtres qu'il impose. Les modifications apportées à la stratégie ou aux filtres d'origine dans le rôle Super administrateur n'affectent pas les copies de la stratégie ou des filtres dans les rôles d'administration déléguée.

Copie de filtres et de stratégies

À l'origine, les filtres et les stratégies créés par un Super administrateur ne sont accessibles qu'aux administrateurs du rôle Super administrateur. Vous pouvez utiliser l'option **Copier dans le rôle** pour copier des filtres et des stratégies vers un rôle d'administration déléguée sans déplacer un client vers ce rôle. Voir *Copie de filtres et de stratégies vers des rôles*, page 172.

Lorsque vous copiez directement des filtres et des stratégies, les contraintes imposées lors de la copie de filtres et de stratégies dans le cadre d'un déplacement de client s'appliquent également.

- Les restrictions du Verrouillage du filtre sont implémentées pendant la copie.
- Les filtres de catégories et de protocoles Autoriser tout ne sont pas copiés.
- Les filtres et les stratégies copiés sont identifiés dans le rôle par la mention (Copié) qui apparaît dans le nom.

Le cas échéant, pensez à modifier les descriptions de la stratégie avant de démarrer la copie de manière à les rendre significatives pour les administrateurs des rôles visés.

Application de stratégies aux clients restants

Les clients qui ne sont pas attribués de façon spécifique à un rôle d'administration déléguée sont gérés par les Super administrateurs. Il n'existe pas de liste de Clients gérés pour le rôle Super administrateur.

Pour appliquer des stratégies à ces clients, ajoutez-les à la page Gestion des stratégies > Clients. Voir *Ajout d'un client*, page 68. Les clients qui n'ont pas été attribués à une stratégie spécifique sont gérés par la stratégie Par défaut de leur rôle.

Il peut arriver que vous ne puissiez pas ajouter de clients dans la page Clients. Cela peut se produire lorsque le client est membre d'un réseau, d'un groupe, d'un domaine ou d'une unité d'organisation attribué(e) à un autre rôle. Si l'administrateur de cet autre rôle a appliqué une stratégie à des membres individuels du réseau ou du groupe, ces clients ne peuvent pas être ajoutés au rôle Super administrateur.

Notification des administrateurs

Rubriques connexes :

- *Présentation des rôles d'administration*, page 238
- *Mise en place des rôles d'administration*, page 243

Après avoir attribué des individus en tant qu'administrateurs dans un rôle d'administration, assurez-vous de leur donner les informations suivantes.

- URL permettant de se connecter à Websense Manager. Par défaut :

  ```
  https://<IP_du_serveur>:9443/mng/
  ```

  Remplacez <IP_du_serveur>, par l'adresse IP de l'ordinateur exécutant Websense Manager.
- Serveur Policy Server à sélectionner lors de la connexion, le cas échéant. Dans un environnement disposant de plusieurs serveurs Policy Server, les administrateurs doivent en choisir un lors de leur connexion. Ils doivent dans ce cas choisir le serveur Policy Server configuré pour communiquer avec le service d'annuaire qui authentifie les clients qu'ils gèrent.

- S'ils doivent utiliser leur compte de connexion réseau ou un compte utilisateur Websense pour se connecter à Websense Manager. Si des administrateurs se connectent avec des comptes utilisateur Websense, fournissez-leur un nom d'utilisateur et un mot de passe.
- Leurs autorisations, qu'il s'agisse de créer et d'appliquer des stratégies aux clients du rôle, de générer des rapports, ou les deux.

  Conseillez aux administrateurs qui disposent à la fois des autorisations de stratégie et de génération de rapports de tenir compte des activités qu'ils prévoient d'effectuer au cours de la session. S'ils prévoient uniquement de générer des rapports, conseillez-leur d'accéder au champ **Rôle** dans la bannière et de choisir **Libérer les autorisations de stratégie**. Cette option libère les autorisations de stratégie pour le rôle, ce qui permet à un autre administrateur d'accéder à Websense Manager et de gérer une stratégie pour ce rôle.
- Comment trouver la liste des clients gérés par leur rôle. Les administrateurs peuvent ouvrir la page Gestion des stratégies > Administration déléguée et cliquer sur le nom de leur rôle pour afficher la page Modifier le rôle, qui présente la liste des clients gérés.
- Les limites imposées par le Verrouillage du filtre, lorsque des catégories ou des protocoles ont été bloqués et verrouillés.
- Les tâches généralement effectuées par les administrateurs. Voir *Tâches des administrateurs délégués*, page 246.

N'oubliez pas d'avertir les administrateurs délégués lorsque vous ajoutez ou modifiez des protocoles et des types de fichiers personnalisés. Ces composants s'affichant automatiquement dans les filtres et les stratégies de tous les rôles, il est donc important que ces administrateurs sachent que des modifications ont été apportées.

Tâches des administrateurs délégués

Rubriques connexes :

- *Présentation des rôles d'administration*, page 238
- *Mise en place des rôles d'administration*, page 243
- *Notification des administrateurs*, page 245

Les administrateurs délégués qui disposent d'autorisations de **stratégie** peuvent effectuer les tâches suivantes.

- *Affichage de votre compte utilisateur*, page 247
- *Affichage de la définition de votre rôle*, page 247
- *Ajout de clients dans la page Clients*, page 248
- *Création de stratégies et de filtres*, page 249
- *Application de stratégies à des clients*, page 250

Des autorisations de **génération de rapports** peuvent être accordées à un niveau granulaire. Les autorisations de génération de rapports spécifiques accordées à votre rôle déterminent les tâches disponibles aux administrateurs autorisés à générer des rapports parmi les tâches suivantes. Voir *Génération de rapports*, page 250.

Affichage de votre compte utilisateur

Rubriques connexes :

- *Tâches des administrateurs délégués*, page 246
- *Affichage de la définition de votre rôle*, page 247
- *Ajout de clients dans la page Clients*, page 248
- *Création de stratégies et de filtres*, page 249
- *Application de stratégies à des clients*, page 250

Si vous vous connectez à Websense Manager avec un identifiant réseau, les modifications du mot de passe sont gérées via le service d'annuaire de votre réseau. Au besoin, demandez l'aide de votre administrateur système.

Si un nom d'utilisateur et un mot de passe Websense vous ont été attribués, vous pouvez consulter les informations relatives à votre compte et modifier votre mot de passe dans Websense Manager.

1. Ouvrez la page **Gestion des stratégies > Administration déléguée**.
2. Cliquez sur **Gérer les comptes utilisateur Websense** en haut de la page.
3. Si vous souhaitez changer votre mot de passe, cliquez sur **Modifier le mot de passe**. Voir *Modification du mot de passe d'un utilisateur Websense*, page 254.
4. Pour afficher la liste des rôles pour lesquels vous êtes administrateur, cliquez sur **Afficher**.

Affichage de la définition de votre rôle

Rubriques connexes :

- *Tâches des administrateurs délégués*, page 246
- *Affichage de votre compte utilisateur*, page 247
- *Ajout de clients dans la page Clients*, page 248
- *Création de stratégies et de filtres*, page 249
- *Application de stratégies à des clients*, page 250

Ouvrez la page Administration déléguée et cliquez sur le nom de votre rôle pour afficher la page Modifier le rôle qui présente la liste des clients gérés du rôle. Cette

page présente également les fonctions de rapports disponibles aux administrateurs autorisés à générer des rapports dans ce rôle.

Les administrateurs qui ne disposent que des autorisations de génération de rapports ne peuvent pas consulter cette page. Ces administrateurs ne peuvent consulter que les fonctions de génération de rapports spécifiées.

Ajout de clients dans la page Clients

Rubriques connexes :

- *Tâches des administrateurs délégués*, page 246
- *Affichage de votre compte utilisateur*, page 247
- *Affichage de la définition de votre rôle*, page 247
- *Création de stratégies et de filtres*, page 249
- *Application de stratégies à des clients*, page 250

Les super administrateurs attribuent des clients gérés à un rôle, mais les administrateurs délégués doivent les ajouter dans la page Clients avant d'appliquer des stratégies. Reportez-vous à la section *Ajout d'un client*, page 68 pour obtenir des instructions.

Dès que des clients sont ajoutés dans la liste des clients gérés du rôle, ils sont filtrés par la stratégie Par défaut de ce rôle. Les clients qui ont été déplacés vers le rôle à partir de la page Clients du super administrateur sont gérés par la stratégie appliquée par ce dernier, copiée vers le rôle lors du déplacement du client.

Tous les clients apparaissant dans la liste de la page Administration déléguée > Modifier le rôle de votre rôle peuvent être ajoutés à la page Clients et attribués à une stratégie. Vous pouvez également ajouter des utilisateurs ou des ordinateurs individuels membres d'un groupe, d'un domaine, d'une unité d'organisation ou d'une plage réseau attribué en tant que client géré dans votre rôle.

Comme un utilisateur peut faire parti de plusieurs groupes, domaines ou unités d'organisation, l'ajout d'individus à partir d'un regroupement plus important de clients peut éventuellement créer des conflits lorsque des rôles différents gèrent les groupes, les domaines ou les unités d'organisation présentant des membres communs. Si des administrateurs de rôles différents accèdent à Websense Manager en même temps, ils peuvent ajouter le même client (membre individuel d'un groupe, par exemple) à leur page Clients. Dans ce cas, le filtrage Internet de ce client est régi par la priorité établie pour chaque rôle. Voir *Gestion des conflits entre rôles*, page 263.

Création de stratégies et de filtres

Rubriques connexes :

- *Tâches des administrateurs délégués*, page 246
- *Affichage de votre compte utilisateur*, page 247
- *Affichage de la définition de votre rôle*, page 247
- *Ajout de clients dans la page Clients*, page 248
- *Application de stratégies à des clients*, page 250

Lorsque votre rôle a été créé, il a automatiquement hérité de la stratégie par défaut, du filtre de catégories et du filtre de protocoles préinstallés, tels qu'ils étaient définis à ce moment-là. Le Super administrateur a également pu choisir de copier des stratégies et des filtres dans votre rôle.

Outre les stratégies et les filtres, vous héritez également des protocoles et des types de fichiers personnalisés créés par le Super administrateur.

Vous êtes libre de modifier les stratégies et lesfiltres hérités du Super administrateur. Les modifications que vous apportez n'affectent que votre rôle. Toutes les modifications apportées par le Super administrateur aux stratégies et aux filtres dont vous avez hérités précédemment n'affectent pas votre rôle.

Remarque

Les modifications apportées par le Super administrateur aux protocoles et aux types de fichiers personnalisés affectent automatiquement les filtres et les stratégies de votre rôle.

Lorsque votre Super administrateur vous signale des modifications de ces composants, vérifiez vos filtres et vos stratégies pour vous assurer qu'ils sont correctement gérés.

Vous pouvez également créer autant de filtres et de stratégies que nécessaire. Les filtres et les stratégies créés par un administrateur délégué ne sont disponibles qu'aux administrateurs connectés à votre rôle. Pour plus d'informations sur la création de stratégies, consultez la section *Fonctionnement des stratégies*, page 75. Pour plus d'informations sur la création de filtres, consultez la section *Fonctionnement des filtres*, page 48.

Vous pouvez modifier les composants de filtre pour votre rôle, avec certaines restrictions.

- **Catégories** : ajoutez des catégories personnalisées et modifiez la base de données principale et les catégories personnalisées, en définissant des URL recatégorisées et des mots-clés à utiliser au sein de leur rôle. Modifiez l'action et l'option de filtrage avancé appliquées par défaut dans les filtres de catégories qu'elles créent.

(Les modifications apportées à l'action par défaut d'une catégorie ne sont implémentées que si la catégorie n'est pas verrouillée par le Verrouillage du filtre.)

- **Protocoles** : modifiez l'action et les options de filtrage avancé appliquées par défaut dans les filtres de protocoles qu'ils créent. (Les modifications apportées à l'action par défaut d'un protocole ne sont implémentées que si le protocole n'est pas verrouillé par le Verrouillage du filtre.) Les administrateurs délégués ne peuvent pas ajouter ni supprimer de définitions de protocole.
- **Types de fichiers** : affichez les extensions de fichier affectées à chaque type de fichiers. Les administrateurs délégués ne peuvent pas ajouter de types de fichiers ni modifier les extensions affectées à un type de fichier.
- **URL non filtrées** : ajoutez des URL et des expressions régulières représentant les sites à autoriser pour tous les clients gérés dans leur rôle uniquement.

Pour plus d'informations, consultez *Construction de composants de filtres*, page 174.

Si un Super administrateur a implémenté des restrictions de Verrouillage du filtre, certains protocoles ou catégories peuvent être automatiquement bloqués et ne plus être modifiables dans les filtres que vous créez et modifiez. Voir *Définition de restrictions de filtrage pour tous les rôles*, page 267.

Application de stratégies à des clients

Rubriques connexes :

- *Tâches des administrateurs délégués*, page 246
- *Affichage de votre compte utilisateur*, page 247
- *Affichage de la définition de votre rôle*, page 247
- *Ajout de clients dans la page Clients*, page 248
- *Création de stratégies et de filtres*, page 249

Après avoir créé une stratégie, vous pouvez l'appliquer directement aux clients qui ont déjà été ajoutés à la page Clients en cliquant sur le bouton **Appliquer aux clients**. Voir *Attribution d'une stratégie aux clients*, page 79.

Vous pouvez également ouvrir la page Clients et ajouter les clients devant être régis par cette stratégie. Voir *Fonctionnement des clients*, page 60.

Génération de rapports

Si vous disposez d'autorisations de génération de rapports, les options de rapports spécifiques disponibles sont définies par le Super administrateur. Pour voir quelles options vous pouvez utiliser, ouvrez la page Administration déléguée et cliquez sur le nom du rôle. La page Modifier le rôle présente les fonctions de rapports pour lesquelles vous disposez d'autorisations. Pour plus d'informations, consultez *Modification des rôles*, page 257.

Activation de l'accès à Websense Manager

Lorsque vous configurez des rôles d'administration déléguée, vous déterminez les fonctions de Websense Manager auxquelles les administrateurs peuvent accéder. Pour garantir que les utilisateurs qui se connectent à Websense Manager disposent des fonctions appropriées, chaque utilisateur doit se connecter avec un nom d'utilisateur et un mot de passe. Deux types de comptes peuvent être utilisés :

- Les **comptes réseau** utilisent les identifiants déjà définis dans le service d'annuaire de votre réseau (voir *Comptes de l'annuaire*, page 251).
- Les **comptes utilisateur Websense** vous permettent de créer un nom d'utilisateur et un mot de passe à utiliser exclusivement dans Websense Manager (voir *Comptes utilisateur Websense*, page 253).

Comptes de l'annuaire

Rubriques connexes :

- *Activation de l'accès à Websense Manager*, page 251
- *Comptes utilisateur Websense*, page 253

Les Super administrateurs inconditionnels peuvent utiliser la page **Paramètres > Général > Annuaire de connexion** pour entrer les informations de services d'annuaire nécessaires pour autoriser les administrateurs à se connecter à Websense Manager avec leurs identifiants réseau.

Remarque

Ces informations servent uniquement à authentifier les utilisateurs de Websense Manager. Elles ne s'appliquent pas au filtrage des clients. Les informations du service d'annuaire des clients sont configurées à la page Paramètres > Services d'annuaire (voir *Services d'annuaire*, page 63).

Les identifiants réseau des utilisateurs de Websense Manager doivent être authentifiés par rapport au contenu d'un seul service d'annuaire. Si votre réseau comprend plusieurs services d'annuaire, une relation approuvée doit exister entre le service Annuaire de connexion que vous configurez dans Websense Manager et les autres services.

S'il n'est pas possible de définir un seul service d'annuaire à utiliser avec Websense Manager, envisagez plutôt la création de comptes utilisateur Websense pour les administrateurs (voir *Comptes utilisateur Websense*, page 253).

Pour définir le service d'annuaire que Websense Manager doit utiliser pour authentifier les administrateurs, vérifiez d'abord que l'option d'utilisation d'un service

d'annuaire pour l'authentification des administrateurs est sélectionnée, puis sélectionnez un type de **Service d'annuaire** dans la liste.

Si vous sélectionnez le service par défaut, **Annuaire Windows NT/Active Directory (Mixed Mode)**, aucune configuration supplémentaire n'est nécessaire. Cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Si vous sélectionnez **Active Directory (mode natif)** ou **Autre annuaire LDAP**, fournissez les informations suivantes :

1. Entrez l'adresse IP ou le nom de l'ordinateur sur lequel le service d'annuaire est installé.

   Si vous utilisez Active Directory (mode natif) et que vous avez configuré vos serveurs de catalogues global pour le basculement, vous pouvez entrer le nom de domaine DNS à la place.
2. Entrez le **Port** utilisé pour la communication du service d'annuaire.
3. Pour crypter la communication avec le service d'annuaire, cochez la case **Utiliser SSL**.
4. Entrez le **Nom distinctif de l'utilisateur** et le **Mot de passe** que Websense doit utiliser pour se connecter au service d'annuaire.
5. Entrez le **Contexte du domaine par défaut** que Websense doit utiliser lors de l'authentification des administrateurs.
   - Si vous utilisez Active Directory (mode natif), la configuration est terminée. Cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.
   - Si vous utilisez un autre service d'annuaire de type LDAP, continuez la procédure.
6. Entrez les **Attributs d'ID de connexion utilisateur** et le **Filtre de recherche d'utilisateur**, que Websense doit éventuellement utiliser pour accélérer l'authentification des utilisateurs.

   Ces informations s'affichent également à la page **Paramètres > Services d'annuaire**, sous **Paramètres de l'annuaire avancés**. Le cas échéant, vous pouvez copier et coller ces valeurs.
7. Dans Options de groupe, spécifiez si votre schéma LDAP comprend l'attribut **MemberOf** :
   - Si MemberOf n'est pas utilisé, spécifiez le **Filtre de recherche de groupe d'utilisateurs** que Websense doit appliquer pour authentifier les administrateurs.
   - Si MemberOf est utilisé, spécifiez l'**Attribut de groupe** qui doit être appliqué.
8. Si votre schéma LDAP comprend des groupes imbriqués, cochez la case **Effectuez une recherche de groupe imbriqué supplémentaire**.
9. Si votre service d'annuaire utilise des références LDAP, indiquez si Websense doit les utiliser ou les ignorer.

10. Cliquez sur **OK** pour mettre en cache vos modifications. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Comptes utilisateur Websense

Rubriques connexes :

- *Activation de l'accès à Websense Manager*, page 251
- *Ajout de comptes utilisateur Websense*, page 253

Les Super administrateurs utilisent la page **Administration déléguée > Gérer les comptes utilisateur Websense** pour créer des comptes permettant aux administrateurs d'accéder à Websense Manager sans avoir à saisir leurs identifiants réseau. Cette page permet également aux Super administrateurs de modifier le mot de passe des comptes utilisateur Websense et d'afficher les rôles auxquels un utilisateur Websense est attribué en tant qu'administrateur.

Les Super administrateurs inconditionnels peuvent également supprimer des comptes utilisateur Websense à partir de cette page.

Les administrateurs délégués utilisent cette page pour modifier leur mot de passe Websense et afficher les rôles dont ils sont administrateurs.

Option	Description
Ajouter	Ouvre la page de création d'un nouveau compte utilisateur Websense. Voir *Ajout de comptes utilisateur Websense*, page 253.
Modifier le mot de passe	Ouvre la page permettant de modifier le mot de passe du compte associé. Voir *Modification du mot de passe d'un utilisateur Websense*, page 254.
Afficher	Affiche la liste des rôles dont cet utilisateur est administrateur.
Supprimer	Cochez la case d'un ou plusieurs comptes utilisateur obsolètes, puis cliquez sur ce bouton pour le(s) supprimer.
Fermer	Permet de revenir à la page Administration déléguée.

Ajout de comptes utilisateur Websense

Rubriques connexes :

- *Activation de l'accès à Websense Manager*, page 251
- *Comptes utilisateur Websense*, page 253
- *Modification du mot de passe d'un utilisateur Websense*, page 254

La page **Administration déléguée > Gérer les comptes utilisateur Websense > Ajouter un utilisateur Websense** permet d'ajouter des comptes utilisateur Websense .

1. Entrez un **Nom d'utilisateur** unique comportant jusqu'à 50 caractères.

   Le nom doit être compris entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Les noms d'utilisateur peuvent comprendre des espaces et des tirets.
2. Entrez et confirmez un **Mot de passe** compris entre 4 et 255 caractères.

   Des mots de passe renforcés sont conseillés : 8 caractères minimum, avec au moins chacun de l'un des éléments suivants :

   - Lettre majuscule
   - Lettre minuscule
   - Chiffre
   - Caractère spécial (par exemple un tiret, un trait de soulignement ou un espace)
3. Lorsque vous avez terminé, cliquez sur **OK** pour mettre en cache les modifications et revenir à la page Gérer les comptes utilisateur Websense. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Modification du mot de passe d'un utilisateur Websense

Rubriques connexes :

- *Activation de l'accès à Websense Manager*, page 251
- *Comptes utilisateur Websense*, page 253
- *Ajout de comptes utilisateur Websense*, page 253

La page **Administration déléguée > Gérer les comptes utilisateur Websense > Modifier le mot de passe** permet aux administrateurs délégués de modifier le mot de passe de leur propre compte utilisateur Websense. Les Super administrateurs peuvent utiliser cette page pour modifier le mot de passe de n'importe quel compte utilisateur Websense.

1. Vérifiez que le **Nom d'utilisateur** approprié apparaît en haut de la page.
2. Entrez et confirmez le nouveau **Mot de passe** (4 à 255 caractères) de cet utilisateur.

   Des mots de passe renforcés sont conseillés : 8 caractères minimum, avec au moins chacun de l'un des éléments suivants :

   - Lettre majuscule
   - Lettre minuscule
   - Chiffre
   - Caractère spécial (par exemple un tiret, un trait de soulignement ou un espace)

3. Lorsque vous avez terminé, cliquez sur **OK** pour mettre en cache les modifications et revenir à la page Gérer les comptes utilisateur Websense. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Utilisation de l'administration déléguée

Rubriques connexes :

- *Présentation des rôles d'administration*, page 238
- *Gestion des conflits entre rôles*, page 263

La page **Gestion des stratégies > Administration déléguée** propose des options différentes selon si elle est affichée par un Super administrateur ou par un administrateur délégué.

Les Super administrateurs voient la liste de tous les rôles actuellement définis et disposent des options suivantes.

Option	Description
Ajouter	Cliquez sur cette option pour ajouter un nouveau rôle. Voir *Ajout de rôles*, page 256.
Rôle	Cliquez sur cette option pour afficher ou configurer le rôle. Voir *Modification des rôles*, page 257.
Supprimer	Cliquez cette option pour supprimer les rôles sélectionnés dans la liste. Cette option n'est disponible que pour les Super administrateurs inconditionnels. Pour plus d'informations sur la gestion des clients après la suppression du rôle, consultez la section *Considérations particulières*, page 264.
Avancé	Cliquez sur cette option pour accéder à la fonction Gérer la priorité des rôles.
Gérer la priorité des rôles	Cliquez sur cette option pour définir les paramètres de stratégie du rôle devant être utilisés lorsque le même client est membre de plusieurs groupes gérés par des rôles différents. Voir *Gestion des conflits entre rôles*, page 263.

Option	Description
Gérer les comptes utilisateur Websense	Cliquez sur cette option pour ajouter, modifier et supprimer les noms d'utilisateur et les mots de passe des comptes utilisés uniquement pour accéder à Websense Manager. Voir *Comptes utilisateur Websense*, page 253.
Gérer les groupes LDAP personnalisés	Cliquez sur cette option pour ajouter, modifier et supprimer les groupes LDAP personnalisés pouvant être attribués en tant que clients gérés dans les rôles d'administration déléguée. Voir *Travail avec des groupes LDAP personnalisés*, page 66. Cette option n'est pas disponible si le service d'annuaire configuré est Windows NT/Active Directory (Mixed Mode).

Les administrateurs délégués ne voient que les rôles dont ils sont administrateurs et disposent d'options limitées.

Option	Description
Rôle	Cliquez sur cette option pour afficher les clients attribués au rôle et les autorisations de génération de rapports spécifiques accordées. Voir *Modification des rôles*, page 257.
Gérer les comptes utilisateur Websense	Cliquez sur cette option pour accéder aux options de modification de votre mot de passe Websense Manager et d'affichage des rôles qui vous sont attribués. Voir *Comptes utilisateur Websense*, page 253.

Ajout de rôles

Rubriques connexes :

- *Modification des rôles*, page 257
- *Considérations particulières*, page 264

La page **Administration déléguée > Ajouter un rôle** permet d'entrer le nom et la description du nouveau rôle.

1. Entrez le **Nom** du nouveau rôle.

   Le nom doit être compris entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Les noms de rôle peuvent comprendre des espaces et des tirets.

2. Entrez la **Description** du nouveau rôle.

   Cette description peut comprendre jusqu'à 255 caractères. Les restrictions de caractères qui s'appliquent aux noms de rôle s'appliquent également aux descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).

3. Cliquez sur **OK** pour afficher la page **Modifier le rôle** et définir les caractéristiques de ce rôle. Voir *Modification des rôles*, page 257.

   Le nouveau rôle apparaît dans la liste déroulante Rôle de la bannière dès votre prochaine connexion à Websense Manager.

Modification des rôles

Rubriques connexes :

- *Utilisation de l'administration déléguée*, page 255
- *Ajout de rôles*, page 256
- *Gestion des conflits entre rôles*, page 263

Les administrateurs délégués peuvent utiliser la page **Administration déléguée > Modifier le rôle** pour consulter la liste des clients gérés par leur rôle, et les autorisations de génération de rapports spécifiques accordées.

Les Super administrateurs peuvent utiliser cette page pour sélectionner les administrateurs et les clients d'un rôle et définir les autorisations des administrateurs, tel que décrit ci-dessous. Seuls les Super administrateurs inconditionnels peuvent supprimer des administrateurs et des clients dans un rôle.

1. Modifiez le **Nom** et la **Description** du rôle, selon vos besoins.

   Remarque
   Le nom du rôle Super administrateur ne peut pas être modifié.

2. Ajoutez et supprimez des administrateurs pour ce rôle. (Disponible pour les Super administrateurs uniquement, cette section n'apparaît pas si vous êtes connecté(e) en tant qu'administrateur délégué.)

Élément	Description
Nom d'utilisateur	Nom d'utilisateur de l'administrateur.
Type de compte	Indique si l'utilisateur est défini dans le service d'annuaire réseau (Annuaire) ou en tant que compte utilisateur Websense (Websense).
Génération de rapports	Cochez cette case pour autoriser l'administrateur à utiliser des outils de génération de rapports.
Stratégie	Cochez cette case pour autoriser l'administrateur à créer des filtres et des stratégies et appliquer des stratégies aux clients gérés du rôle. Dans le rôle Super administrateur, les administrateurs disposant d'une autorisation de stratégie peuvent également gérer certains paramètres de configuration de Websense. Voir *Super administrateurs*, page 239.

Élément	Description
Inconditionnel	Disponible uniquement pour le rôle Super administrateur. Cochez cette case pour autoriser l'administrateur à gérer tous les paramètres de configuration de Websense et le Verrouillage du filtre. Seuls les Super administrateurs inconditionnels peuvent accorder des autorisations inconditionnelles à un nouvel administrateur.
Ajouter	Ouvre la page **Ajouter des administrateurs**. Voir *Ajout d'administrateurs*, page 260.
Supprimer	Supprime du rôle tous les administrateurs cochés dans la liste Administrateurs. (Cette option n'est disponible que pour les Super administrateurs inconditionnels).

3. Ajoutez et supprimez des **Clients gérés** pour le rôle. (Seuls les Super administrateurs peuvent apporter des modifications. Les administrateurs délégués peuvent consulter les clients attribués à leur rôle.)

Élément	Description
<Nom>	Affiche le nom de chaque client attribué explicitement au rôle. Les administrateurs du rôle doivent ajouter les clients dans la page Clients avant que des stratégies ne puissent être appliquées. Voir *Tâches des administrateurs délégués*, page 246.
Ajouter	Ouvre la page **Ajouter des clients gérés**. Voir *Ajout de clients gérés*, page 262.
Supprimer	Disponible uniquement pour les Super administrateurs inconditionnels, ce bouton supprime du rôle tous les clients cochés dans la liste des clients gérés. Certains clients ne peuvent pas être supprimés directement de la liste des clients gérés. Pour plus d'informations, consultez *Considérations particulières*, page 264.

4. Utilisez la zone **Autorisations de génération de rapports** pour sélectionner les fonctions disponibles aux administrateurs de ce rôle qui disposent d'un droit d'accès à la création de rapports.

a. Choisissez le niveau général des autorisations de génération de rapports :

Option	Description
Rapport sur tous les clients	Sélectionnez cette option pour autoriser les administrateurs à générer des rapports sur tous les utilisateurs du réseau. Servez-vous des options restantes de la zone Autorisations de génération de rapports pour définir des autorisations spécifiques pour les administrateurs de ce rôle.
Rapport sur les clients gérés uniquement	Sélectionnez cette option pour limiter les administrateurs à la génération de rapports sur les clients gérés attribués à ce rôle. Sélectionnez ensuite les fonctions de rapports d'investigation auxquels ces administrateurs peuvent accéder. Les administrateurs limités à la création de rapports sur les clients gérés ne peuvent pas accéder aux rapports de présentation ou aux rapports basés sur les utilisateurs dans les pages Aujourd'hui et Historique. Ils ne peuvent pas non plus gérer les paramètres de la base de données d'activité.

b. Cochez la case de chaque fonction de génération de rapports que les administrateurs du rôle peuvent utiliser.

Option	Description
Accéder aux rapports de présentation	Permet d'accéder aux fonctions des rapports de présentation. Cette option n'est disponible que si les administrateurs peuvent générer des rapports sur tous les clients. Voir *Rapports de présentation*, page 98.
Afficher des rapports dans les pages Aujourd'hui et Historique	Permet d'afficher des graphiques illustrant l'activité Internet dans ces pages. Voir *Aujourd'hui : état, sécurité et utilité depuis minuit*, page 22 et *Historique : 30 derniers jours*, page 25. Si cette option est désactivée, les administrateurs ne peuvent afficher que les zones Alertes d'état et Valeur de la page Aujourd'hui et la zone Estimations de valeurs de la page Historique.
Accéder aux rapports d'investigation	Permet d'accéder aux fonctions de base des rapports d'investigation. Lorsque cette option est activée, d'autres fonctions de rapports d'investigation peuvent également être sélectionnées. Voir *Rapports d'investigation*, page 118.
Afficher des noms d'utilisateurs dans les rapports d'investigation	Permet aux administrateurs de ce rôle d'afficher les noms d'utilisateur, s'ils sont connectés. Voir *Configuration de Filtering Service pour la journalisation*, page 308. Désactivez cette option pour n'afficher que les codes d'identification générés par le système à la place des noms. Cette option n'est disponible que si les administrateurs sont autorisés à accéder aux rapports d'investigation.

Option	Description
Enregistrer les rapports d'investigation comme favoris	Permet aux administrateurs de ce rôle de créer des rapports d'investigation favoris. Voir *Rapports d'investigation favoris*, page 136. Cette option n'est disponible que si les administrateurs sont autorisés à accéder aux rapports d'investigation.
Planifier les rapports d'investigation	Permet aux administrateurs de ce rôle de planifier l'exécution ultérieure ou périodique de rapports d'investigation. Voir *Planification des rapports d'investigation*, page 138. Cette option n'est disponible que si les administrateurs sont autorisés à enregistrer les rapports d'investigation comme favoris.
Gérer la base de données d'activité	Permet aux administrateurs d'accéder à la page Paramètres > Base de données d'activité. Voir *Paramètres d'administration de la base de données d'activité*, page 324. Cette option n'est disponible que si les administrateurs peuvent générer des rapports sur tous les clients.

5. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Administration déléguée. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout d'administrateurs

Rubriques connexes :

- *Modification des rôles*, page 257
- *Activation de l'accès à Websense Manager*, page 251

Les Super administrateurs peuvent utiliser la page **Administration déléguée > Modifier le rôle** > **Ajouter des administrateurs** pour désigner les administrateurs d'un rôle.

Remarque

Des administrateurs peuvent être ajoutés à plusieurs rôles. Ces administrateurs doivent alors choisir un rôle lors de leur connexion. Dans ce cas, l'administrateur dispose d'autorisations de génération de rapports combinées pour tous les rôles.

Les administrateurs délégués exercent un contrôle important sur les activités Internet de leurs clients gérés. Pour être certain que ce contrôle soit géré de façon responsable et selon les stratégies d'utilisation acceptées par l'organisation, les Super administrateurs peuvent utiliser la page Journal d'audit pour surveiller les

modifications apportées par les administrateurs. Voir *Affichage et exportation du journal d'audit*, page 284.

1. Si vous envisagez d'ajouter des comptes d'annuaire en tant qu'administrateurs délégués, assurez-vous d'être connecté(e) au serveur Policy Server dont la configuration du Service d'annuaire (voir *Services d'annuaire*, page 63) correspond à celle de l'Annuaire de connexion (voir *Comptes de l'annuaire*, page 251).

   Si vous ajoutez uniquement des comptes utilisateur Websense comme administrateurs, vous pouvez être connecté(e) à n'importe quel serveur Policy Server.

2. Sous **Comptes de l'annuaire**, cochez la case d'un ou plusieurs utilisateurs, puis cliquez sur la flèche droite (>) pour les déplacer vers la liste **Sélectionné**.

   > **Remarque**
   > Les groupes LDAP personnalisés ne peuvent pas être ajoutés en tant qu'administrateurs.

   Si votre environnement utilise Active Directory (mode natif) ou un autre service d'annuaire de type LDAP, vous pouvez rechercher dans l'annuaire des noms d'utilisateur, de groupe, de domaine ou d'unité d'organisation spécifiques. Voir *Recherche dans le service d'annuaire*, page 69.

3. Sous **Comptes utilisateur Websense**, cochez la case d'un ou plusieurs utilisateurs, puis cliquez sur la flèche droite pour déplacer les utilisateurs sélectionnés vers la liste **Sélectionné**.

4. Définissez les **Autorisations** des administrateurs de ce rôle.

Option	Description
Stratégie	Cochez cette option pour autoriser les administrateurs de ce rôle à appliquer des stratégies à leurs clients gérés. Cette option permet également d'accéder à certains paramètres de configuration de Websense.
Inconditionnel	Cochez cette option pour autoriser l'accès à tous les paramètres de configuration de Websense. Cette option n'est disponible que lorsqu'un Super administrateur inconditionnel ajoute des administrateurs au rôle Super administrateur avec des autorisations de stratégie.
Génération de rapports	Cochez cette option pour autoriser l'accès aux outils de génération de rapports. Utilisez la page Modifier le rôle pour définir les fonctions de rapport autorisées de façon spécifique.

5. Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier le rôle.

6. Dans la page Modifier le rôle, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout de clients gérés

Rubriques connexes :

- *Utilisation de l'administration déléguée*, page 255
- *Modification des rôles*, page 257

Les clients gérés sont des utilisateurs et des ordinateurs attribués à un rôle, et dont les stratégies sont définies par les administrateurs de ce rôle. Les clients de l'annuaire (utilisateurs, groupes, domaines et unités d'organisation), les ordinateurs et les réseaux peuvent tous être définis en tant que clients gérés.

Les Super administrateurs peuvent utiliser la page **Administration déléguée > Modifier le rôle > Ajouter des clients gérés** pour ajouter autant de clients que nécessaire dans un rôle. Chaque client ne peut être attribué qu'à un seul rôle.

Si vous attribuez une plage réseau en tant que client géré dans un rôle, vous ne pouvez pas attribuer les adresses IP individuelles de cette plage à un autre rôle. De plus, vous ne pouvez pas attribuer de façon spécifique un utilisateur, un groupe, un domaine ou une unité d'organisation à deux rôles différents. Vous pouvez cependant attribuer un utilisateur à un rôle, puis attribuer un groupe, un domaine ou une unité d'organisation dont cet utilisateur est membre à un autre rôle.

> **Remarque**
> Si un groupe est un client géré dans un rôle et que l'administrateur de ce rôle applique une stratégie à chaque membre du groupe, les utilisateurs individuels de ce groupe ne peuvent pas ensuite être attribués à un autre rôle.

Lorsque vous ajoutez des clients gérés, tenez compte des types de clients à inclure. Si vous ajoutez des adresses IP à un rôle, ses administrateurs peuvent générer des rapports sur **toute** l'activité des ordinateurs spécifiés. Si vous ajoutez des utilisateurs à un rôle, les administrateurs peuvent générer des rapports sur toute l'activité de ces utilisateurs, quel que soit l'ordinateur sur lequel cette activité est détectée.

Les administrateurs ne sont pas automatiquement inclus en tant que clients gérés dans les rôles qu'ils administrent car cela leur permettrait de définir leur propre stratégie. Pour autoriser des administrateurs à consulter leur propre utilisation d'Internet, activez la fonction de génération de rapports sur leur propre activité (voir *Rapports sur activité propre*, page 339).

Si votre organisation a déployé plusieurs serveurs Policy Server et que ces derniers communiquent avec des annuaires différents, assurez-vous de sélectionner le serveur Policy Server connecté à l'annuaire contenant les clients que vous souhaitez ajouter.

> **Remarque**
> Les meilleures pratiques montrent qu'il est préférable que tous les clients gérés dans le même rôle appartiennent au même service d'annuaire.

1. Sélectionnez des clients pour le rôle :
   - Sous **Annuaire**, cochez la case d'un ou plusieurs utilisateurs.

     Si votre environnement utilise Active Directory (mode natif) ou un autre service d'annuaire de type LDAP, vous pouvez rechercher dans l'annuaire des noms d'utilisateur, de groupe, de domaine ou d'unité d'organisation spécifiques. Voir *Recherche dans le service d'annuaire*, page 69.
   - Sous **Ordinateur**, entrez l'adresse IP d'un ordinateur à ajouter à ce rôle.
   - Sous **Réseau**, entrez la première et la dernière adresse IP d'une plage d'ordinateurs à ajouter en tant qu'unité.
2. Cliquez sur la flèche droite (>) accolée au type de client pour déplacer les clients vers la liste **Sélectionné**.
3. Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier le rôle.
4. Dans la page Modifier le rôle, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Gestion des conflits entre rôles

Rubriques connexes :

- *Utilisation de l'administration déléguée*, page 255
- *Ajout de clients gérés*, page 262

Dans les services d'annuaire, le même utilisateur peut appartenir à plusieurs groupes. Par conséquent, un même utilisateur peut être membre de groupes gérés par des rôles d'administration déléguée différents. Il en est de même pour les domaines et les unités d'organisation.

De plus, un utilisateur peut être géré par un seul rôle et appartenir à un groupe, un domaine ou une unité d'organisation géré(e) par un rôle différent. Si les administrateurs de ces rôles sont connectés simultanément, l'administrateur responsable de l'utilisateur peut lui appliquer une stratégie alors même que l'administrateur responsable du groupe applique une stratégie aux membres individuels du groupe.

La page **Administration déléguée > Gérer la priorité des rôles** permet d'indiquer à Websense le comportement qu'il doit adopter lorsque des stratégies différentes s'appliquent simultanément aux mêmes utilisateurs. En cas de conflit, Websense applique alors la stratégie de filtrage du rôle apparaissant en premier dans cette liste.

1. Sélectionnez un rôle quelconque dans la liste, à l'exception du rôle Super administrateur.

   Remarque
   Le rôle Super administrateur est toujours le premier rôle de cette liste. Il ne peut pas être déplacé.

2. Cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier sa position dans la liste.
3. Répétez les étapes 1 et 2 jusqu'à ce que tous les rôles aient la priorité désirée.
4. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Administration déléguée. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Considérations particulières

Rubriques connexes :

- *Utilisation de l'administration déléguée*, page 255
- *Modification des rôles*, page 257

Avant de supprimer des rôles d'administration déléguée ou des clients gérés dans un rôle, consultez les informations suivantes.

Suppression de rôles

Dans la page **Administration déléguée**, les Super administrateurs inconditionnels peuvent supprimer tous les rôles devenus obsolètes.

La suppression d'un rôle retire également tous les clients que les administrateurs du rôle ont ajoutés à la page Clients. Une fois le rôle supprimé, si ces clients appartiennent à des réseaux, des groupes ou des domaines gérés par d'autres rôles, ils sont gérés par la stratégie appropriée appliquée à ces derniers (voir *Ordre du filtrage*, page 80). Sinon, ils sont gérés par la stratégie Par défaut du Super administrateur.

1. Dans la page **Administration déléguée**, cochez la case accolée à chaque rôle à supprimer.

   Remarque
   Vous ne pouvez pas supprimer le rôle Super administrateur.

2. Cliquez sur **Supprimer**.
3. Confirmez la suppression pour supprimer les rôles sélectionnés de la page Administration déléguée. Les modifications ne sont pas définitives tant que vous ne cliquez pas sur **Enregistrer tout**.

Le rôle supprimé est retiré de la liste déroulante Rôle de la bannière dès votre prochaine connexion à Websense Manager.

Suppression de clients gérés

Les clients ne peuvent pas être supprimés directement de la liste des clients gérés (Administration déléguée > Modifier le rôle) si :

- L'administrateur a appliqué une stratégie au client.
- L'administrateur a appliqué une stratégie à un ou plusieurs membres d'un réseau, d'un groupe, d'un domaine ou d'une unité d'organisation.

Des problèmes peuvent également survenir si, lors de la connexion à Websense Manager, le Super administrateur choisit un autre serveur Policy Server que celui qui communique avec le service d'annuaire contenant les clients à supprimer. Dans ce cas, le serveur Policy Server et le service d'annuaire en cours ne reconnaissent pas les clients.

Un Super administrateur inconditionnel peut vérifier que les clients appropriés peuvent être supprimés, comme suit.

1. Connectez-vous à Websense Manager en sélectionnant le serveur Policy Server dont le service d'annuaire contient les clients gérés à supprimer. Vous devez vous connecter en tant que Super administrateur inconditionnel.
2. Ouvrez la liste **Rôle** dans la bannière et sélectionnez le rôle duquel les clients gérés doivent être retirés.
3. Ouvrez la page **Gestion des stratégies > Clients** pour voir la liste de tous les clients auxquels l'administrateur délégué a explicitement attribué une stratégie.

   Cela peut comprendre les clients spécifiquement identifiés dans la liste des clients gérés du rôle et les clients membres de réseaux, de groupes, de domaines ou d'unités d'organisation présents dans la liste des clients gérés.
4. Supprimez les clients appropriés.
5. Cliquez sur **OK** pour mettre vos modifications en cache.
6. Ouvrez la liste **Rôle** dans la bannière et sélectionnez le rôle **Super administrateur**.
7. Ouvrez la page **Gestion des stratégies > Administration déléguée > Modifier le rôle**.
8. Supprimez les clients appropriés de la liste des clients gérés, puis cliquez sur **OK** pour confirmer l'opération.
9. Dans la page Modifier le rôle, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Accès à Websense Manager par plusieurs administrateurs

Rubriques connexes :

- *Présentation des administrateurs*, page 238
- *Activation de l'accès à Websense Manager*, page 251

Les administrateurs de différents rôles peuvent accéder simultanément à Websense Manager pour exécuter leurs tâches autorisées. Par exemple, les administrateurs du Rôle A et du Rôle B disposant d'autorisations de stratégies peuvent se connecter simultanément à Websense Manager. Comme ils gèrent des clients différents, ils peuvent créer et appliquer des stratégies sans provoquer de conflits.

La situation est différente si les administrateurs qui disposent d'autorisations de stratégie dans le même rôle se connectent en même temps. Pour préserver l'intégrité de la structure et des attributions de stratégies, un seul administrateur d'un rôle peut accéder à Websense Manager avec des autorisations de stratégie à un moment donné. Lorsqu'un second administrateur disposant des mêmes autorisations pour le même rôle tente de se connecter alors que le premier administrateur l'est toujours, le second a plusieurs possibilités :

- Se connecter pour la génération de rapports uniquement, s'il dispose des autorisations appropriées.
- Se connecter à un rôle différent, s'il est attribué à d'autres rôles.
- Se reconnecter ultérieurement, après la déconnexion du premier administrateur.

Lorsque des administrateurs disposant à la fois des autorisations de stratégie et de génération de rapports se connectent pour générer des rapports, ils peuvent libérer immédiatement leurs autorisations de stratégie de sorte que les autres administrateurs du rôle puissent effectuer des activités de gestion des stratégies.

▶ Ouvrez la liste déroulante **Rôle** de la bannière et choisissez **Libérer les autorisations de stratégie**.

Une autre approche consiste à créer un compte utilisateur Websense spécial (voir *Comptes utilisateur Websense*, page 253) pour chaque rôle et à ne donner à cet utilisateur que des autorisations de génération de rapports. Donnez ces identifiants de connexion (nom d'utilisateur et mot de passe) aux administrateurs du rôle qui disposent à la fois d'autorisations de stratégie et de génération de rapports. Lorsque des administrateurs doivent exécuter des rapports, ils peuvent se connecter avec ce compte d'administration de rapports, pendant qu'un autre administrateur peut accéder aux stratégies.

Définition de restrictions de filtrage pour tous les rôles

Rubriques connexes :

- *Présentation des administrateurs*, page 238
- *Création d'un verrouillage du filtre*, page 267

Websense permet aux Super administrateurs inconditionnels de définir un Verrouillage du filtre bloquant certaines catégories et certains protocoles pour tous les clients gérés par les rôles d'administration déléguée. Pour plus d'informations, consultez *Création d'un verrouillage du filtre*, page 267.

Les administrateurs de ces rôles peuvent appliquer toute action de filtrage aux autres catégories et protocoles de leurs stratégies, mais pas aux catégories et aux protocoles bloqués par le Verrouillage du filtre.

Les modifications apportées au Verrouillage du filtre sont implémentées pour tous les clients gérés dès l'enregistrement des modifications. Les administrateurs délégués connectés à Websense Manager lorsque les modifications prennent effet ne voient pas les modifications apportées avant leur prochaine connexion.

Remarque

Lorsqu'un filtre est copié du rôle Super administrateur vers un autre rôle, la copie est soumise aux contraintes du Verrouillage du filtre.

Les Super administrateurs ne sont pas limités par le Verrouillage du filtre. Ils peuvent définir des stratégies autorisant l'accès aux catégories et aux protocoles bloqués et verrouillés pour les rôles d'administration déléguée. Les utilisateurs qui doivent disposer de droits d'accès particuliers doivent donc être gérés par le rôle Super administrateur.

Création d'un verrouillage du filtre

Rubriques connexes :

- *Définition de restrictions de filtrage pour tous les rôles*, page 267
- *Verrouillage de catégories*, page 268
- *Verrouillage de protocoles*, page 269

La page **Gestion des stratégies > Verrouillage du filtre** vous permet de modifier les catégories ou les protocoles devant être bloqués pour tous les clients gérés dans les rôles d'administration déléguée. Toute fonction de catégorie ou de protocole bloquée dans le Verrouillage du filtre est considérée comme **bloquée et verrouillée**.

- Cliquez sur le bouton **Catégories** pour bloquer et verrouiller des catégories ou des éléments de catégorie spécifiques (mots-clés et types de fichiers). Voir *Verrouillage de catégories*, page 268.
- Cliquez sur le bouton **Protocoles** pour bloquer et verrouiller des protocoles, ou la journalisation des protocoles. Voir *Verrouillage de protocoles*, page 269.

Verrouillage de catégories

Rubriques connexes :

- *Définition de restrictions de filtrage pour tous les rôles*, page 267
- *Création d'un verrouillage du filtre*, page 267
- *Verrouillage de protocoles*, page 269

La page **Gestion des stratégies > Verrouillage du filtre > Catégories** permet de sélectionner des catégories à bloquer et à verrouiller pour tous les membres des rôles d'administration déléguée. Vous pouvez également bloquer et verrouiller des mots-clés et des types de fichiers pour une catégorie.

1. Sélectionnez une catégorie dans l'arborescence.

   Les rôles d'administration déléguée n'ont pas accès aux catégories personnalisées créées par les Super administrateurs. Les catégories personnalisées n'apparaissent donc pas dans cette arborescence.

2. Définissez les restrictions de cette catégorie dans le champ qui apparaît à côté de l'arborescence des catégories.

Option	Description
Verrouiller la catégorie	Bloque et verrouille l'accès aux sites de cette catégorie.
Verrouiller des mots-clés	Bloque et verrouille l'accès en fonction des mots-clés définis pour cette catégorie dans chaque rôle.
Verrouiller des types de fichiers	Bloque et verrouille les types de fichiers sélectionnés pour les sites de cette catégorie. Assurez-vous de cocher la case de chaque type de fichier à bloquer et à verrouiller. Les types de fichiers personnalisés créés par le Super administrateur sont inclus dans cette liste car ils sont disponibles pour les rôles d'administration déléguée.
Appliquer aux sous-catégories	Applique les mêmes paramètres à toutes les sous-catégories de cette catégorie.

Au besoin, vous pouvez bloquer et verrouiller des éléments sélectionnés pour toutes les catégories en même temps. Sélectionnez **Toutes les catégories** dans l'arborescence, puis les éléments à bloquer pour toutes les catégories. Cliquez ensuite sur **Appliquer aux sous-catégories**.

3. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Verrouillage du filtre. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Verrouillage de protocoles

Rubriques connexes :

- *Définition de restrictions de filtrage pour tous les rôles*, page 267
- *Création d'un verrouillage du filtre*, page 267
- *Verrouillage de catégories*, page 268

La page **Gestion des stratégies > Verrouillage du filtre > Protocoles** permet de bloquer et de verrouiller l'accès ou de verrouiller la journalisation des protocoles sélectionnés pour tous les clients gérés par les rôles d'administration déléguée.

> **Remarque**
> La journalisation des protocoles est associée aux alertes d'utilisation des protocoles. Vous ne pouvez pas générer d'alertes d'utilisation d'un protocole si ce dernier n'est pas défini pour la journalisation dans au moins un filtre de protocole. L'activation de l'option **Verrouiller la journalisation du protocole** via le verrouillage du filtre permet de s'assurer que des alertes d'utilisation pourront être générées pour le protocole. Voir *Configuration des alertes d'utilisation de protocole*, page 292.

1. Sélectionnez un protocole dans l'arborescence.

   Les rôles d'administration déléguée ont accès aux protocoles personnalisés créés par le Super administrateur. Les protocoles personnalisés apparaissent donc dans cette arborescence.

2. Définissez les restrictions de ce protocole dans le champ qui apparaît à côté de l'arborescence des protocoles.

Option	Description
Verrouiller le protocole	Bloque et verrouille l'accès aux applications et aux sites Web qui utilisent ce protocole.
Verrouiller la journalisation du protocole	Journalise les informations liées à l'accès à ce protocole et empêche les administrateurs délégués de désactiver la journalisation.
Appliquer au groupe	Applique les mêmes paramètres à tous les protocoles du groupe.

3. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Verrouillage du filtre. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

12 Administration du serveur Websense

Rubriques connexes :

- *Composants de Websense*, page 272
- *Fonctionnement de Policy Server*, page 277
- *Affichage et exportation du journal d'audit*, page 284
- *Arrêt et démarrage des services Websense*, page 286
- *Alertes*, page 287
- *Sauvegarde et restauration des données Websense*, page 295

Le filtrage de l'utilisation Internet requiert une interaction entre plusieurs composants de Websense :

- Les demandes d'accès à Internet des utilisateurs sont reçues par Network Agent ou un produit d'intégration tiers.
- Les requêtes sont envoyées à Websense Filtering Service pour être traitées.
- Filtering Service communique avec le serveur Policy Server et Policy Broker pour appliquer la stratégie appropriée en réponse à la requête.

Dans la plupart des environnements, une même base de données de stratégies gère les informations des clients, des filtres, des stratégies et de la configuration générale, qu'il existe un ou plusieurs serveurs Policy Server.

Chaque instance de Websense Manager est associée à une unique base de données de stratégies et peut être utilisée pour configurer chaque serveur Policy Server associé à cette base de données.

La configuration des stratégies effectuée dans Websense Manager étant stockée dans la base de données centrale, les informations de stratégies sont automatiquement accessibles à tous les serveurs Policy Server associés à cette base de données de stratégies.

Composants de Websense

Rubriques connexes :

- *Composants du filtrage*, page 273
- *Composants de la génération de rapports*, page 275
- *Composants de l'identification des utilisateurs*, page 276
- *Fonctionnement de Policy Server*, page 277
- *Arrêt et démarrage des services Websense*, page 286
- *Vérification de l'état du système en cours*, page 294

Websense est constitué de plusieurs composants qui travaillent ensemble pour assurer l'identification des utilisateurs, le filtrage Internet et la génération des rapports. Pour vous aider à mieux comprendre et à mieux gérer votre environnement de filtrage, cette section présente chaque composant.

Les principaux composants de Websense comprennent :

- Base de données de stratégies (Policy Database)
- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- Base de données principale
- Websense Manager
- Usage Monitor
- User Service
- Log Server
- Base de données d'activité (Log Database)

Websense comprend également des agents d'identification transparente facultatifs :

- DC Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent

D'autres composants facultatifs comprennent :

- Serveur Remote Filtering
- Client Remote Filtering
- Websense Content Gateway

Composants du filtrage

Composant	Description
Base de données de stratégies	Stocke les paramètres et les informations des stratégies de Websense.
Policy Broker	Gère les requêtes provenant des composants de Websense pour les informations de stratégies et de configuration générale.
Policy Server	• Identifie et surveille l'emplacement et l'état des autres composants de Websense. • Stocke les informations de configuration spécifiques à une seule instance Policy Server. • Communique les données de configuration au service Filtering Service, qui filtre les requêtes Internet. Configurez les paramètres du serveur Policy Server dans Websense Manager (voir *Fonctionnement de Policy Server*, page 277). Les paramètres des stratégies et la plupart des paramètres de configuration sont partagés entre les serveurs Policy Server qui partagent une même base de données de stratégies (voir *Fonctionnement d'un environnement contenant plusieurs serveurs Policy Server*, page 279).
Filtering Service	Assure le filtrage Internet avec Network Agent ou un produit d'intégration tiers. Lorsqu'un utilisateur demande un site, Filtering Service reçoit la requête et détermine la stratégie à appliquer. • Filtering Service doit s'exécuter pour que les requêtes Internet soient filtrées et journalisées. • Chaque instance de Filtering Service télécharge sa propre copie de la base de données principale Websense. Configurez le filtrage et le comportement de Filtering Service dans Websense Manager (voir *Filtres d'utilisation Internet*, page 37 et *Configuration des paramètres de filtrage de Websense*, page 56).
Network Agent	• Étend les fonctions de filtrage et de journalisation • Autorise la gestion des protocoles • Autorise le filtrage dans un environnement autonome Pour plus d'informations, consultez *Configuration du réseau*, page 343.

Composant	Description
Base de données principale	• Comprend plus de 36 millions de sites Web, classés en plus de 90 catégories et sous-catégories • Contient plus de 100 définitions de protocole à utiliser dans le filtrage de protocoles Téléchargez la base de données principale Websense pour activer le filtrage Internet et veillez à ce que cette base de données reste à jour. Si la Base de données principale date de plus de 2 jours, aucun filtrage n'est effectué. Pour plus d'informations, consultez *Base de données principale Websense*, page 32.
Websense Manager	Sert d'interface de gestion et de configuration de Websense. Websense Manager permet de définir et de personnaliser les stratégies d'accès à Internet, d'ajouter ou de supprimer des clients, de configurer les composants de Websense, etc. Pour plus d'informations, consultez *Utilisation de Websense Manager*, page 17.
Usage Monitor	Autorise les alertes basées sur l'utilisation d'Internet. Usage Monitor surveille les accès aux catégories d'URL et aux protocoles et génère des messages d'alerte en fonction du comportement d'alerte configuré. Pour plus d'informations, consultez *Alertes*, page 287.
Client Remote Filtering	• Réside sur les ordinateurs client situés hors du pare-feu réseau. • Identifie les ordinateurs en tant que clients à filtrer et communique avec le serveur Remote Filtering. Pour plus d'informations, consultez *Filtrage des clients distants*, page 157.
Serveur Remote Filtering	• Autorise le filtrage des clients situés hors d'un pare-feu réseau. • Communique avec Filtering Service pour assurer la gestion des accès Internet des ordinateurs distants. Pour plus d'informations, consultez *Filtrage des clients distants*, page 157.

Composant	Description
Websense Content Gateway	• Fournit un proxy et une plate-forme de mise en cache robustes. • Peut analyser le contenu des sites Web et des fichiers en temps réel pour catégoriser les sites précédemment non catégorisés. Voir *Analyse du contenu avec les options en temps réel*, page 145.
Websense Security Gateway	En plus de la fonction Websense Content Gateway standard : • Analyse le code HTML pour rechercher des risques pour la sécurité (par exemple, le phishing, la redirection d'URL, les exploits Web et l'antiblocage par proxy). • Analyse le contenu des fichiers pour attribuer une catégorie de menaces (par exemple virus, Chevaux de Troie ou vers). • Découpe le contenu actif de certaines pages Web. Voir *Analyse du contenu avec les options en temps réel*, page 145.

Composants de la génération de rapports

Composant	Description
Log Server	Journalise les données des requêtes Internet, dont : • La source de la requête • La catégorie ou le protocole associé à la requête • Si la requête a été autorisée ou bloquée • Si le blocage par mot-clé, le blocage de type de fichiers, l'attribution de temps contingenté, des niveaux de bande passante ou la protection par mot de passe ont été appliqués. Avec Network Agent et certains produits d'intégration, Log Server stocke également des informations sur la quantité de bande passante utilisée. Log Server doit être installé sur un ordinateur Windows pour autoriser les rapports d'investigation et de présentation et les graphiques des pages Aujourd'hui et Historique dans Websense Manager. Après l'installation de Log Server, configurez Filtering Service pour transmettre les données de journalisation à l'emplacement approprié (voir *Configuration de Filtering Service pour la journalisation*, page 308).
Base de données d'activité	Stocke les données des requêtes Internet collectées par Log Server en vue de leur utilisation dans les outils de génération de rapports de Websense.

Composants de l'identification des utilisateurs

Composant	Description
User Service	• Communique avec votre service d'annuaire. • Transmet les informations liées aux utilisateurs, y compris les relations utilisateur/groupe et utilisateur/domaine, à Policy Server et Filtering Service en vue de leur application dans les stratégies de filtrage. Si vous avez installé et configuré un agent d'identification transparente Websense (voir *Identification transparente*, page 201), User Service simplifie l'interprétation des informations relatives à l'ouverture de session des utilisateurs, et utilise ces informations pour fournir des associations nom d'utilisateur/adresse IP à Filtering Service. Lorsque vous ajoutez des utilisateurs et des groupes en tant que clients Websense (voir *Ajout d'un client*, page 68), User Service fournit à Websense Manager les informations de nom et de chemin provenant du service d'annuaire. Pour plus d'informations sur la configuration des accès aux services d'annuaire, consultez la section *Services d'annuaire*, page 63.
DC Agent	• Autorise l'identification transparente des utilisateurs dans un service d'annuaire basé sur Windows. • Communique avec User Service pour fournir à Websense des informations actualisées sur l'ouverture de session des utilisateurs à employer lors du filtrage. Pour plus d'informations, consultez *DC Agent*, page 213.
Logon Agent	• Assure une identification transparente des utilisateurs sans précédent dans les réseaux Linux et Windows. • Ne s'appuie pas sur un service d'annuaire ou sur un autre intermédiaire pour la capture des sessions de connexion des utilisateurs. • Détecte les sessions de connexion des utilisateurs dès qu'elles se produisent. Logon Agent communique avec l'application de connexion des ordinateurs client pour faire en sorte que les sessions de connexion des utilisateurs individuelles soient capturées et traitées directement par Websense. Pour plus d'informations, consultez *Logon Agent*, page 216.

Composant	Description
eDirectory Agent	• Fonctionne avec Novell eDirectory pour identifier les utilisateurs de façon transparente. • Collecte les informations des sessions de connexion des utilisateurs auprès de Novell eDirectory, qui authentifie les utilisateurs qui se connectent au réseau. • Associe chaque utilisateur authentifié à une adresse IP, puis travaille avec User Service pour fournir les informations à Filtering Service. Pour plus d'informations, consultez *eDirectory Agent*, page 224.
RADIUS Agent	Autorise l'identification transparente des utilisateurs qui accèdent au réseau par une connexion distante, un VPN (Virtual Private Network), une ligne ADSL ou une autre connexion à distance. Pour plus d'informations, consultez *RADIUS Agent*, page 219.

Fonctionnement de la base de données de stratégies

La Base de données de stratégies Websense stocke les données des stratégies (y compris les paramètres des clients, des filtres, des composants de filtre et de l'administration déléguée) et les paramètres de configuration globaux dans Websense Manager. Les paramètres spécifiques à une instance de Policy Server sont stockés séparément.

Dans la plupart des environnements Policy Server, une même base de données de stratégies gère les données de stratégies et de configuration générale pour plusieurs serveurs Policy Server.

1. Au démarrage, chaque composant Websense demande les informations de configuration applicables dans la base de données de stratégies via Policy Broker.
2. Les composants qui s'exécutent vérifient fréquemment la présence de modifications dans la base de données de stratégies.
3. La base de données de stratégies est mise à jour chaque fois que des administrateurs apportent des modifications dans Websense Manager et cliquent sur Enregistrer tout.
4. Lorsque la base de données de stratégies a été modifiée, chaque composant demande et reçoit les modifications affectant son fonctionnement.

Sauvegardez régulièrement la base de données de stratégies pour protéger les informations de stratégie et de configuration importantes. Pour plus d'informations, consultez *Sauvegarde et restauration des données Websense*, page 295.

Fonctionnement de Policy Server

Policy Server est le composant de Websense qui gère les informations de stratégie et communique avec Filtering Service pour l'application des stratégies. Policy Server

identifie également les autres composants de Websense et surveille leur emplacement et leur état.

Lorsque vous vous connectez à Websense Manager, vous êtes connecté(e) à l'interface graphique de Policy Server.

- Vous ne pouvez pas vous connecter à Websense Manager s'il n'est pas configuré pour communiquer avec Policy Server.
- Si votre installation Websense comprend plusieurs serveurs Policy Server, vous avez le choix entre plusieurs instances de Policy Server au moment de la connexion.
- Vous pouvez ajouter ou supprimer des instances de Policy Server dans Websense Manager.

Par défaut, la communication entre Websense Manager et une instance centrale de Policy Server est établie lors de l'installation de Websense Manager.

La plupart des environnements ne requièrent qu'un seul serveur Policy Server. Un même serveur Policy Server peut communiquer avec plusieurs instances de Filtering Service et Network Agent pour l'équilibrage de la charge. Toutefois, dans les très grandes organisations (plus de 10 000 utilisateurs), l'installation de plusieurs instances de Policy Server peut s'avérer judicieuse. Si vous installez d'autres serveurs Policy Server, ajoutez chaque instance dans Websense Manager (voir *Ajout et modification des instances de Policy Server*, page 278).

Ajout et modification des instances de Policy Server

La page **Paramètres > Policy Server** permet d'ajouter des instances de Policy Server dans Websense Manager, ou de configurer ou de supprimer des serveurs Policy Server existants.

Pour ajouter une instance de Policy Server :

1. Cliquez sur **Ajouter**. La page Ajouter un serveur Policy Server s'ouvre.
2. Entrez l'adresse IP ou le nom d'hôte de l'ordinateur Policy Server dans le champ **IP ou nom du serveur**.
3. Entrez le numéro de **Port** que Websense Manager doit utiliser pour communiquer avec cette instance de Policy Server. La valeur par défaut est **55806**.
4. Cliquez sur **OK** pour revenir à la page Policy Server. La nouvelle instance de Policy Server apparaît dans la liste.
5. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Policy Server. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Pour modifier une instance de Policy Server (par exemple, si le nom ou l'adresse IP de l'ordinateur Policy Server change), sélectionnez une adresse IP ou un nom d'hôte dans la liste Policy Server et cliquez sur le lien correspondant.

Pour supprimer une instance de Policy Server, sélectionnez une adresse IP ou un nom d'hôte dans la liste Policy Server, puis cliquez sur **Supprimer**. Le fait de cliquer sur

Supprimer retire l'instance de Policy Server dans Websense Manager, mais ne désinstalle pas, ni n'arrête le service Websense Policy Server. Si la liste ne contient qu'une seule instance de Policy Server, vous ne pouvez pas la supprimer.

Fonctionnement d'un environnement contenant plusieurs serveurs Policy Server

Dans certains environnements distribués, comportant un grand nombre d'utilisateurs, il peut s'avérer judicieux d'installer plusieurs serveurs Policy Server. Ce choix impose toutefois de tenir compte de plusieurs éléments.

- Si vous implémentez une configuration qui autorise la gestion du même client par plusieurs serveurs Policy Server, selon la charge actuelle, n'implémentez **pas** d'actions de stratégie dépendant du temps :
  - Accès par mot de passe
  - Confirmer
  - Contingent

  Les informations de temps associées à ces fonctions ne sont pas partagées entre les serveurs Policy Server, et les clients pourraient se voir accorder plus ou moins d'accès Internet que prévu.

  N'oubliez pas que la stratégie Par défaut s'applique lorsque aucune autre stratégie n'est appliquée à un client. Si des clients peuvent être gérés par plusieurs serveurs Policy Server, vérifiez que la stratégie par défaut n'impose pas de filtres de catégories appliquant des actions dépendant du temps.
- Les informations de stratégie étant stockées dans la base de données de stratégies, leurs modifications sont automatiquement partagées par tous les serveurs Policy Server lorsque vous cliquez sur **Enregistrer tout**.
- La plupart des paramètres de configuration globaux (tels que les définitions de classe de risque et les options d'alerte) sont également partagés par les serveurs Policy Server.
- Les paramètres de configuration propres à un seul serveur Policy Server (tels que ses connexions à Filtering Service et à Network Agent) sont stockés localement par chaque serveur Policy Server et ne sont pas distribués.

Pour basculer entre plusieurs serveurs Policy Server dans Websense Manager afin de revoir ou de configurer les paramètres s'appliquant à une instance de Policy Server :

1. Dans la bannière Websense, développez la liste **Policy Server** et sélectionnez une adresse IP.
2. Si des modifications apportées à l'instance en cours de Policy Server n'ont pas été enregistrées, la liste des modifications s'affiche. Procédez de l'une des manières suivantes :
   - Cliquez sur **Annuler** pour rester connecté(e) à l'instance de Policy Server en cours pour pouvoir enregistrer les modifications.
   - Cliquez sur **Ok** pour annuler les modifications et vous connecter à une nouvelle instance de Policy Server.

- Cliquez sur **Retour** pour continuer à configurer l'instance de Policy Server en cours.

S'il n'y a pas de modifications non enregistrées, vous revenez automatiquement à l'écran de connexion.

3. Dans l'écran de connexion, entrez un nom d'utilisateur et un mot de passe vous permettant de vous connecter à l'instance de Policy Server sélectionnée, puis cliquez sur **Se connecter**.

Modification de l'adresse IP de Policy Server

Avant de modifier l'adresse IP de l'ordinateur Policy Server, **arrêtez tous les services Websense** s'exécutant sur l'ordinateur. Si Websense Manager est également installé sur l'ordinateur, cela comprend également les services Apache2Websense et ApacheTomcatWebsense.

Après avoir modifié l'adresse IP, vous devez mettre à jour manuellement les fichiers de configuration de Websense utilisés par Websense Manager, Policy Server et les autres services de Websense pour que le filtrage puisse reprendre.

Étape 1 : Mise à jour de la configuration de Websense Manager

Mettez à jour Websense Manager pour qu'il utilise la nouvelle adresse IP pour se connecter à Policy Server.

1. Sur l'ordinateur Websense Manager, arrêtez les services **Apache2Websense** et **ApacheTomcatWebsense** (si nécessaire).

   Si Websense Manager et Policy Server sont installés sur ce même ordinateur, les services Apache devraient déjà être arrêtés.
2. Naviguez jusqu'au répertoire suivant :
   - Windows :

     `C:\Program Files\Websense\tomcat\conf\Catalina\localhost\`
   - Linux :

     `/opt/Websense/tomcat/conf/Catalina/localhost/`
3. Localisez le fichier **mng.xml** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
4. Ouvrez le fichier **mng.xml** dans un éditeur de texte (tel que Notepad ou vi) et remplacez chaque instance de l'ancienne adresse IP de Policy Server par la nouvelle.

   L'adresse IP de Policy Server apparaît deux fois : dans la valeur **ps/default/host** et dans la valeur **psHosts**.
5. Lorsque vous avez terminé, enregistrez et fermez le fichier.

Ne redémarrez pas les services Apache avant d'avoir terminé les mises à jour restantes de la configuration dans cette section.

Étape 2 : Mise à jour de la configuration de Policy Server

Mettez à jour le fichier de configuration de Policy Server et le fichier d'initialisation utilisé pour configurer la communication entre les composants de Websense.

1. Si vous ne l'avez pas déjà fait, arrêtez tous les services Websense sur l'ordinateur Policy Server (voir *Arrêt et démarrage des services Websense*, page 286).
2. Naviguez jusqu'au répertoire **bin** de Websense.
   - Windows :

     ```
     C:\Program Files\Websense\bin
     ```

   - Linux

     ```
     /opt/Websense/bin
     ```

3. Localisez le fichier **config.xml** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
4. Ouvrez le fichier **config.xml** dans un éditeur de texte et remplacez chaque instance de l'ancienne adresse IP de Policy Server par la nouvelle.
5. Lorsque vous avez terminé, enregistrez et fermez le fichier.
6. Dans le répertoire **bin**, localisez le fichier **websense.ini** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
7. Ouvrez le fichier **websense.xml** dans un éditeur de texte et remplacez chaque instance de l'ancienne adresse IP de Policy Server par la nouvelle.
8. Lorsque vous avez terminé, enregistrez et fermez le fichier.

Étape 3 : Vérification de la connexion à la base de données d'activité

Sur l'ordinateur Policy Server, utilisez l'Administrateur de la source de données ODBC de Windows pour vérifier la connexion ODBC à la base de données d'activité.

1. Sélectionnez **Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Sources de données (ODBC)**.
2. Dans l'onglet **Système DSN**, sélectionnez le nom de la source de données appropriée (par défaut, **wslogdb70**), puis cliquez sur **Configurer**.
3. Vérifiez que le serveur de base de données approprié est sélectionné, puis cliquez sur **Suivant**.
4. Vérifiez les identifiants utilisés pour la connexion à la base de données, puis cliquez sur **Suivant**.
5. Acceptez les paramètres par défaut des deux écrans suivants, puis cliquez sur **Tester la source de données**.

Remarque

Si le test échoue, vérifiez le nom du serveur de base de données et réessayez.

Si le test échoue encore alors que le nom de l'ordinateur est correct, vérifiez que le port de connexion utilisé est correct et que le pare-feu autorise les communications sur le port sélectionné.

Étape 4 : Redémarrage des services Websense

1. Redémarrez l'ordinateur Policy Server. Vérifiez que tous les services Websense de l'ordinateur redémarrent normalement.
2. Si l'instance Websense Manager utilisée pour configurer ce serveur Policy Server est installée sur un autre ordinateur, redémarrez les services **Apache2Websense** et **ApacheTomcatWebsense** sur cet ordinateur.

> **Remarque**
> Si Websense Manager est installé sur le même ordinateur que Policy Server, les administrateurs doivent utiliser la nouvelle adresse IP pour se connecter.

Fonctionnement de Filtering Service

Filtering Service est le composant de Websense qui fonctionne avec Network Agent ou un produit d'intégration tiers pour filtrer l'activité Internet. Lorsqu'un utilisateur demande un site, Filtering Service reçoit la requête, détermine la stratégie à appliquer et utilise la stratégie applicable pour déterminer comment le site est filtré.

Chaque instance de Filtering Service télécharge sa propre copie de la base de données principale Websense qu'il utilise pour déterminer comment filtrer les requêtes Internet.

Filtering Service transmet également les informations relatives à l'activité Internet à Log Server, de sorte qu'elles puissent être enregistrées et utilisées dans les rapports.

Lorsque vous vous connectez à Websense Manager, le **Résumé du Filtering Service** de la page État > Aujourd'hui présente l'adresse IP et l'état en cours de chaque instance de Filtering Service associée au serveur Policy Server actif. Cliquez sur l'adresse IP d'un service Filtering Service pour obtenir plus d'informations sur l'instance sélectionnée.

Vérification des détails du service Filtering Service

La page **État > Aujourd'hui > Détails sur Filtering Service** permet de vérifier l'état d'une instance de Filtering Service.

Cette page indique :

- L'adresse IP du service Filtering Service
- Si l'instance sélectionnée s'exécute ou non
- La version de Filtering Service

  Cette version doit correspondre à votre version de Websense, y compris aux correctifs appliqués.
- Le système d'exploitation s'exécutant sur l'ordinateur Filtering Service
- La plate-forme Websense

  Cette information indique si Websense s'exécute en mode autonome ou est intégré à un produit tiers.

- L'adresse IP et l'état des instances de Network Agent avec lesquels le service Filtering Service sélectionné communique.

Cliquez sur **Fermer** pour revenir à la page Aujourd'hui.

Vérification de l'état du téléchargement de la base de données principale

Chaque instance de Filtering Service de votre réseau télécharge sa propre copie de la base de données principale. Lorsque vous travaillez dans Websense Manager, le Résumé sur les alertes de santé de la page État > Aujourd'hui présente un message d'état lorsqu'un téléchargement de la base de données principale est en cours ou si une tentative de téléchargement échoue.

Pour plus d'informations sur les téléchargements récents ou en cours de la base de données, cliquez sur **Téléchargement de la base de données** dans la barre d'outils de la page Aujourd'hui. La page Téléchargement de la base de données comprend une entrée pour chaque instance de Filtering Service associée au serveur Policy Server actif.

Au départ, la page Téléchargement de la base de données présente un bref résumé du téléchargement, indiquant l'emplacement et la version de la base de données téléchargée et si le téléchargement a réussi. À partir de cette vue de résumé, vous pouvez :

- Démarrer un téléchargement de base de données pour un service Filtering Service (cliquez sur **Mettre à jour**).
- Démarrer des téléchargements de base de données pour toutes les instances de Filtering Service de la liste (cliquez sur **Tout mettre à jour**).
- Annuler une ou toutes les mises à jour en cours.

Cliquez sur une adresse IP dans la liste située à droite pour obtenir un état plus détaillé du téléchargement de la base de données pour l'instance de Filtering Service sélectionnée.

- Si des problèmes de téléchargement sont survenus pour l'instance de Filtering Service sélectionnée, des conseils permettant de résoudre le problème peuvent s'afficher.
- Pour démarrer manuellement un téléchargement de base de données pour l'instance de Filtering Service sélectionnée, cliquez sur **Mettre à jour**.

Pendant le téléchargement de la base de données, l'écran d'état présente des informations détaillées sur la progression de chaque étape du téléchargement. Cliquez sur **Fermer** pour masquer les informations de progression et continuer à travailler dans Websense Manager.

Reprise des téléchargements de la base de données principale

Lorsqu'un téléchargement de la base de données principale est interrompu, Websense tente automatiquement de reprendre le téléchargement. Si Filtering Service peut se reconnecter au serveur de téléchargement, le téléchargement reprend là où il s'était arrêté.

Vous pouvez redémarrer manuellement un téléchargement interrompu ou qui a échoué. Dans ce cas, le téléchargement ne reprend pas au point d'interruption mais recommence au début.

1. Dans Websense Manager, sélectionnez **État > Aujourd'hui**, puis cliquez sur **Téléchargement de la base de données**.
2. Cliquez sur **Arrêter toutes les mises à jour** pour arrêter le processus interrompu.
3. Sélectionnez une instance de Filtering Service et cliquez sur **Mettre à jour**, ou sur **Tout mettre à jour**, pour redémarrer le processus de téléchargement du début.

Affichage et exportation du journal d'audit

Websense fournit un suivi d'audit qui montre comment les administrateurs ont accédé à Websense Manager et les modifications qu'ils ont pu apporter aux stratégies et aux paramètres. Ces informations ne sont disponibles que pour les Super administrateurs qui disposent d'autorisations de stratégie (voir *Super administrateurs*, page 239).

Les administrateurs délégués exercent un contrôle important sur les activités Internet de leurs clients gérés. La surveillance de leurs modifications via le journal d'audit vous permet de vérifier que ce contrôle est exercé de façon responsable et selon les stratégies d'utilisation acceptées par l'organisation.

Utilisez la page **État > Journal d'audit** pour afficher le journal d'audit et, le cas échéant, pour exporter les parties sélectionnées dans le journal dans une feuille de calcul Excel (XLS).

Les enregistrements d'audit sont conservés pendant 60 jours. Pour les conserver plus longtemps, servez-vous de l'option d'exportation pour exporter le journal régulièrement. Le processus d'exportation ne supprime pas les enregistrements du journal d'audit.

Lorsque la page Journal d'audit s'affiche, les enregistrements les plus récents apparaissent. Servez-vous de la barre de défilement et des boutons de pagination situés au-dessus du journal pour consulter les enregistrements plus anciens.

Le journal présente les informations suivantes. Si un élément est tronqué, cliquez sur l'entrée partielle pour afficher l'intégralité de l'enregistrement dans une fenêtre contextuelle.

Colonne	Description
Date	Date et heure de la modification, ajustées en fonction du fuseau horaire. Pour assurer la cohérence des données du journal d'audit, assurez-vous que tous les ordinateurs qui exécutent Websense présentent les mêmes paramètres de date et heure.
Utilisateur	Nom d'utilisateur de l'administrateur qui a effectué la modification.

Colonne	Description
Serveur	Adresse IP ou nom de l'ordinateur exécutant le serveur Policy Server affecté par la modification. N'apparaît que pour les modifications qui affectent Policy Server, par exemple les modifications apportées dans l'onglet Paramètres.
Rôle	Rôle d'administration déléguée affecté par la modification. Lorsqu'une modification affecte un client explicitement attribué en tant que client géré d'un rôle d'administration déléguée, cette modification apparaît comme affectant le rôle Super administrateur. Si la modification affecte un client membre d'une plage réseau, d'un groupe, d'un domaine ou d'une unité d'organisation attribué(e) au rôle, elle apparaît comme affectant le rôle d'administration déléguée.
Type	Élément de configuration modifié, tel qu'une stratégie, un filtre de catégories ou connexion/déconnexion.
Élément	Identificateur de l'objet spécifique modifié, tel que le nom du filtre de catégories ou du rôle.
Action	Type de modification apporté, par exemple ajout, suppression, modification, connexion, etc.
Précédent	Valeur d'origine, avant la modification.
Actuel	Nouvelle valeur, après la modification.

Tous les éléments n'apparaissent pas pour tous les enregistrements. Par exemple, le rôle n'apparaît pas pour les enregistrements de connexion et de déconnexion.

Pour exporter les enregistrements du journal d'audit :

1. Sélectionnez une période dans la liste **Plage d'export**.

   Choisissez **60 derniers jours** pour exporter le fichier du journal d'audit complet.
2. Cliquez sur **Aller**.

   Si Microsoft Excel est installé sur l'ordinateur qui exécute Websense Manager, le fichier exporté s'ouvre. Pour enregistrer ou imprimer le fichier, utilisez les options d'Excel.

   Si Microsoft Excel n'est pas installé sur l'ordinateur qui exécute Websense Manager, suivez les instructions qui s'affichent à l'écran pour localiser le logiciel ou enregistrer le fichier.

Arrêt et démarrage des services Websense

Les services Websense sont configurés pour démarrer à chaque redémarrage de l'ordinateur. Toutefois, il vous faudra dans certains cas arrêter ou démarrer un ou plusieurs composants du produit indépendamment de l'ordinateur.

> **Remarque**
> Si le service Filtering Service est en train de télécharger la base de données principale, il ne s'arrête pas avant la fin du téléchargement.

Lorsque vous arrêtez tous les services Websense, terminez toujours par les suivants, dans l'ordre :

1. Websense Policy Server
2. Websense Policy Broker
3. Base de données de stratégies Websense

Notez qu'à moins que le problème affecte spécifiquement Policy Broker ou la base de données de stratégies, il est rarement nécessaire de redémarrer ces services. Dans la mesure du possible, évitez de les redémarrer.

Lorsque vous démarrez tous les services Websense, commencez toujours par les suivants, dans l'ordre :

1. Base de données de stratégies Websense
2. Websense Policy Broker
3. Websense Policy Server

Windows

1. Ouvrez la boîte de dialogue Services de Windows (**Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services**).
2. Cliquez du bouton droit sur le nom du service Websense, puis choisissez **Arrêter** ou **Démarrer**.

Linux

Sur les ordinateurs Linux, tous les services s'arrêtent et redémarrent simultanément lorsque vous utilisez cette procédure.

1. Naviguez jusqu'au répertoire **/opt/Websense**.
2. Vérifiez l'état des services Websense avec la commande :
   - `./WebsenseAdmin status`
3. Arrêtez, démarrez ou redémarrez tous les services Websense avec les commandes :
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`

- `./WebsenseAdmin restart`

Avertissement

N'utilisez pas la commande **kill** pour arrêter un service Websense car cela pourrait le corrompre.

Alertes

Rubriques connexes :

- *Contrôle des flux*, page 288
- *Configuration des options d'alerte générales*, page 288
- *Configuration des alertes système*, page 290
- *Configuration des alertes d'utilisation de catégories*, page 291
- *Configuration des alertes d'utilisation de protocole*, page 292

Pour simplifier le suivi et la gestion de Websense et de l'activité Internet des clients, les Super administrateurs peuvent configurer des alertes à envoyer lorsque les éléments sélectionnés se produisent.

- **Alertes système** : notification quel que soit l'état de l'abonnement et l'activité de la base de données principale.
- **Alertes d'utilisation** : notification lorsque l'activité Internet liée à des catégories ou des protocoles particuliers atteint les seuils configurés.

Les alertes peuvent être envoyées aux destinataires sélectionnés par e-mail, sous forme de messages contextuels s'affichant à l'écran (messagerie **réseau** de Windows) ou sous forme de messages SNMP.

Remarque

Les alertes contextuelles s'affichant à l'écran ne peuvent pas être envoyées à des ordinateurs Linux. Elle peuvent cependant être envoyées à partir d'un ordinateur Linux exécutant Policy Server vers des ordinateurs Windows, pour autant que le client Samba soit installé sur l'ordinateur Linux. Voir le *Guide de déploiement*.

Les alertes d'utilisation peuvent être générées pour des catégories ou des protocoles définis par Websense et personnalisés.

Contrôle des flux

Rubriques connexes :

- *Alertes*, page 287
- *Configuration des options d'alerte générales*, page 288
- *Configuration des alertes d'utilisation de catégories*, page 291
- *Configuration des alertes d'utilisation de protocole*, page 292

Des contrôles intégrés liés aux alertes d'utilisation permettent d'éviter de générer un nombre excessif de messages d'alerte. Le paramètre **Maximum d'alertes par jour et par type d'utilisation** permet de spécifier une limite du nombre d'alertes envoyées en réponse aux requêtes des utilisateurs pour des catégories et des protocoles particuliers. Pour plus d'informations, consultez *Configuration des options d'alerte générales*, page 288.

Vous pouvez également définir des seuils pour chaque alerte d'utilisation de catégorie et de protocole. Par exemple, si vous définissez un seuil de 10 pour une certaine catégorie, une alerte est générée après 10 requêtes pour cette catégorie (pour toutes les combinaisons de clients). Pour plus d'informations, consultez *Configuration des alertes d'utilisation de catégories*, page 291 et *Configuration des alertes d'utilisation de protocole*, page 292.

Supposons que le maximum d'alertes par jour soit défini sur 20 et le seuil d'alerte de catégorie sur 10. Les administrateurs ne sont alertés que les 20 premières fois où les requêtes de catégorie dépassent le seuil. Cela signifie que seules les 200 premières occurrences entraînent des messages d'alerte (seuil de 10 multiplié par la limite d'alertes de 20).

Configuration des options d'alerte générales

Rubriques connexes :

- *Alertes*, page 287
- *Configuration des alertes système*, page 290
- *Configuration des alertes d'utilisation de catégories*, page 291
- *Configuration des alertes d'utilisation de protocole*, page 292

Websense peut signaler aux administrateurs divers types d'événements système, tels que les problèmes de mises à jour et d'abonnement de la base de données principale et le dépassement des seuils définis pour l'utilisation d'Internet.

Utilisez la page **Paramètres > Alertes et notifications > Alertes** pour sélectionner et configurer les méthodes de notification désirée, décrites ci-dessous. Servez-vous ensuite des autres pages de la section Paramètres > Alertes et notifications pour activer les alertes que vous souhaitez recevoir.

1. Entrez un nombre dans le champ **Maximum d'alertes par jour et par type d'utilisation** pour limiter le nombre total d'alertes générées chaque jour pour chaque alerte d'utilisation de catégorie et de protocole.

   Par exemple, vous pouvez configurer l'envoi d'alertes d'utilisation dès qu'une personne demande un site de la catégorie Sports à 5 reprises (seuil). Selon le nombre d'utilisateurs et leur schéma d'utilisation d'Internet, des centaines d'alertes pourraient être générées chaque jour.

   Si vous définissez le maximum d'alertes par jour et par type d'utilisation sur 10, 10 messages d'alertes seulement sont générés chaque jour pour la catégorie Sports. Dans cet exemple, les messages vous signalent les 50 premières demandes pour les sites de Sports (5 requêtes par alerte multiplié par 10 alertes).
2. Cochez la case **Activer les alertes par e-mail** pour envoyer les alertes et les notifications par courrier électronique. Configurez ensuite les paramètres de messagerie :

IP ou nom du serveur SMTP	Nom ou adresse IP du serveur SMTP qui doit acheminer les alertes par e-mail.
Depuis l'adresse de messagerie	Adresse e-mail à utiliser comme expéditeur les alertes.
Adresse de messagerie de l'administrateur (À)	Adresse e-mail du principal destinataire des alertes.
Adresses de messagerie des destinataires (Cc)	Adresse e-mail de jusqu'à 50 destinataires supplémentaires. Chaque adresse doit être placée sur une ligne distincte.

3. Cochez la case **Activer les alertes contextuelles** pour afficher des messages contextuels sur des ordinateurs spécifiques. Entrez ensuite l'adresse IP ou le nom de l'ordinateur de jusqu'à 50 **Destinataires**, chacun sur une ligne distincte.

   Remarque

   Les alertes contextuelles ne peuvent pas être envoyées à des ordinateurs Linux. Elle peuvent cependant être envoyées à partir d'un ordinateur Linux exécutant Policy Server vers des ordinateurs Windows, pour autant que le client Samba soit installé sur l'ordinateur Linux. Voir le *Guide de déploiement*.
4. Cochez la case **Activer les alertes SNMP** pour envoyer des messages d'alertes via le système d'interruption SNMP de votre réseau. Fournissez ensuite les informations relatives à votre système d'interruption SNMP.

Nom de la communauté	Nom de la communauté d'interruption sur votre serveur d'interruption SNMP.
Adresse IP ou nom du serveur	Adresse IP ou nom du serveur d'interruption SNMP.
Port	Numéro de port utilisé par les messages SNMP.

5. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Configuration des alertes système

Rubriques connexes :

- *Alertes*, page 287
- *Configuration des options d'alerte générales*, page 288
- *Vérification de l'état du système en cours*, page 294

Websense Manager affiche les informations détaillées de santé et d'état du système via la page **État > Alertes** (informations détaillées), décrite à la section *Vérification de l'état du système en cours*, page 294.

Pour que les événements système importants, tel qu'un échec de téléchargement de la base de données ou un abonnement sur le point d'expirer, soient signalés aux administrateurs lorsqu'ils ne sont pas connectés à Websense Manager, configurez des alertes système Websense à envoyer par e-mail, message contextuel ou par votre système d'interruption SNMP.

Dans l'onglet Paramètres, utilisez la page **Alertes et notifications > Système** pour sélectionner la méthode utilisée pour envoyer ces alertes aux administrateurs Websense, ainsi que les alertes à envoyer.

1. Pour chaque alerte, cochez les méthodes de livraison à utiliser. Selon les méthodes activées à la page Alertes, les choix potentiels sont **E-mail**, **Fenêtre contextuelle** et **SNMP**.

   Remarque

   Outre l'alerte générée, les informations relatives aux échecs de téléchargement de la base de données principale et aux niveaux d'abonnement dépassés sont enregistrées dans l'Observateur d'événements (Windows uniquement) et dans le fichier Websense.log (Windows et Linux).

   Des alertes sont disponibles pour les événements suivants :

   - Votre abonnement expire dans une semaine.
   - Modification des moteurs de recherche pris en charge par Search Filtering.
   - Échec du téléchargement de la base de données principale Websense.
   - Ajout ou suppression d'une catégorie ou d'un protocole dans la base de données principale.
   - Le nombre d'utilisateurs en cours dépasse votre niveau d'abonnement.
   - Le nombre d'utilisateurs en cours a atteint 90 % de votre niveau d'abonnement.

- Votre abonnement expire dans un mois.
- La base de données principale Websense a été mise à jour.

2. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Configuration des alertes d'utilisation de catégories

Rubriques connexes :

- *Alertes*, page 287
- *Contrôle des flux*, page 288
- *Configuration des options d'alerte générales*, page 288
- *Ajout d'alertes d'utilisation de catégories*, page 292

Websense peut vous avertir lorsque l'activité Internet liée à des catégories d'URL particulières atteint un seuil défini. Vous pouvez définir des alertes pour les requêtes autorisées ou bloquées de la catégorie.

Par exemple, vous pourriez souhaiter être prévenu(e) chaque fois que 50 requêtes ont été autorisées pour des sites de la catégorie Shopping afin de voir si vous devez placer des restrictions sur cette catégorie. Vous pourriez également souhaiter recevoir une alerte chaque fois que 100 requêtes ont été bloquées pour des sites de la catégorie Divertissement afin de savoir si les utilisateurs s'adaptent à la nouvelle stratégie d'utilisation d'Internet.

Dans l'onglet Paramètres, utilisez la page **Alertes et notifications > Utilisation de catégorie** pour consulter les alertes déjà établies et ajouter ou supprimer des catégories d'alertes d'utilisation.

1. Consultez les listes **Alertes d'utilisation de catégorie autorisée** et **Alertes d'utilisation de catégorie bloquée** pour découvrir les catégories configurées pour des alertes, le seuil de chacune et les méthodes d'alerte sélectionnées.
2. Cliquez sur **Ajouter** sous la liste appropriée pour ouvrir la page Ajouter des alertes d'utilisation de catégorie (voir *Ajout d'alertes d'utilisation de catégories*, page 292) et configurer d'autres catégories d'URL pour les alertes.
3. Cochez la case des catégories que vous souhaitez supprimer de la liste, puis cliquez sur **Supprimer** sous la liste appropriée.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Utilisation de catégorie. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout d'alertes d'utilisation de catégories

Rubriques connexes :

- *Alertes*, page 287
- *Configuration des options d'alerte générales*, page 288
- *Configuration des alertes d'utilisation de catégories*, page 291

La page **Ajouter des alertes d'utilisation de catégorie** s'affiche lorsque vous cliquez sur Ajouter dans la page Alertes d'utilisation de catégorie. Cette page vous permet de sélectionner de nouvelles catégories pour des alertes d'utilisation, de définir le seuil de ces alertes et de choisir les méthodes d'alerte.

1. Cochez la case accolée à chaque catégorie à ajouter avec le même seuil et les mêmes méthodes d'alerte.

   Remarque
   Vous ne pouvez pas ajouter d'alertes d'utilisation pour les catégories exclues de la journalisation. Voir *Configuration de Filtering Service pour la journalisation*, page 308.

2. Définissez le **Seuil** en sélectionnant le nombre de requêtes entraînant l'envoi d'une alerte.
3. Cochez la case de chaque méthode d'alerte désirée (**E-mail**, **Fenêtre contextuelle**, **SNMP**) pour ces catégories.

   Seules les méthodes d'alerte activées dans la page Alertes (voir *Configuration des options d'alerte générales*, page 288) peuvent être sélectionnées ici.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Alertes d'utilisation de catégorie (voir *Configuration des alertes d'utilisation de catégories*, page 291). Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Configuration des alertes d'utilisation de protocole

Rubriques connexes :

- *Alertes*, page 287
- *Contrôle des flux*, page 288
- *Configuration des options d'alerte générales*, page 288
- *Ajout d'alertes d'utilisation de protocole*, page 293

Websense peut vous avertir lorsque l'activité Internet liée à un protocole particulier atteint un seuil défini. Vous pouvez définir des alertes pour les requêtes autorisées ou bloquées du protocole sélectionné.

Par exemple, vous pourriez souhaiter être prévenu(e) chaque fois que 50 requêtes ont été autorisées pour un protocole de messagerie instantanée spécifique afin de voir si vous devez placer des restrictions sur ce protocole. Vous pourriez également souhaiter recevoir une alerte chaque fois que 100 requêtes ont été bloquées pour un protocole de partage de fichiers (P2P) afin de savoir si les utilisateurs s'adaptent à la nouvelle stratégie d'utilisation d'Internet.

Dans l'onglet Paramètres, utilisez la page **Alertes et notifications > Utilisation de protocole** pour consulter les alertes déjà établies et ajouter ou supprimer des protocoles pour les alertes d'utilisation.

1. Consultez les listes **Alertes d'utilisation de protocole autorisée** et **Alertes d'utilisation de protocole bloquée** pour découvrir les protocoles configurés pour des alertes, le seuil de chacune et les méthodes d'alerte sélectionnées.
2. Cliquez sur **Ajouter** sous la liste appropriée pour ouvrir la page Ajouter des alertes d'utilisation de protocole (voir *Ajout d'alertes d'utilisation de protocole*, page 293) et configurer d'autres protocoles pour les alertes.
3. Cochez la case des protocoles que vous souhaitez supprimer, puis cliquez sur **Supprimer** sous la liste appropriée.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Alertes d'utilisation de protocole. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout d'alertes d'utilisation de protocole

Rubriques connexes :

- *Alertes*, page 287
- *Configuration des options d'alerte générales*, page 288
- *Configuration des alertes d'utilisation de protocole*, page 292

Consultez les listes **Alertes d'utilisation de protocole > et Ajouter des alertes d'utilisation de protocole** pour sélectionner de nouveaux protocoles pour les alertes d'utilisation, définir le seuil de ces alertes et choisir les méthodes d'alerte.

1. Cochez la case accolée à chaque protocole à ajouter avec le même seuil et les mêmes méthodes d'alerte.

   Remarque

   Vous ne pouvez pas sélectionner un protocole pour les alertes si ce dernier n'est pas défini pour la journalisation dans un ou plusieurs filtres de protocoles.

   Les alertes de protocole ne reflètent que l'utilisation des clients gérés par un filtre de protocoles qui journalise le protocole.

2. Définissez le **Seuil** en sélectionnant le nombre de requêtes entraînant l'envoi d'une alerte.
3. Sélectionnez la méthode d'alerte désirée (**E-mail**, **Fenêtre contextuelle**, **SNMP**) pour ces protocoles.

   Seules les méthodes d'alerte activées dans la page Alertes (voir *Configuration des options d'alerte générales*, page 288) peuvent être sélectionnées ici.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Alertes d'utilisation de protocole (voir *Configuration des alertes d'utilisation de protocole*, page 292). Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Vérification de l'état du système en cours

Utilisez la page **État > Alertes** pour obtenir des informations sur les problèmes qui affectent la santé de votre logiciel Websense, de l'aide sur le dépannage et consulter les détails des mises à jour en temps réel récentes de la base de données principale Websense.

La liste **Alertes actives** présente l'état des composants Websense surveillés.

- Pour plus d'informations sur les composants surveillés, cliquez sur **Sur quoi porte la surveillance ?** au-dessus de la liste des messages d'alerte.
- Pour résoudre un problème, cliquez sur le bouton **Solutions** accolé au message d'erreur ou d'avertissement.
- Pour masquer un message d'alerte, cliquez sur **Avancé**. Si votre organisation n'utilise pas Log Server, Network Agent ou User Service, ou si vous n'envisagez pas d'activer WebCatcher, cochez la case pour masquer l'alerte associée. Lorsque vous avez terminé, cliquez sur **OK** pour activer la modification.

  Cliquez de nouveau sur **Avancé** pour masquer les options avancées.

La liste **Mises à jour de la base de données en temps réel** vous renseigne sur les mises à jour d'urgence de la base de données principale Websense, en indiquant :

- La date et l'heure de la mise à jour
- Le type de mise à jour
- Le nouveau numéro de version de la base de données

- La raison de la mise à jour
- L'adresse IP de l'instance de Filtering Service qui a reçu la mise à jour

Ces mises à jour supplémentaires viennent compléter les mises à jour régulières et planifiées de la base de données principale et peuvent être utilisées, par exemple, pour recatégoriser un site classé temporairement dans la mauvaise catégorie. Websense vérifie la présence de mises à jour de la base de données toutes les heures.

Pour les utilisateurs de Websense Web Security, la page Alertes comprend une troisième liste : **Mises à jour de sécurité en temps réel**. Cette liste est au même format que la liste Mises à jour de la base de données en temps réel, mais indique de façon plus spécifique les mises à jour de base de données liées à la sécurité.

L'installation des mises à jour de sécurité dès leur création élimine les failles liées aux attaques de type phishing (usurpation d'identité), aux applications et au code malveillants infectant les applications ou les sites Web.

Pour plus d'informations sur les mises à jour de la sécurité en temps réel, consultez la section *Real-Time Security Updates™*, page 33.

Servez-vous du bouton **Imprimer** situé en haut de la page pour ouvrir une fenêtre secondaire présentant une version imprimable de la zone Alertes. Servez-vous des options du navigateur pour imprimer la page, qui omet toutes les options de navigation affichées dans la fenêtre Websense Manager principale.

Sauvegarde et restauration des données Websense

Rubriques connexes :

- *Planification des sauvegardes*, page 297
- *Exécution de sauvegardes immédiates*, page 298
- *Maintenance des fichiers de sauvegarde*, page 299
- *Restauration des données Websense*, page 300
- *Interruption des sauvegardes planifiées*, page 301
- *Références des commandes*, page 301

L'utilitaire de sauvegarde et restauration de Websense simplifient la sauvegarde des données de stratégie et des paramètres Websense et permet de restaurer une configuration précédente. Les données enregistrées par l'utilitaire sont également utilisées pour importer les informations de configuration de Websense après une mise à niveau.

L'utilitaire de sauvegarde enregistre :

- Les informations de configuration globales, y compris les données des clients et des stratégies, stockées dans la base de données de stratégies

- Les informations de configuration locales, telles que les paramètres de Filtering Service et Log Server, stockées par chaque serveur Policy Server
- Les fichiers d'initialisation et de configuration des composants de Websense

Le processus de sauvegarde fonctionne de la manière suivante :

1. Vous déclenchez une sauvegarde immédiate (voir *Exécution de sauvegardes immédiates*, page 298) ou vous définissez un planning de sauvegarde (voir *Planification des sauvegardes*, page 297).
   - Déclenchez manuellement une sauvegarde à tout moment.
   - Les fichiers de sauvegarde sont stockés dans le répertoire défini lors de l'exécution ou de la planification de la sauvegarde.
2. L'utilitaire de sauvegarde vérifie tous les composants Websense de l'ordinateur, collecte les données éligibles pour la sauvegarde et crée un fichier d'archive. Le nom du fichier est au format suivant :

   `wsbackup_aaaa-mm-jj_hhmmss.tar.gz`

   Ici, *aaaa-mm-jj_hhmmss* représente la date et l'heure de la sauvegarde. **tar.gz** est un format de fichier compressé portable.

   Seul l'utilisateur racine (Linux) et les membres du groupe Administrateurs (Windows) peuvent accéder aux fichiers de sauvegarde.

Exécutez l'utilitaire de sauvegarde Websense sur chaque ordinateur comprenant des composants Websense. L'outil identifie et enregistre tous les fichiers suivants qu'il détecte sur l'ordinateur en cours :

Chemin	Nom du fichier
\Program Files\Websense\bin *ou* **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf securewispproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf pg_hba.conf

Chemin	Nom du fichier
BlockPages/*/Custom	Tous les paramètres de pages de blocage personnalisées
tomcat/conf/Catalina/Localhost	mng.xml
Windows\system32	isa_ignore.txt
Windows\system32\bin	ignore.txt
/etc/wsLib	wsSquid.ini

Stockez les fichiers de sauvegarde de Websense dans un endroit sécurisé. Ces fichiers doivent faire partie des procédures de sauvegarde régulières de votre organisation.

Pour restaurer une configuration précédente :

1. Récupérez les fichiers de sauvegarde sur leur site de stockage.
2. Copiez chaque fichier de sauvegarde sur l'ordinateur Websense sur lequel il a été créé.
3. Exécutez l'utilitaire de sauvegarde en mode restauration.

Important

Servez-vous toujours de l'utilitaire de sauvegarde pour restaurer une configuration de Websense. N'utilisez pas d'autres utilitaires d'extraction pour récupérer les fichiers de l'archive.

Si le fichier de sauvegarde est corrompu, vous ne pourrez pas restaurer vos paramètres.

Au cours du processus de sauvegarde, les messages d'erreur ou d'avertissement éventuels s'affichent sur l'ordinateur sur lequel la restauration est effectuée.

Planification des sauvegardes

Rubriques connexes :

- *Exécution de sauvegardes immédiates*, page 298
- *Maintenance des fichiers de sauvegarde*, page 299
- *Restauration des données Websense*, page 300
- *Interruption des sauvegardes planifiées*, page 301
- *Références des commandes*, page 301

Pour planifier des sauvegardes, ouvrez une fenêtre d'invite de commande et naviguez jusqu'au répertoire bin de Websense (**C:\Program Files\Websense\bin** ou **opt/Websense/bin**, par défaut). Entrez la commande suivante :

```
wsbackup -s -t "<m> <h> <jour_du_mois> <mois>
   <jour_de_la_semaine>" -d <répertoire>
```

Notez que les informations de date utilisent le format **crontab** et que les guillemets et les espaces sont obligatoires.

Remplacez les variables de l'exemple par les informations suivantes :

Variable	Informations
<m>	0 - 59 Spécifie la minute exacte de démarrage de la sauvegarde.
<h>	0 - 23 Spécifie l'heure générale du jour de démarrage de la sauvegarde.
<jour_du_mois>	1 - 31 Spécifie la date à laquelle la sauvegarde doit être effectuée. Si vous planifiez une sauvegarde pour les jours 29 à 31, l'utilitaire se sert de la procédure de substitution standard du système d'exploitation pour les mois qui ne comprennent pas cette date.
<mois>	1 - 12 Spécifie le mois au cours duquel la sauvegarde doit être effectuée.
<jour_de_la_semaine>	0 - 6 Définit un jour de la semaine. 0 correspond au dimanche.

Chaque champ peut recevoir un nombre, un astérisque ou une liste de paramètres. Consultez les références **crontab** pour plus d'informations.

Exécution de sauvegardes immédiates

Rubriques connexes :

- *Planification des sauvegardes*, page 297
- *Maintenance des fichiers de sauvegarde*, page 299
- *Restauration des données Websense*, page 300
- *Interruption des sauvegardes planifiées*, page 301
- *Références des commandes*, page 301

Pour déclencher une sauvegarde immédiate, ouvrez une fenêtre d'invite de commande et naviguez jusqu'au répertoire bin de Websense (**C:\Program Files\Websense\bin** ou **opt/Websense/bin**, par défaut). Entrez la commande suivante :

```
wsbackup -b -d <répertoire>
```

Ici, *répertoire* désigne le répertoire de destination de l'archive de la sauvegarde.

> **Avertissement**
> Ne stockez pas les fichiers de sauvegarde dans le répertoire **bin** de Websense. Ce répertoire est supprimé si vous désinstallez Websense.

Lorsque vous démarrez une sauvegarde immédiate, les messages d'erreur et les notifications éventuels s'affichent sur la console de l'ordinateur exécutant la sauvegarde.

Maintenance des fichiers de sauvegarde

Rubriques connexes :

- *Planification des sauvegardes*, page 297
- *Exécution de sauvegardes immédiates*, page 298
- *Restauration des données Websense*, page 300
- *Interruption des sauvegardes planifiées*, page 301
- *Références des commandes*, page 301

Lorsque vous effectuez une sauvegarde, un fichier de configuration (**WebsenseBackup.cfg**) est créé et stocké avec l'archive de la sauvegarde. Ce fichier de configuration spécifie :

- Le délai de conservation de l'archive dans le répertoire de sauvegarde
- La quantité maximale d'espace disque pouvant être utilisée par tous les fichiers de sauvegarde dans le répertoire

Modifiez le fichier **WebsenseBackup.cfg** dans un éditeur de texte quelconque pour changer ces paramètres :

Paramètre	Valeur
KeepDays	Nombre de jours pendant lesquels les fichiers d'archive doivent rester dans le répertoire de sauvegarde. La valeur par défaut est 365.
KeepSize	Nombre d'octets alloués aux fichiers de sauvegarde. La valeur par défaut est 10857600.

Tous les fichiers antérieurs à la valeur **KeepDays** sont supprimés du répertoire de sauvegarde. Si la quantité d'espace disque allouée est dépassée, les fichiers les plus anciens sont supprimés du répertoire de sauvegarde pour faire de la place aux nouveaux.

Restauration des données Websense

Rubriques connexes :

- *Planification des sauvegardes*, page 297
- *Exécution de sauvegardes immédiates*, page 298
- *Maintenance des fichiers de sauvegarde*, page 299
- *Interruption des sauvegardes planifiées*, page 301
- *Références des commandes*, page 301

Lorsque vous restaurez les données de configuration de Websense, veillez à restaurer les données des composants existants sur l'ordinateur en cours.

Pour déclencher le processus de restauration, ouvrez une fenêtre d'invite de commande et naviguez jusqu'au répertoire bin de Websense (**C:\Program Files\Websense\bin** ou **opt/Websense/bin**, par défaut). Entrez la commande suivante :

```
wsbackup -r -f fichier_archive.tar.gz
```

Important

Le processus de restauration peut durer plusieurs minutes. Ne l'interrompez pas avant la fin.

Pendant le processus de restauration, l'utilitaire de sauvegarde arrête tous les services Websense. Si l'utilitaire ne peut pas arrêter les services, il envoie un message pour inviter l'utilisateur à les arrêter manuellement. Les services doivent être arrêtés dans l'ordre indiqué à la section *Arrêt et démarrage des services Websense*, page 286.

L'utilitaire de sauvegarde enregistre certains fichiers utilisés pour la communication avec les produits d'intégration tiers. Ces fichiers étant situés hors de la structure de répertoires de Websense, vous devez les restaurer manuellement, en copiant chacun d'eux dans le répertoire approprié.

Les fichiers qui doivent être restaurés manuellement comprennent :

Nom du fichier	Restaurer dans
isa_ignore.txt	**Windows\system32**
ignore.txt	**Windows\system32\bin**
wsSquid.ini	**/etc/wsLib**

Interruption des sauvegardes planifiées

Rubriques connexes :

- *Planification des sauvegardes*, page 297
- *Exécution de sauvegardes immédiates*, page 298
- *Maintenance des fichiers de sauvegarde*, page 299
- *Restauration des données Websense*, page 300
- *Références des commandes*, page 301

Pour effacer le planning de sauvegardes et interrompre l'exécution des sauvegardes actuellement planifiées, ouvrez une fenêtre d'invite de commande et naviguez jusqu'au répertoire bin de Websense (**C:\Program Files\Websense\bin** ou **opt/Websense/bin**, par défaut). Entrez la commande suivante :

```
wsbackup -u
```

Références des commandes

Rubriques connexes :

- *Planification des sauvegardes*, page 297
- *Exécution de sauvegardes immédiates*, page 298
- *Maintenance des fichiers de sauvegarde*, page 299
- *Restauration des données Websense*, page 300
- *Interruption des sauvegardes planifiées*, page 301

Seul l'utilisateur racine (Linux) ou un membre du groupe Administrateurs (Windows) peut exécuter l'utilitaire de sauvegarde.

Pour consulter la liste complète des options des commandes de l'utilitaire de sauvegarde, entrez à tout moment :

```
wsbackup -h
```

ou

```
wsbackup --help
```

La commande **wsbackup** reconnaît les options suivantes :

- `-b` *ou* `--backup`
- `-d` *chemin_répertoire* *ou* `--dir` *chemin_répertoire*
- `-f` *nom_de_fichier_complet* *ou* `--file` *nom_de_fichier_complet*
- `-h` *ou* `--help` *ou* `-?`

- `-r` *ou* `--restore`
- `-s` *ou* `--schedule`
- `-t` *ou* `--time`
- `-u` *ou* `--unschedule`
- `-v` *ou* `--verbose [0...3]`

13 Administration de la génération de rapports

Rubriques connexes :

- *Planification de votre configuration*, page 304
- *Gestion de l'accès aux outils de génération de rapports*, page 304
- *Configuration de base*, page 305
- *Utilitaire Configuration de Log Server*, page 310
- *Administration de la base de données d'activité*, page 323
- *Configuration des rapports d'investigation*, page 334
- *Rapports sur activité propre*, page 339

Pour utiliser les rapports de présentation et d'investigation de Websense, vous devez installer Websense Manager et les composants de génération de rapports sur un serveur Windows. Vous devez également configurer Websense pour journaliser l'activité du filtrage Internet.

La journalisation envoie des enregistrements à Websense Log Server, qui les traite dans une base de données d'activité devant être installée avec un moteur de base de données pris en charge : Microsoft SQL Server Desktop Engine (généralement appelé MSDE dans ce document) ou Microsoft SQL Server Enterprise ou Standard Editions (généralement appelé Microsoft SQL Server). Pour des instructions sur l'installation de ces composants de génération de rapports, consultez le *Guide d'installation*.

Lorsque vous générez un rapport, Websense Manager présente les informations de la base de données d'activité en fonction du filtre que vous avez défini pour ce rapport.

Les organisations qui installent Websense Manager sur un serveur Linux, ou qui préfèrent utiliser Linux pour la génération de rapports, peuvent installer le produit Websense Explorer pour Linux pour générer des rapports. Ce produit fonctionne indépendamment de Websense Manager. Reportez-vous au *Guide d'administration d'Explorer pour Linux* pour plus d'informations sur l'installation et l'utilisation de ce programme.

Planification de votre configuration

Selon le volume du trafic Internet de votre réseau, la taille de la base de données d'activité peut devenir très importante. Pour établir une stratégie de journalisation et de génération de rapports efficace pour votre organisation, posez-vous les questions suivantes :

- À quel moment le trafic réseau est-il le plus important ?

  Pensez à planifier les travaux de base de données et de génération de rapports consommateurs de ressources à des heures où le trafic est plus faible. Vous améliorerez ainsi les performances de la journalisation et de la génération de rapports pendant les périodes de pointe. Voir *Configuration des options du temps de navigation sur Internet*, page 328 et *Configuration des options de maintenance de la base de données d'activité*, page 329.

- Pendant combien de temps les données d'activité doivent-elles être conservées pour les rapports historiques ?

  Pensez à supprimer automatiquement les partitions lorsque ce délai est écoulé. Vous réduirez ainsi la quantité d'espace disque requise pour la base de données d'activité. Voir *Configuration des options de maintenance de la base de données d'activité*, page 329.

- Quels sont les détails réellement nécessaires ?

  Identifiez les options de journalisation devant être activées : la journalisation des URL complètes et des accès augmente la taille de la base de données d'activité. Pour réduire la taille de la base d'activité, envisagez de :

  - désactiver la journalisation des URL complètes (voir *Configuration de la journalisation des URL complètes*, page 326)
  - journaliser les visites plutôt que les accès (voir *Configuration des fichiers cache du journal*, page 315)
  - activer la consolidation (voir *Configuration des options de consolidation*, page 316)
  - activer la journalisation sélective des catégories (voir *Configuration de Filtering Service pour la journalisation*, page 308)

Les implémentations de génération de rapports les plus réussies sont déployées sur du matériel répondant ou dépassant les exigences nécessaires par rapport à la charge attendue et au délai de conservation des données historiques.

Gestion de l'accès aux outils de génération de rapports

Lorsque Websense Manager et les composants de génération de rapports sont installés sur des serveurs Windows, les options de génération de rapports apparaissent dans Websense Manager et dans l'utilitaire de configuration de Log Server.

Lorsque vous installez les composants de génération de rapports, Log Server est connecté à un serveur Policy Server spécifique. Pour accéder aux fonctionnalités de

génération de rapports, vous devez sélectionner ce serveur Policy Server lors de la connexion à Websense Manager. Si vous vous connectez à un autre serveur Policy Server, vous n'avez pas accès aux rapports de présentation ou d'investigation dans l'onglet Principal, ni à l'ensemble de la section Génération de rapports de l'onglet Paramètres.

Dans les organisations qui utilisent uniquement le compte de connexion WebsenseAdministrator, toutes les personnes qui utilisent Websense Manager ont accès à toutes les options de génération de rapports de Websense Manager, y compris aux rapports de présentation et d'investigation et aux paramètres des outils de génération de rapports.

Dans les organisations qui utilisent l'administration déléguée, l'accès aux outils de génération de rapports au sein de Websense Manager est contrôlé par le compte WebsenseAdministrator et les membres du rôle Super administrateur. Lorsqu'il crée un rôle, le Super administrateur indique si ce rôle a accès à des options de génération de rapports spécifiques.

Pour plus d'informations sur la configuration des accès aux outils de génération de rapports, consultez la section *Modification des rôles*, page 257.

L'utilitaire Configuration de Log Server est accessible dans le menu Démarrer de Windows. Seules les personnes qui ont accès à l'ordinateur d'installation peuvent ouvrir cet utilitaire et modifier les paramètres de Log Server. Voir *Utilitaire Configuration de Log Server*, page 310.

Si votre organisation a installé Websense Manager sur un serveur Linux, ou choisi le programme de création de rapports Websense Explorer pour Linux à la place des composants de création de rapport fonctionnant sous Windows, les options de création de rapports ne s'affichent pas dans Websense Manager. Aucun graphique de filtrage Internet ne peut s'afficher dans les pages Aujourd'hui et Historique. Reportez-vous au *Guide d'administration d'Explorer pour Linux* pour plus d'informations sur l'installation de ce programme et son utilisation pour l'exécution des rapports.

Configuration de base

Rubriques connexes :

- *Configuration de Filtering Service pour la journalisation*, page 308
- *Attribution de catégories aux classes de risque*, page 306
- *Configuration des préférences de génération de rapports*, page 308
- *Utilitaire Configuration de Log Server*, page 310
- *Administration de la base de données d'activité*, page 323

Un large éventail d'options de configuration vous permettent de personnaliser la génération de rapports pour votre environnement.

La base de données principale Websense regroupe les catégories dans des **classes de risque**. Les classes de risque suggèrent des types ou des niveaux possibles de vulnérabilité représentés par les sites présents dans ces catégories. Pour personnaliser les classes de risque de votre organisation, utilisez la page Général > Classes de risque, accessible depuis l'onglet Paramètres. Voir *Attribution de catégories aux classes de risque*, page 306.

La page Génération de rapports > Préférences, accessible depuis l'onglet Paramètres, permet de configurer le serveur de messagerie utilisé pour diffuser les rapports et d'activer la fonction de génération de rapports sur l'activité propre. Voir *Configuration des préférences de génération de rapports*, page 308.

La journalisation est le processus qui consiste à stocker les informations relatives aux activités de filtrage de Websense dans une base de données d'activité dans le but de générer des rapports.

La page Général > Journalisation, accessible depuis l'onglet Paramètres, permet d'activer la journalisation et de sélectionner les catégories et les informations des utilisateurs à journaliser. Pour plus d'informations, consultez *Configuration de Filtering Service pour la journalisation*, page 308.

Servez-vous de l'utilitaire Configuration de Log Server pour gérer le traitement des enregistrements de journal et les connexions à la base de données d'activité. Pour plus d'informations, consultez *Utilitaire Configuration de Log Server*, page 310.

La page Génération de rapports > Base de données d'activité, accessible depuis l'onglet Paramètres, permet d'administrer la base de données d'activité, y compris le temps de navigation Internet, les options de partition de la base de données et les journaux d'erreurs. Pour plus d'informations, consultez *Administration de la base de données d'activité*, page 323.

Attribution de catégories aux classes de risque

Rubriques connexes :

- *Classes de risque*, page 41
- *Pages de blocage*, page 85
- *Utilisation des rapports pour évaluer l'efficacité des stratégies de filtrage*, page 95

La base de données principale Websense regroupe les catégories dans des **classes de risque**. Les classes de risque suggèrent des types ou des niveaux possibles de vulnérabilité représentés par les sites présents dans ces catégories.

Les classes de risques sont essentiellement utilisées pour la génération de rapports. Les pages Aujourd'hui et Historiques comprennent des graphiques qui illustrent l'activité Internet par classe de risques et vous permettent de générer des rapports de présentation ou d'investigation triés par classe de risques.

Les Super administrateurs inconditionnels peuvent afficher ou modifier les catégories affectées à chaque classe de risques dans la page **Paramètres > Classes de risque**. Par exemple, certaines entreprises considèrent que les sites de vidéo publiées par les utilisateurs relèvent des classes de risque de responsabilité légale, de perte de bande passante réseau et de perte de productivité. Toutefois, si votre entreprise réalise des études de marché sur certaines populations, vous pouvez estimer que ces sites relèvent de la classe de risque Utilisation professionnelle.

> **Remarque**
> La page de blocage de sécurité s'affiche pour les sites bloqués dans les catégories par défaut de la classe Risque de sécurité. Les modifications apportées aux catégories de la classe Risque de sécurité affectent la génération des rapports, mais pas les pages de blocage. Voir *Pages de blocage*, page 85.

Les informations sur les classes de risque des rapports Websense reflètent les attributions effectuées dans cette page.

1. Sélectionnez une entrée dans la liste **Classes de risque**.
2. Examinez la liste **Catégories** pour identifier les catégories actuellement incluses dans cette classe de risque.

   Une coche indique que la catégorie est actuellement attribuée à la classe de risque sélectionnée. L'icône W bleue désigne les catégories incluses par défaut dans la classe de risque.
3. Pour inclure ou exclure une catégorie de la classe de risque sélectionnée, cochez ou supprimez la coche de cette catégorie dans l'arborescence. Chaque catégorie peut appartenir à plusieurs Classes de risque.

   Les autres choix disponibles sont les suivants :

Option	Description
Sélectionner tout	Sélectionne toutes les catégories dans l'arborescence.
Effacer tout	Désélectionne toutes les catégories dans l'arborescence.
Restaurer les valeurs par défaut	Réinitialise les choix de catégories définis par Websense pour la classe de risque sélectionnée. Une icône W bleue désigne une catégorie par défaut.

4. Répétez ce processus pour chaque classe de risque.
5. Cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Configuration des préférences de génération de rapports

Rubriques connexes :

- *Rapports sur activité propre*, page 339
- *Planification des rapports de présentation*, page 110
- *Planification des rapports d'investigation*, page 138

Lorsque vous planifiez l'exécution ultérieure ou périodique de rapports de présentation ou d'investigation, ces rapports sont envoyés par e-mail aux destinataires spécifiés. Définissez les informations relatives à ces messages électroniques à la page **Génération de rapports > Préférences**, accessible depuis l'onglet Paramètres.

Cette page permet également d'activer la fonction de génération de rapports sur l'activité propre, qui permet aux utilisateurs de générer des rapports d'investigation sur leur propre activité Internet.

1. Entrez l'**Adresse de messagerie** devant s'afficher dans le champ De lorsque des rapports planifiés sont envoyés par e-mail.
2. Entrez l'**IP ou nom du serveur SMTP** du serveur de messagerie utilisé pour distribuer les rapports planifiés par e-mail.
3. Cochez la case **Permettre aux utilisateurs de générer des rapports sur leur propre activité** pour autoriser les utilisateurs de votre organisation à accéder à Websense Manager et à exécuter des rapports d'investigation sur leur propre activité Internet. Voir *Rapports sur activité propre*, page 339.
4. Cliquez sur **Enregistrer** pour implémenter vos modifications.

Configuration de Filtering Service pour la journalisation

Rubriques connexes :

- *Présentation de la base de données d'activité*, page 321
- *Utilitaire Configuration de Log Server*, page 310

La page **Général > Journalisation** de l'onglet Paramètres permet de spécifier l'adresse IP et le port permettant d'envoyer les enregistrements de journal à Log Server. Cette page permet également de sélectionner les informations de l'utilisateur et les catégories d'URL que Websense Filtering Service doit envoyer à Log Server et utilisées pour la génération de rapports et les alertes d'utilisation des catégories (voir *Configuration des alertes d'utilisation de catégories*, page 291).

Dans un environnement comprenant plusieurs serveurs Policy Server, configurez la page Général > Journalisation séparément pour chaque serveur. Tous les services Filtering Service associés au serveur Policy Server actif envoient leurs enregistrements de journal au serveur Log Server identifié sur cette page.

Lorsque vous utilisez plusieurs serveurs Policy Server, n'oubliez pas les points suivants :

- Si les champs d'adresse IP et de port de Log Server ne sont pas renseignés pour un serveur Policy Server, les services Filtering Service associés à ce serveur ne peuvent journaliser aucun trafic pour la génération de rapports ou d'alertes.
- Chaque service Filtering Service journalise le trafic en fonction des paramètres du serveur Policy Server auquel il est connecté. Si vous modifiez les informations utilisateur ou les choix de journalisation des catégories pour les différents serveurs Policy Server, les rapports générés pour les utilisateurs associés à des serveurs Policy Server différents peuvent sembler incohérents.

Si votre environnement comprend plusieurs serveurs Policy Server et Log Server, assurez-vous de vous connecter à chaque serveur Policy Server séparément et que ce dernier communique bien avec le serveur Log Server approprié.

1. Pour journaliser les informations d'identification des ordinateurs qui accèdent à Internet, cochez la case **Journaliser les adresses IP**.
2. Pour journaliser les informations d'identification des utilisateurs qui accèdent à Internet, cochez la case **Journaliser les noms d'utilisateurs.**

   Remarque

   Si vous ne journalisez pas les adresses IP ou les noms d'utilisateur, vos rapports ne contiennent aucune donnée relative aux utilisateurs. On parle parfois dans ce cas de **journalisation anonyme**.

3. Entrez l'adresse IP ou le nom de l'ordinateur sur lequel le serveur Log Server est installé dans le champ **Adresse IP ou nom de Log Server**.

   Important

   Si Log Server n'est pas installé sur le même ordinateur que Policy Server, cette entrée peut être définie par défaut sur localhost. Si cela se produit, entrez l'adresse IP de l'ordinateur Log Server pour autoriser l'affichage des graphiques sur les pages Aujourd'hui et Historique, ainsi que les autres fonctions de génération de rapports.

4. Entrez le numéro de **Port** pour envoyer les enregistrements du journal à Log Server.
5. Cliquez sur **Vérifier l'état** pour déterminer si Websense Manager peut communiquer avec le Log Server spécifié.

   Un message indique si le test de la connexion a réussi. Actualisez l'adresse IP ou le nom d'ordinateur et le port, le cas échéant, jusqu'à ce que le test réussisse.
6. Cliquez sur le bouton **Journalisation de catégorie sélective** pour ouvrir la section permettant de spécifier les catégories d'URL à journaliser.

Les choix que vous spécifiez ici s'appliquent à tous les filtres de catégories dans l'ensemble des stratégies actives.

Remarques

Si vous désactivez la journalisation de catégories pour lesquelles des alertes d'utilisation sont configurées (voir *Configuration des alertes d'utilisation de catégories*, page 291), aucune alerte d'utilisation ne peut être envoyée.

Les rapports ne peuvent pas comprendre d'informations sur les catégories non journalisées.

a. Selon vos besoins, développez ou réduisez les catégories parentes pour voir les catégories qui vous intéressent.

b. Sélectionnez chaque catégorie à journaliser en cochant la case accolée.

   Vous devez sélectionner ou désélectionner chaque catégorie séparément. La sélection d'une catégorie parente ne sélectionne pas automatiquement ses sous-catégories. Pour simplifier vos sélections, utilisez **Sélectionner tout** et **Effacer tout**.

7. Cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Utilitaire Configuration de Log Server

Rubriques connexes :

- *Gestion de l'accès aux outils de génération de rapports*, page 304
- *Configuration de base*, page 305
- *Arrêt et démarrage de Log Server*, page 321

Au cours de l'installation, vous configurez certains aspects du fonctionnement de Log Server, y compris ses interactions avec les composants de filtrage de Websense.

L'utilitaire Configuration de Log Server vous permet au besoin de modifier ces paramètres et de configurer d'autres détails relatifs au fonctionnement de Log Server. Cet utilitaire est installé sur le même ordinateur que Log Server.

1. Dans le menu Démarrer de Windows, sélectionnez **Programmes > Websense > Utilitaires > Configuration de Log Server**.

   L'utilitaire Configuration de Log Server apparaît.

2. Sélectionnez un onglet pour afficher ses options et les modifier. Pour plus d'informations, consultez :

   - *Configuration des connexions de Log Server*, page 311
   - *Configuration des options de base de données de Log Server*, page 312

- *Configuration des fichiers cache du journal*, page 315
- *Configuration des options de consolidation*, page 316
- *Configuration de WebCatcher*, page 318

3. Cliquez sur **Appliquer** pour enregistrer vos modifications.
4. Utilisez l'onglet **Connexion** pour arrêter et redémarrer Log Server afin que les modifications soient prises en compte.

IMPORTANT

Après avoir apporté des modifications dans l'onglet Configuration de Log Server, cliquez sur **Appliquer**. Vous **devez** ensuite arrêter et redémarrer Log Server pour que les modifications soient prises en compte. Pour éviter de redémarrer Log Server plusieurs fois, effectuez toutes les modifications nécessaires avant de le redémarrer.

Configuration des connexions de Log Server

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration des options de base de données de Log Server*, page 312
- *Configuration des fichiers cache du journal*, page 315
- *Configuration des options de consolidation*, page 316
- *Configuration de WebCatcher*, page 318
- *Arrêt et démarrage de Log Server*, page 321

Les options de l'onglet **Connexion** de l'utilitaire Configuration de Log Server permettent de créer et d'établir une connexion entre Log Server et les composants de filtrage de Websense.

1. Acceptez le **Port d'entrée Log Server** par défaut (55805) ou entrez un autre port disponible.

   Il s'agit du port par lequel Log Server doit communiquer avec Filtering Service. Le port saisi ici doit correspondre au port indiqué à la page Général > Journalisation (onglet Paramètres) de Websense Manager.
2. Dans le champ **Intervalle de mise à jour des utilisateurs/groupes** entrez un nombre d'heures pour spécifier la fréquence à laquelle Log Server doit contacter le service d'annuaire pour des mises à jour.

   Log Server contacte le service d'annuaire pour obtenir de nouvelles informations, par exemple les attributions de groupes et de noms d'utilisateur, sur les utilisateurs possédant des enregistrements dans la base de données d'activité.

L'activité d'un utilisateur dont le groupe a changé continue à être prise en compte pour le groupe précédent jusqu'à la prochaine mise à jour. Les organisations qui mettent fréquemment à jour leur service d'annuaire ou qui possèdent un grand nombre d'utilisateurs doivent envisager d'actualiser plus fréquemment les informations des utilisateurs/groupes que la valeur de 12 heures par défaut.

3. Cliquez sur **Appliquer** pour enregistrer vos modifications.
4. Utilisez le bouton de la section État du service pour **Démarrer** ou **Arrêter** Log Server. L'intitulé du bouton change en fonction de l'action devant se produire lorsque vous cliquez sur son entrée.

> **Remarque**
> Aucune activité d'accès à Internet ne peut être enregistrée lorsque Log Server est arrêté.

Les modifications apportées dans l'utilitaire de configuration de Log Server ne prennent pas effet avant l'arrêt et le redémarrage de Log Server.

Configuration des options de base de données de Log Server

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration des connexions de Log Server*, page 311
- *Configuration de la connexion à la base de données*, page 314
- *Configuration des fichiers cache du journal*, page 315
- *Configuration des options de consolidation*, page 316
- *Configuration de WebCatcher*, page 318
- *Arrêt et démarrage de Log Server*, page 321

Ouvrez l'onglet **Base de données** de l'utilitaire de configuration de Log Server pour configurer le fonctionnement de Log Server avec la base de données d'activité.

1. Choisissez une **Méthode d'insertion de journal** parmi les options suivantes.
   - ODBC (Open Database Connectivity) : insère individuellement les enregistrements dans la base de donnée, en utilisant un pilote de base de données pour gérer les données entre Log Server et la base de données d'activité.
   - BCP (Bulk Copy Program) *(recommandé)* : insère les enregistrements dans la base de données d'activité par groupes appelés lots. Cette option est recommandée car elle est plus efficace que l'insertion ODBC.

> **Remarque**
> L'option BCP n'est disponible que si vous avez installé les outils SQL Server Client sur l'ordinateur Log Server.

2. Cliquez sur le bouton **Connexion** pour sélectionner la base de données d'activité dans laquelle devront être stockées les informations d'accès à Internet de Websense. Voir *Configuration de la connexion à la base de données*, page 314.

   Nom de la source de données ODBC (DSN) et **Nom de connexion ODBC** affichent les paramètres définis pour la connexion à la base de données.

3. Si vous avez choisi la méthode d'insertion de journal BCP à l'étape 1, définissez les options suivantes. Si vous avez choisi la méthode d'insertion de journal ODBC, ignorez cette étape.

Option	Description
Emplacement du chemin d'accès du fichier BCP	Chemin d'accès du répertoire de stockage des fichiers BCP. Log Server doit pouvoir accéder à ce répertoire en lecture et en écriture. Cette option est disponible uniquement si Log Server est installé sur l'ordinateur de la base de données d'activité ou si les outils SQL Server Client sont installés sur l'ordinateur Log Server.
Taux de création du fichier BCP	Nombre maximal de minutes consacrées par Log Server à placer les enregistrements dans un fichier de traitement par lots avant la fermeture de ce dernier et la création d'un nouveau. Ce paramètre est combiné au paramètre de la taille des lots : Log Server crée un nouveau fichier de traitement par lots dès que l'une des limites est atteinte.
Taille maximum de lot BCP	Nombre maximal d'enregistrements de journal avant la création d'un nouveau fichier de traitement par lots. Ce paramètre est combiné au taux de création : Log Server crée un nouveau fichier de traitement par lots dès que l'une des limites est atteinte.

4. Définissez le **Nombre maximal de connexions autorisées** pour définir le nombre de connexions internes pouvant être établies entre Log Server et le moteur de base de données. Les options disponibles dépendent du moteur de base de données utilisé.
   - **MSDE** : Cette valeur est définie par défaut sur 4 et ne peut pas être modifiée.
   - **SQL Server** : définissez un nombre compris entre 4 et 50, selon votre licence SQL Server. Le nombre minimal de connexions dépend de la méthode d'insertion de journal sélectionnée.

     Remarque

     L'augmentation du nombre de connexions peut accroître la vitesse de traitement des enregistrements du journal mais peut avoir un impact sur d'autres processus réseau qui utilisent le même serveur SQL Server. Dans la plupart des cas, il est préférable de définir un nombre de connexions inférieur à 20. Contactez votre administrateur de base de données pour obtenir de l'aide.

5. Activez ou désactivez l'option **Journalisation améliorée** qui contrôle la reprise de la journalisation de Log Server après son arrêt.

   Si cette option est désactivée (ce qui est le cas par défaut), après un arrêt, Log Server commence le traitement au début du fichier journal le plus ancien. Cette opération peut entraîner l'apparition d'entrées en double dans la base de données d'activité, mais accélère le traitement de Log Server.

   Lorsque cette option est activée, Log Server surveille son emplacement dans le fichier cache du journal actif. Après un redémarrage, Log Server reprend le traitement là où il s'était arrêté. La journalisation améliorée peut ralentir le traitement de Log Server.
6. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis arrêtez et redémarrez Log Server (voir *Arrêt et démarrage de Log Server*, page 321).

Configuration de la connexion à la base de données

Rubriques connexes :

- *Configuration des connexions de Log Server*, page 311
- *Configuration des options de base de données de Log Server*, page 312

Le bouton **Connexion** de l'onglet Base de données de l'utilitaire de configuration de Log Server permet de sélectionner la base de données d'activité dans laquelle doivent être stockées les informations d'accès à Internet de Websense. Cette configuration est automatique pendant l'installation, mais peut-être changée chaque fois que la journalisation de la base de données doit être modifiée. (Pour établir une connexion, la base de données doit déjà exister.)

1. Dans la boîte de dialogue de la source de données, sélectionnez l'onglet **Source de données de l'ordinateur**.
2. Sélectionnez la connexion ODBC de la base de données dans laquelle les nouvelles informations seront enregistrées.
3. Cliquez sur **OK** pour afficher la boîte de dialogue de connexion à SQL Server.
4. Si l'option **Utiliser une connexion approuvée** est disponible, veillez à ce qu'elle soit correctement configurée pour votre environnement.

   Utilisateurs MSDE : désactivez l'option Connexion sécurisée.

   Utilisateurs SQL Server : demandez l'aide de votre administrateur de base de données.

   Remarque

   Si vous utilisez une connexion sécurisée pour les communications avec SQL Server, vous devez configurer plusieurs services Websense avec les nom d'utilisateur et mot de passe approuvés. Pour obtenir des instructions détaillées, reportez-vous au *Guide d'installation* de Websense.

5. Entrez l'**ID de connexion** et le **Mot de passe** définis lors de la création de la base de données. Il s'agit généralement des mêmes ID de connexion et mot de passe saisis lors de l'installation de Log Server et de la création de la base de données.
6. Arrêtez et redémarrez Log Server via l'onglet **Connexion** après avoir modifié les paramètres de l'utilitaire de configuration de Log Server.

Configuration des fichiers cache du journal

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration des connexions de Log Server*, page 311
- *Configuration des options de base de données de Log Server*, page 312
- *Configuration des options de consolidation*, page 316
- *Configuration de WebCatcher*, page 318
- *Arrêt et démarrage de Log Server*, page 321

L'onglet **Paramètres** de l'utilitaire de configuration de Log Server permet de gérer des options de création des fichiers cache du journal et de spécifier si Log Server surveille les fichiers individuels composant chaque site Web demandé ou seulement ce dernier.

1. Entrez le chemin de stockage des fichiers cache du journal dans le champ **Emplacement du chemin d'accès du fichier journal**. Le chemin d'accès par défaut est **<répertoire d'installation>\bin\Cache**. (Le répertoire d'installation par défaut est C:\Program Files\Websense\).
2. Dans le champ **Taux de création du fichier cache**, indiquez le nombre maximal de minutes que Log Server doit consacrer à l'envoi des informations d'accès Internet à un fichier cache du journal (**log*n*.tmp**) avant de le fermer et d'en créer un nouveau.

   Ce paramètre est combiné au paramètre de taille : Log Server crée un nouveau fichier cache de journal dès que l'une des limites est atteinte.
3. Dans le champ **Taille de création du cache**, indiquez la taille que le fichier de cache de journal doit atteindre avant que Log Server ne le ferme et en crée un nouveau.

   Ce paramètre est combiné au taux de création : Log Server crée un nouveau fichier cache de journal dès que l'une des limites est atteinte.
4. Cochez la case **Activer les visites** pour créer un enregistrement de journal pour chaque site Web demandé.

> **Remarque**
>
> La gestion de la taille de la base de données d'activité est essentielle pour les réseaux à fort trafic. L'activation de la journalisation des visites est une manière de contrôler la taille et la croissance de la base de données.

Lorsque cette option est désactivée, un enregistrement de journal distinct est créé pour chaque requête HTTP générée pour afficher les différents éléments de la page, par exemple des graphiques et des publicités. Également appelée journalisation des accès, cette option crée une base de données d'activité de taille beaucoup plus importante et qui croît rapidement.

Lorsque cette action est activée, Log Server combine les éléments individuels composant la page Web (par exemple les graphiques et les publicités) dans un même enregistrement de journal.

Si vous avez installé Websense Web Security Gateway, l'activité d'analyse en temps réel est toujours rapportée en nombre d'accès sur les rapports liés à l'analyse en temps réel, même lorsque la journalisation des visites est activée. Dans ce cas, les chiffres présentés dans les rapports du filtrage Web et incluant le trafic bloqué par l'analyse en temps réel seront inférieurs à ceux qui apparaissent dans les rapports de l'analyse en temps réel.

Remarque

Il est préférable de créer une nouvelle partition de base de données avant de modifier la méthode de journalisation entre visites et accès. Pour créer une nouvelle partition de base de données, reportez-vous à la page Génération de rapports > Base de données d'activité (onglet Paramètres) de Websense Manager.

5. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis arrêtez et redémarrez Log Server (voir *Arrêt et démarrage de Log Server*, page 321).

Configuration des options de consolidation

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration des connexions de Log Server*, page 311
- *Configuration des options de base de données de Log Server*, page 312
- *Configuration des fichiers cache du journal*, page 315
- *Configuration de WebCatcher*, page 318
- *Arrêt et démarrage de Log Server*, page 321

Ouvrez l'onglet **Consolidation** de l'utilitaire de configuration de Log Server pour activer la consolidation et définir ses préférences.

Remarque

La gestion de la taille de la base de données d'activité est essentielle pour les réseaux à fort trafic. L'activation de la consolidation est une manière de contrôler la taille et la croissance de la base de données.

La consolidation réduit la taille de la base de données d'activité en combinant les requêtes Internet qui partagent les éléments suivants :

- Nom du domaine (par exemple : www.websense.com)
- Catégorie
- Mot-clé
- Action (par exemple : Catégorie bloquée)
- Utilisateur/Station de travail

L'exécution des rapports est plus rapide lorsque la base de données d'activité est réduite. La consolidation des données de journal peut cependant réduire la précision de certains rapports détaillés, du fait de la perte d'enregistrements distincts pour le même nom de domaine.

> **Important**
> L'activation de la consolidation peut réduire la précision de certaines données de rapport, telles que les calculs de temps de navigation Internet.

1. Cochez la case **Consolider les enregistrements de journal** pour activer la consolidation, qui combine plusieurs requêtes Internet similaires dans un même enregistrement de journal.

   Lorsque cette option est désactivée, (ce qui est le cas par défaut), la base de données d'activité contient l'ensemble des détails relatifs aux accès ou aux visites pour chaque requête Internet (selon votre sélection dans l'onglet Paramètres, voir *Configuration des fichiers cache du journal*, page 315). Les rapports sont donc plus détaillés, mais la base de données sera plus volumineuse.

   L'activation de cette option crée une base de données d'activité plus petite et des rapports moins détaillés.

   > **Important**
   > Pour garantir la cohérence des rapports, pensez à créer une nouvelle partition de base de données chaque fois que vous activez ou désactivez la consolidation. De même, assurez-vous de générer des rapports à partir de partitions présentant le même paramètre de consolidation.

   Si vous avez installé Websense Web Security Gateway, l'activité d'analyse en temps réel est toujours rapportée en accès distincts sur les rapports liés à l'analyse en temps réel, même lorsque la consolidation est activée. Dans ce cas, les chiffres présentés dans les rapports du filtrage Web et incluant le trafic bloqué par l'analyse en temps réel seront inférieurs à ceux qui apparaissent dans les rapports de l'analyse en temps réel.

2. Dans le champ **Intervalle de temps de la consolidation**, spécifiez le délai maximal devant séparer le premier et le dernier enregistrement à combiner.

Cela représente la plus grande différence de temps entre les enregistrements les plus anciens et les plus récents combinés en un même enregistrement de consolidation.

Réduisez l'intervalle pour accroître la granularité des rapports. Augmentez l'intervalle pour optimiser la consolidation. N'oubliez pas qu'un intervalle plus important peut également accroître l'utilisation des ressources système, telles que la mémoire, le processeur et l'espace disque.

Si vous activez l'option URL complète de la page Génération de rapports > Base de données d'activité (onglet Paramètres) de Websense Manager, l'enregistrement de journal consolidé contiendra le chemin complet (jusqu'à 255 caractères) du premier site correspondant rencontré par Log Server.

Supposons par exemple qu'un utilisateur ait visité les sites suivants, tous classés dans la catégorie Shopping.

- www.domaine.com/chaussures
- www.domaine.com/sacamains
- www.domaine.com/bijoux

Si l'option URL complète est activée, la consolidation crée une seule entrée de journal sous l'URL www.domaine.com/chaussures.

3. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis arrêtez et redémarrez Log Server (voir *Arrêt et démarrage de Log Server*, page 321).

Configuration de WebCatcher

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration des connexions de Log Server*, page 311
- *Configuration des options de base de données de Log Server*, page 312
- *Configuration des fichiers cache du journal*, page 315
- *Configuration des options de consolidation*, page 316
- *Configuration de WebCatcher*, page 318
- *Authentification de WebCatcher*, page 320
- *Arrêt et démarrage de Log Server*, page 321

WebCatcher est une fonction en option qui collecte les URL non reconnues et les URL de sécurité et les envoie à Websense, Inc. afin que les risques potentiels pour la sécurité et la responsabilité légale soient analysés et pour la catégorisation. (La journalisation des URL complètes n'est pas obligatoire pour le traitement de WebCatcher.) Websense, Inc. vérifie les informations et actualise la base de données principale avec les URL nouvellement catégorisées, ce qui améliore le filtrage.

Choisissez les types d'URL à envoyer et définissez la taille des fichiers et le temps de traitement dans l'onglet **WebCatcher** de l'utilitaire de configuration de Log Server.

> **Remarque**
> Dans un environnement composé de plusieurs serveurs Policy Server, WebCatcher est activé pour un seul Log Server. Une fois activé, cet onglet est indisponible lors de l'exécution de l'outil de configuration de Log Server pour d'autres instances de Log Server.

Les informations envoyées à Websense, Inc. ne contiennent que les URL et non des informations sur les utilisateurs.

L'exemple suivant décrit les informations envoyées lorsque WebCatcher est activé. L'adresse IP de cet exemple reflète l'adresse IP de l'ordinateur hébergeant l'URL, pas l'adresse IP du demandeur.

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

Les données de WebCatcher sont envoyées à Websense, Inc. via HTTP. Il vous faudra peut-être créer des rôles ou modifier le serveur proxy ou le pare-feu pour autoriser le trafic HTTP sortant. Reportez-vous à la documentation de votre pare-feu ou du serveur proxy pour obtenir des instructions.

1. Sélectionner l'une des options suivantes :
   - **Oui, envoyer uniquement les URL indiquées à Websense** active le traitement WebCatcher. Vous devez indiquer les URL à envoyer. Passez à l'étape 2.
   - **Non, ne pas envoyer d'informations à Websense** désactive le traitement WebCatcher. Aucune autre entrée n'est nécessaire si vous choisissez cette option.
2. Activez **Envoyer des URL non catégorisées** pour envoyer à Websense, Inc. la liste de toutes les URL non catégorisées présentes dans votre base de données d'activité.

   Websense, Inc. analyse les URL non catégorisées reçues et les ajoute dans la base de données principale, le cas échéant. Cette opération améliore la précision du filtrage pour toutes les organisations.

   > **Remarque**
   > Les sites intranet ne sont pas envoyés par WebCatcher. Cela comprend tous les sites des plages 10.xxx.xxx.xxx, 172.16.xxx.xxx et 192.168.xxx.xxx.

3. Activez **Envoyer des URL de sécurité** pour envoyer la liste de toutes les URL de sécurité présentes dans votre base de données d'activité.

   Les URL de sécurité reçues sont analysées par Websense, Inc. pour déterminer l'activité des sites des catégories Enregistreurs de frappe, Sites Web dangereux, Phishing et autres escroqueries et Logiciels espion.

4. Sous **Sélectionnez le pays reflétant le mieux votre position**, sélectionnez le pays dans lequel la majorité de l'activité est enregistrée.
5. Activez l'option **Enregistrer une copie des données envoyées à Websense** pour enregistrer une copie des données envoyées à Websense, Inc.

   Lorsque cette option est activée, WebCatcher enregistre les données sous forme de fichiers XML non cryptés dans le répertoire Websense\Reporter. Ces fichiers comportent une date et une heure.
6. Sous **Taille maximale du fichier de téléchargement**, indiquez la taille maximale que le fichier peut atteindre (de 4096 Ko à 8192 Ko) avant d'être envoyé à Websense.

   Assurez-vous que votre système peut envoyer un fichier de la taille spécifiée par HTTP.
7. Pour **Heure de début chaque jour (minimum)** , définissez l'heure à partir de laquelle WebCatcher peut envoyer le fichier lorsque la taille limite n'a pas été atteinte ce jour-là.

   Les informations sont ainsi envoyées et effacées de votre système au moins une fois par jour.
8. Cliquez sur le bouton **Authentification** si l'ordinateur Log Server doit s'authentifier pour accéder à Internet.

   Consultez la section *Authentification de WebCatcher*, page 320 pour plus d'informations sur la boîte de dialogue **Authentification**.
9. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis arrêtez et redémarrez Log Server (voir *Arrêt et démarrage de Log Server*, page 321).

Authentification de WebCatcher

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration de WebCatcher*, page 318
- *Arrêt et démarrage de Log Server*, page 321

La boîte de dialogue Authentification apparaît lorsque vous cliquez sur **Authentification** dans l'onglet WebCatcher.

1. Activez l'option **Utiliser un serveur proxy** si l'ordinateur Log Server accède à Internet par l'intermédiaire d'un serveur proxy et fournit ensuite les informations demandées.

Champ	Description
Nom du serveur proxy	Entrez le nom de l'ordinateur ou l'adresse IP du serveur proxy par lequel Log Server accède à Internet.
Port du serveur proxy	Entrez le numéro de port par lequel le serveur proxy communique.

2. Cliquez sur le bouton **Utiliser une authentification de base** si l'ordinateur Log Server doit s'authentifier pour accéder à Internet, puis entrez le nom d'utilisateur et le mot de passe.
3. Cliquez sur **OK** pour enregistrer les modifications et revenir dans l'onglet WebCatcher.

Arrêt et démarrage de Log Server

Rubriques connexes :

- *Utilitaire Configuration de Log Server*, page 310
- *Configuration des connexions de Log Server*, page 311

Log Server reçoit des informations de Filtering Service et les enregistre dans la base de données d'activité en vue de la génération de rapports. Il s'exécute sous forme de service Windows, généralement démarré pendant l'installation, et démarre chaque fois que vous redémarrez l'ordinateur.

Les modifications que vous apportez dans l'utilitaire de configuration de Log Server ne prennent pas effet avant que vous ayez arrêter et redémarrer Log Server. Cette opération peut être effectuée via l'onglet Connexion de l'utilitaire de configuration de Log Server.

1. Dans le menu Démarrer de Windows, sélectionnez **Programmes > Websense > Utilitaires > Configuration de Log Server**.
2. Dans l'onglet **Connexions**, cliquez sur **Arrêter**.
3. Attendez quelques secondes, puis cliquez sur **Démarrer** pour redémarrer le service Log Server.
4. Cliquez sur **OK** pour fermer l'utilitaire de configuration de Log Server.

Remarque

Websense ne peut pas enregistrer les accès Internet survenant pendant l'arrêt de Log Server.

Présentation de la base de données d'activité

Rubriques connexes :

- *Travaux de base de données*, page 322
- *Administration de la base de données d'activité*, page 323

La base de données d'activité (Log Database) stocke les enregistrements de l'activité Internet et les actions de filtrage Websense associées. Elle est créée pendant l'installation avec une base de données de catalogue et une partition de base de données.

La **base de données de catalogue** fournit un unique point de connexion pour les différents composants de Websense qui doivent accéder à la base de données d'activité : pages d'état, Log Server, rapports de présentation et rapports d'investigation. Elle contient des informations sur la prise en charge des partitions de la base de données, y compris la liste des noms de catégorie, les définitions des classes de risque, les correspondances utilisateurs/groupes, les travaux de bases de données, etc. La base de données de catalogue conserve également la liste de toutes les partitions de base de données disponibles.

Les **partitions de base de données** stockent les enregistrements de journal individuels de l'activité Internet. Pour les utilisateurs MSDE, de nouvelles partitions sont créées en fonction des règles de remplacement de taille établies par Websense. Les utilisateurs de Microsoft SQL Server peuvent configurer la base de données d'activité de manière à créer une nouvelle partition en fonction de la taille de la partition ou d'un intervalle de dates (voir *Configuration des options de remplacement*, page 325 pour plus d'informations).

> **Remarque**
> Les partitions à base de dates ne sont disponibles que si Websense utilise Microsoft SQL Server comme moteur de base de données.

Lorsque les partitions sont basées sur la taille, tous les enregistrements de journal entrants sont insérés dans la partition active la plus récente répondant à la règle de taille. Lorsque la partition atteint la taille maximale désignée, une nouvelle partition est créée pour l'insertion des nouveaux enregistrements de journal.

Lorsque les partitions sont basées sur une date, les nouvelles partitions sont créées en fonction du cycle établi. Par exemple, dans le cas d'une option de remplacement mensuelle, une nouvelle partition est créée dès que des enregistrements sont reçus pour le nouveau mois. Les enregistrements de journal entrants sont insérés dans la partition appropriée en fonction de la date.

Les partitions de base de données sont un avantage en termes de souplesse et de performances. Par exemple, vous pouvez générer des rapports à partir d'une seule partition pour limiter l'étendue des données devant être analysées pour localiser les informations demandées.

Travaux de base de données

Les travaux de base de données suivants sont installés en même temps que la base de données d'activité. SQL Server Agent doit s'exécuter sur l'ordinateur qui exécute le moteur de base de données (MSDE ou Microsoft SQL Server).

- La tâche d'extraction, de transformation et de chargement (ETL, Extract, Transform and Load) s'exécute en permanence, en recevant les données de Log Server pour ensuite les traiter et les insérer dans la base de données de partitions. Le travail ETL doit s'exécuter pour traiter les enregistrements de journal dans la base de données d'activité.
- Le travail de maintenance de base de données exécute des tâches de maintenance de base de données et préserve les performances optimales. Par défaut, ce travail s'exécute la nuit.
- Le travail de temps de navigation Internet (IBT) analyse les données reçues et calcule le temps de navigation pour chaque client. Le travail de base de données IBT consomme beaucoup de ressources et affecte la plupart des ressources de base de données. Par défaut, ce travail s'exécute la nuit.

Certains aspects de ces travaux de base de données peuvent être configurés dans la page Paramètres > Base de données d'activité. Pour plus d'informations, consultez *Paramètres d'administration de la base de données d'activité*, page 324.

Lorsque vous configurez l'heure de début des travaux de maintenance et de temps de navigation Internet, tenez compte des ressources système et du trafic réseau. Ces travaux consomment beaucoup de ressources et peuvent ralentir les performances de la journalisation et de la génération de rapports.

Administration de la base de données d'activité

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Configuration des partitions disponibles*, page 332
- *Affichage des journaux d'erreurs*, page 334

L'administration de la base de données d'activité consiste à contrôler la plupart des aspects des opérations de base de données, y compris :

- Les opérations exécutées par les travaux de base de données et le moment de leur exécution
- Les conditions de création de nouvelles partitions de base de données
- Les partitions disponibles pour la génération de rapports

Ces options, et d'autres, donnent un contrôle important à l'administrateur de la base de données d'activité. Voir *Paramètres d'administration de la base de données d'activité*, page 324.

Le Super administrateur désigne la personne qui administre la base de données d'activité lors de la création des rôles. Voir *Modification des rôles*, page 257.

> **Remarque**
> Il est préférable de limiter le nombre d'administrateurs autorisés à modifier les paramètres de la base de données d'activité.

Paramètres d'administration de la base de données d'activité

Rubriques connexes :

- *Administration de la base de données d'activité*, page 323

La page **Génération de rapports > Base de données d'activité**, accessible depuis l'onglet Paramètres, permet de gérer les différents aspects des opérations de la base de la base d'activité. Les options sont regroupées en sections logiques décrites séparément.

Pour activer les modifications apportées à une section, vous devez cliquer sur le bouton Enregistrer maintenant de cette section. Un clic sur le bouton **Enregistrer maintenant** enregistre immédiatement les modifications de cette section. (Il n'est pas nécessaire de cliquer également sur Enregistrer tout.)

Le haut de la page présente le nom de la base de données d'activité active et un lien **Actualiser**. Ce lien Actualiser affiche de nouveau les informations actuellement présentes dans la page Base de données d'activité. Toutes les modifications qui n'ont pas été appliquées via le bouton 'Enregistrer maintenant' approprié sont perdues.

Pour obtenir des instructions détaillées sur l'utilisation de chaque section, cliquez sur le lien approprié ci-dessous.

- Options de remplacement de la base de données : *Configuration des options de remplacement*, page 325.
- Enregistrement d'URL complète : *Configuration de la journalisation des URL complètes*, page 326.
- Configuration du temps de navigation sur Internet : *Configuration des options du temps de navigation sur Internet*, page 328.
- Configuration de la maintenance : *Configuration des options de maintenance de la base de données d'activité*, page 329.
- Création d'une partition de base de données : *Configuration de la création de partitions pour la base de données d'activité*, page 331.
- Partitions disponibles : *Configuration des partitions disponibles*, page 332.

- Activité du journal d'erreurs : *Affichage des journaux d'erreurs*, page 334.

Configuration des options de remplacement

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Configuration des partitions disponibles*, page 332
- *Affichage des journaux d'erreurs*, page 334

La section **Options de remplacement de la base de données** de la page Génération de rapports > Base de données d'activité (onglet Paramètres) vous permet de spécifier à quel moment la Base de données d'activité doit créer une nouvelle partition de base de données (remplacement).

1. Utilisez les options **Remplacer chaque** pour indiquer si les partitions de base de données doivent être remplacées en fonction de la taille (Mo) ou de la date (semaines ou mois), selon le moteur de base de données utilisé.

   Les utilisateurs MSDE doivent utiliser l'option de remplacement basée sur la taille. Les utilisateurs de Microsoft SQL Server ont le choix entre la taille et la date.

   - Dans le cas de remplacements basés sur la date, sélectionnez l'unité de mesure,**semaines** ou **mois**, puis indiquez le nombre de semaines ou de mois de conservation d'une partition de base de données avant la création d'une nouvelle partition.
   - Pour les remplacements basés sur la taille, sélectionnez **Mo** et définissez le nombre de méga-octets que la base de données doit atteindre avant que le remplacement ne commence.

     Les utilisateurs de **Microsoft SQL Server** peuvent définir une taille maximale de 204 800 Mo.

Les utilisateurs **MSDE** doivent définir une taille comprise entre 100 et 1 536 Mo.

Remarque

Si le remplacement commence au cours de l'une des périodes de pointe de la journée, le processus peut ralentir les performances.

Pour contourner le problème, certains environnements choisissent de définir un remplacement automatique sur une longue période ou sur une taille maximale, puis effectuent des remplacements manuels réguliers pour éviter que le remplacement automatique ne se produise. Pour plus d'informations sur les remplacements manuels, consultez la section *Configuration de la création de partitions pour la base de données d'activité*, page 331.

N'oubliez pas que les partitions individuelles très volumineuses ne sont pas conseillées. En effet, si les données ne sont pas divisées en plusieurs partitions plus petites, les performances de la génération de rapports peuvent diminuer.

Lors de la création d'une nouvelle partition de base de données, la génération de rapports est automatiquement activée pour la partition (voir *Configuration des partitions disponibles*, page 332).

2. Cliquez sur **Enregistrer maintenant** pour activer les modifications apportées aux options de remplacement de la base de données.

Configuration de la journalisation des URL complètes

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Configuration des partitions disponibles*, page 332
- *Affichage des journaux d'erreurs*, page 334

La section **Enregistrement d'URL complète** de la page Génération de rapports > Base de données d'activité (onglet Paramètres) vous permet de choisir la partie de l'URL enregistrée pour chaque requête Internet.

> **Remarque**
> La gestion de la taille de la base de données d'activité est essentielle pour les réseaux à fort trafic. La désactivation de l'option 'Enregistrement d'URL complète' est une manière de contrôler la taille et la croissance de la base de données.

1. Cochez la case **Enregistrer l'URL complète de chaque site demandé** pour enregistrer l'URL complète, y compris le domaine (www.domaine.com) et le chemin d'accès de la page (/produits/produitA.html).

   > **Important**
   > Si vous prévoyez de créer des rapports sur l'activité d'analyse en temps réel, activez la journalisation des URL complètes (voir *Création de rapports sur l'activité d'analyse en temps réel*, page 153), Sinon les rapports ne pourront afficher que le domaine (www.domaine.com) du site catégorisé, même si les pages individuelles d'un site appartiennent à des catégories différentes ou contiennent des menaces différentes.

   Si cette option n'est pas activée, seuls les noms de domaine sont enregistrés. Il en résulte une base de données plus petite, mais moins de détails.

   La journalisation des URL complètes augmente la taille de la base de données d'activité mais offre plus de détails.

   Si vous activez la journalisation des URL complètes alors que la consolidation est active, l'enregistrement consolidé contient l'URL complète du premier enregistrement du groupe de consolidation. Pour plus d'informations, consultez *Configuration des options de consolidation*, page 316.

2. Cliquez sur **Enregistrer maintenant** pour activer les modifications apportées aux options de journalisation des URL complètes.

Configuration des options du temps de navigation sur Internet

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Configuration des partitions disponibles*, page 332
- *Affichage des journaux d'erreurs*, page 334

Les rapports du Temps de navigation sur Internet (IBT) donnent un aperçu du temps passé par les utilisateurs sur Internet. Un travail de base de données exécuté pendant la nuit calcule le temps de navigation de chaque client sur la base des nouveaux enregistrements de journal reçus au cours de la journée. Définissez les options de temps de navigation dans la section **Configuration du temps de navigation sur Internet** de la page Paramètres > Base de données d'activité.

1. Choisissez l'**Heure de début du travail** de base de données IBT.

   Le temps et les ressources système requis pour ce travail dépendent du volume de données enregistrées chaque jour. Il est préférable de ne pas exécuter ce travail en même temps que le travail de maintenance nocturne (voir *Configuration des options de maintenance de la base de données d'activité*, page 329) et de sélectionner un moment de faible activité sur le réseau afin de minimiser l'impact sur la génération de rapports.

   Le travail de base de données IBT consomme beaucoup de ressources et affecte la plupart des ressources de base de données. Si vous activez ce travail, définissez l'heure de début de manière à ne pas interférer avec les capacités du système de base de données à traiter les rapports planifiés et d'autres opérations importantes. De même, surveillez le travail afin de déterminer si un matériel plus robuste permettrait de mieux répondre à l'ensemble des besoins du traitement.

2. Pour **Seuil de temps de lecture**, définissez un nombre moyen de minutes pour la lecture d'un site Web spécifique.

   Le seuil de temps de lecture définit les sessions de navigation en vue des rapports de temps de navigation sur Internet. L'ouverture d'un navigateur génère du trafic HTTP. Cela représente le début d'une session de navigation. La session reste ouverte tant que du trafic HTTP est généré de façon continue au cours de

l'intervalle de temps défini ici. La session de navigation est considérée comme fermée dès que ce délai s'écoule sans trafic HTTP. Une nouvelle session de navigation commence dès que du trafic HTTP est à nouveau généré.

> **Remarque**
>
> Il est préférable de ne modifier le Seuil de temps de lecture qu'aussi rarement que possible et de créer une nouvelle partition de base de données chaque fois que vous le modifiez.
>
> Pour ne pas obtenir d'incohérences dans les rapports, générez les rapports IBT à partir de partitions de base de données utilisant la même valeur de Seuil de temps de lecture.

N'oubliez pas que certains sites Web utilisent l'actualisation automatique pour fréquemment mettre à jour les informations. Un site d'actualités qui rajoute régulièrement les dernières infos à l'affichage en est un exemple. Cette actualisation génère un nouveau trafic HTTP. De ce fait, lorsque ce type de site reste ouvert, de nouveaux enregistrements de journal sont générés à chaque actualisation du site. Le trafic HTTP ne s'interrompt pas suffisamment longtemps pour que la session de navigation se ferme.

3. Définissez une valeur **Dernier temps de lecture** pour connaître le temps passé à lire le dernier site avant la fin d'une session de navigation.

   Lorsque le délai d'inactivité du trafic HTTP est supérieur au Seuil de temps de lecture, la session est interrompue et la valeur du Dernier temps de lecture est ajoutée au temps de session.
4. Cliquez sur **Enregistrer maintenant** pour activer les modifications apportées à la configuration du temps de navigation sur Internet.

Configuration des options de maintenance de la base de données d'activité

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Configuration des partitions disponibles*, page 332
- *Affichage des journaux d'erreurs*, page 334

Utilisez la section **Configuration de la maintenance** de la page Génération de rapports > Base de données d'activité (onglet Paramètres) pour contrôler certains aspects du traitement de la base de données, par exemple l'heure d'exécution du travail de maintenance, certaines de ses tâches, et la suppression des partitions et des journaux d'erreurs.

1. Pour **Heure de début de la maintenance**, sélectionnez l'heure d'exécution du travail de maintenance de la base de données.

   Le temps et les ressources système requis pour ce travail dépendent des tâches sélectionnées dans cette section. Pour minimiser l'impact sur les autres activités et systèmes, il est préférable d'exécuter ce travail pendant l'une des périodes de faible activité du réseau, et pas en même temps que le travail IBT (voir *Configuration des options du temps de navigation sur Internet*, page 328).

2. Cochez l'option **Supprimer automatiquement des partitions si tous les jours de la partition sont antérieurs à ce nombre de jours** , puis spécifiez le nombre de jours (entre 2 et 365) devant s'écouler avant que les partitions ne soient supprimées.

   Avertissement

   Lorsqu'une partition a été supprimée, ses données ne peuvent pas être récupérées. Consultez la section *Configuration des partitions disponibles*, page 332 pour découvrir une autre façon de supprimer des partitions.

3. Cochez l'option **Activer la réindexation automatique des partitions lorsque nécessaire chaque**, puis sélectionnez le jour où cette opération doit s'effectuer automatiquement chaque semaine.

   La réindexation de la base de données est importante pour l'intégrité de la base de données et l'optimisation de la vitesse de création des rapports.

   Important

   Il est préférable d'exécuter cette opération au cours de l'une des périodes de faible activité du réseau. La réindexation des partitions de base de données consomme beaucoup de ressources et prend un certain temps. Il est donc également préférable de ne pas exécuter de rapports pendant cette opération.

4. Activez l'option **Nombre de jours avant la suppression des lots ayant échoué** et entrez un nombre de jours (compris entre 0 et 90) devant s'écouler avant la suppression des lots ayant échoué.

   Si cette option n'est pas activée, les lots ayant échoué sont conservés indéfiniment pour le traitement futur.

   Lorsque l'espace disque est insuffisant ou lorsque les autorisations de base de données ne permettent pas d'insérer des enregistrements de journal dans la base de données, les enregistrements sont désignés en tant que **lots ayant échoué**. En général, ces lots sont ensuite retraités et insérés avec succès dans la base de données grâce au travail de maintenance de base de données nocturne.

Toutefois, ce nouveau traitement ne peut réussir si le problème d'espace disque ou d'autorisation n'a pas été résolu. De plus, si l'option **Traiter les lots non traités** n'est pas activée, les lots en échec ne sont jamais retraités, mais sont supprimés lorsque le délai défini ici est écoulé.

5. Pour que le travail de maintenance de base de données nocturne traite à nouveau les lots ayant échoué, activez l'option **Traiter les lots non traités**.

   Si cette option n'est pas activée, les lots ayant échoué ne sont jamais retraités, mais sont éventuellement supprimés lorsque le délai défini ici est écoulé.

6. Activez l'option **Nombre de jours avant la suppression du journal d'erreurs** et entrez le nombre de jours (compris entre 0 et 90) devant s'écouler avant la suppression des enregistrements d'erreur de la base de données dans la base de données de catalogue.

   Si cette option n'est pas activée, les journaux d'erreurs sont conservés indéfiniment.

7. Cliquez sur **Enregistrer maintenant** pour activer les modifications apportées aux options de configuration de la maintenance.

Configuration de la création de partitions pour la base de données d'activité

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration des partitions disponibles*, page 332
- *Affichage des journaux d'erreurs*, page 334

La section **Création d'une partition de base de données** de la page Génération de rapports > Base de données d'activité (onglet Paramètres) permet de définir les caractéristiques des nouvelles partitions de base de données, par exemple les options d'emplacement et de taille. Cette section permet également de créer directement une nouvelle partition au lieu d'attendre le remplacement prévu (voir *Configuration des options de remplacement*, page 325).

1. Entrez le **Chemin du fichier** permettant de créer des fichiers de **Données** et de **Journal** pour les nouvelles partitions de la base de données.
2. Sous **Taille init**, définissez la taille initiale des fichiers (de 100 à 204 800 Mo) de **Données** et **Journal** pour les nouvelles partitions de la base de données.

   Utilisateurs Microsoft SQL Server : la fourchette acceptable est comprise entre 100 et 204 800.

Utilisateurs MSDE : la fourchette acceptable est comprise entre 100 et 1 500.

> **Remarque**
> Les meilleures pratiques consistent à calculer une taille de partition moyenne pour une période et de définir ensuite la taille initiale sur cette valeur. Cette approche réduit la fréquence des développements de la partition et libère des ressources pour le traitement des données au sein des partitions.

3. Sous **Croissance**, définissez l'incrément par lequel la taille les fichiers de **Données** et **Journal** d'une partition doit augmenter, en méga-octets (Mo), lorsque de l'espace supplémentaire est requis.

   Utilisateurs Microsoft SQL Server : la fourchette acceptable est comprise entre 1 et 999 999.

   Utilisateurs MSDE : la fourchette acceptable est comprise entre 1 et 450.
4. Cliquez sur **Enregistrer maintenant** pour implémenter les modifications apportées aux chemins d'accès, à la taille et aux options de croissance.

   Les partitions de base de données créées après ces modifications utilisent les nouveaux paramètres.
5. Cliquez sur **Créer maintenant** pour créer une nouvelle partition lors des prochaines exécutions du travail ETL (voir *Travaux de base de données*, page 322), quels que soient les paramètres du remplacement automatique. Ce processus prend généralement quelques minutes.

   Pour que la nouvelle partition utilise les modifications apportées dans cette section, n'oubliez pas de cliquer sur **Enregistrer maintenant** avant de cliquer sur **Créer maintenant**.

   Cliquez régulièrement sur le lien Actualiser du panneau de contenu. Lorsque le processus de création est terminé, la section Partitions disponibles présente la nouvelle partition.

Configuration des partitions disponibles

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Affichage des journaux d'erreurs*, page 334

La section **Partitions disponibles** de la page Génération de rapports > Base de données d'activité (onglet Paramètres) présente la liste de toutes les partitions de base de données disponibles pour la génération des rapports. La liste présente les dates couvertes, de même que la taille et le nom de chaque partition.

Servez-vous de cette liste pour contrôler les partitions de base de données devant être incluses dans les rapports et pour sélectionner des partitions individuelles à supprimer.

1. Cochez l'option **Activer** accolée à chaque partition à inclure dans les rapports.

   Servez-vous éventuellement des options **Toutes** et **Aucune** situées au-dessus de la liste.

   Vous devez activer au moins une partition pour la génération des rapports. Servez-vous de l'option **Aucune** pour désactiver simultanément toutes les partitions avant de n'en activer que quelques-unes.

   Ces options permettent de gérer la quantité de données analysées lors de la génération des rapports et leur vitesse de traitement. Par exemple, si vous envisagez de générer une série de rapports pour le mois de juin, désactivez toutes les partitions à l'exception de celles contenant des dates correspondant au mois de juin.

   Important

   Cette section affecte les rapports planifiés et les rapports exécutés de façon interactive. Pour éviter de générer des rapports ne contenant aucune donnée, assurez-vous que les partitions appropriées soient activées lorsque l'exécution des rapports est planifiée.

2. Cliquez sur l'option **Supprimer** accolée au nom de la partition lorsque celle-ci n'est plus nécessaire. La partition sera alors supprimée lors de la prochaine exécution du travail de maintenance de la base de données nocturne.

   Avertissement

   Servez-vous de cette option avec précaution car les partitions supprimées ne peuvent pas être récupérées.

   La suppression des partitions obsolètes minimise le nombre de partitions présentes dans la base de données d'activité, ce qui améliore les performances de cette dernière et de la génération des rapports. Servez-vous aux besoins de l'option Supprimer pour effacer des partitions individuelles. Si vous préférez supprimer les anciennes partitions en fonction d'un planning défini, consultez la section *Configuration des options de maintenance de la base de données d'activité*, page 329.

3. Cliquez sur **Enregistrer maintenant** pour activer les modifications apportées aux options de partitions disponibles.

Affichage des journaux d'erreurs

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 324
- *Configuration des options de remplacement*, page 325
- *Configuration des options du temps de navigation sur Internet*, page 328
- *Configuration de la journalisation des URL complètes*, page 326
- *Configuration des options de maintenance de la base de données d'activité*, page 329
- *Configuration de la création de partitions pour la base de données d'activité*, page 331
- *Configuration des partitions disponibles*, page 332

La section **Activité du journal d'erreurs** de la page Génération de rapports > Base de données d'activité (onglet Paramètres) permet d'afficher les enregistrements des erreurs survenues au cours des travaux exécutés sur la base de données d'activité Websense (voir *Travaux de base de données*, page 322). Ces informations peuvent se révéler très utiles pour le dépannage.

Choisissez l'une des options suivantes :

- Choisissez un nombre dans la liste déroulante pour afficher ce nombre d'entrées du journal d'erreurs.
- Choisissez **Afficher tout** pour afficher toutes les entrées du journal d'erreurs.
- Choisissez **Afficher aucune** pour masquer toutes les entrées du journal d'erreurs.

Configuration des rapports d'investigation

Rubriques connexes :

- *Connexion à la base de données et paramètres par défaut des rapports*, page 335
- *Options d'affichage et de sortie*, page 337

Les rapports d'investigation vous permettent de rechercher des informations sur l'utilisation Internet de votre organisation de façon interactive. Voir *Rapports d'investigation*, page 118.

Le lien Options de la page principale des rapports d'investigation permet de choisir quelle base de données d'activité est utilisée pour la génération des rapports. Il permet également de modifier l'affichage par défaut des rapports détaillés. Voir *Connexion à la base de données et paramètres par défaut des rapports*, page 335.

Le fichier **wse.ini** permet de configurer certains paramètres par défaut liés à l'affichage des rapports résumés et des rapports multi-niveaux. Il permet également de mieux contrôler la taille des pages par défaut utilisées lors de la publication d'un rapport au format PDF. Voir *Options d'affichage et de sortie*, page 337.

Connexion à la base de données et paramètres par défaut des rapports

Rubriques connexes :

- *Configuration des rapports d'investigation*, page 334
- *Options d'affichage et de sortie*, page 337
- *Rapports résumés*, page 120
- *Rapports résumés multi-niveaux*, page 124

Utilisez la page **Rapports d'investigation > Options** pour vous connecter à la base de données d'activité désirée et contrôler les paramètres par défaut de l'affichage détaillé des rapports d'investigation.

Les modifications apportées dans cette page affectent vos rapports. Les autres administrateurs, de même que les utilisateurs enregistrés pour la journalisation sur leur activité propre, peuvent modifier ces valeurs pour leurs propres activités de génération de rapports.

1. Choisissez la base de données d'activité à utiliser pour les rapports d'investigation.
   - Activez l'option **Afficher la base de données de catalogue** pour vous connecter à la base de données d'activité dans laquelle Log Server effectue la journalisation. Passez à l'étape 2.
   - Pour accéder à une autre base de données d'activité :
     a. Désactivez l'option **Afficher la base de données de catalogue**.
     b. Entrez les informations suivantes pour identifier la base de données d'activité désirée. (Les rapports d'investigation peuvent être générés à partir d'une base de données v6.3.x ou v7.0.)

Champ	Description
Serveur	Entrez le nom ou l'adresse IP de l'ordinateur sur lequel la base de données d'activité est stockée.
Base de données	Entrez le nom de la base de données d'activité.

Champ	Description
ID utilisateur	Entrez l'ID utilisateur d'un compte autorisé à accéder à la base de données. Ne renseignez pas ce champ si Log Server a été installé pour utiliser une connexion sécurisée pour accéder à la base de données d'activité. Si vous avez des doutes, entrez **sa**. Il s'agit de l'ID utilisateur par défaut pour MSDE et de l'ID de l'administrateur par défaut dans Microsoft SQL Server.
Mot de passe	Entrez le mot de passe associé à l'ID utilisateur spécifié. Dans le cas d'une connexion sécurisée, ne renseignez pas ce champ.

2. Sélectionnez les paramètres par défaut suivants pour les rapports détaillés.

Champ	Description
Sélectionnez l'intervalle de dates des rapports d'investigation par défaut.	Choisissez la plage de dates pour l'affichage initial des rapports résumés.
Sélectionnez le format de rapport détaillé par défaut	Choisissez **Sélection intelligente de colonnes** pour afficher les rapports détaillés avec ses colonnes par défaut définies pour les informations rapportées. Choisissez **Sélection personnalisée de colonnes** pour définir avec précision les colonnes de l'affichage initial de tous les rapports détaillés. Servez-vous de la liste Colonnes disponibles pour effectuer vos sélections. Les utilisateurs pourront modifier les colonnes affichées après avoir généré le rapport.
Type de rapport	Indiquez si les rapports détaillés doivent initialement présenter : • **Détail** : chaque enregistrement s'affiche sur une ligne distincte ; l'heure peut être affichée. • **Résumé** : regroupe en une seule entrée tous les enregistrements qui partagent un élément commun. L'élément spécifique varie en fonction des informations utilisées dans le rapport. En général, la colonne située immédiatement à droite avant la mesure présente l'élément résumé. L'heure ne peut pas être affichée.
Colonnes disponibles / Rapport en cours	Sélectionnez un nom de colonne dans la liste Colonnes disponibles et cliquez sur la flèche appropriée pour le déplacer vers la liste Rapport en cours. La liste Rapport en cours peut contenir jusqu'à 7 colonnes. Une fois que la liste Rapport en cours contient toutes les colonnes des rapports détaillés initiaux, définissez l'ordre des colonnes. Sélectionnez une entrée dans la liste et utilisez les boutons vers le haut et vers le bas pour en modifier la position.

3. Cliquez sur **Enregistrer les options** pour enregistrer immédiatement toutes les modifications.

Options d'affichage et de sortie

Rubriques connexes :

- *Configuration des rapports d'investigation*, page 334
- *Connexion à la base de données et paramètres par défaut des rapports*, page 335
- *Sortie dans un fichier*, page 142

Vous pouvez ajuster la façon dont certains choix et résultats de rapports apparaissent dans les rapports d'investigation résumés et multi-niveaux. Vous pouvez également spécifier la taille par défaut des pages lorsque les rapports sont publiés au format PDF.

Ces options de configuration des rapports d'investigation sont définies dans le fichier **wse.ini**. L'emplacement par défaut est :

```
C:\Program Files\Websense\webroot\Explorer\wse.ini
```

Le tableau suivant présente la liste des paramètres qui affectent l'affichage et la sortie des rapports d'investigation, ce qu'ils contrôlent et leur valeur par défaut. (Ne modifiez AUCUN autre paramètre du fichier wse.ini.)

Paramètre	Description
maxUsersMenu	La base de données doit comprendre moins d'utilisateurs que cette valeur (par défaut, 5 000) pour afficher Utilisateur en tant que choix de rapport dans la liste Utilisation d'Internet par.
maxGroupsMenu	La base de données doit comprendre moins de groupes que cette valeur (par défaut, 3 000) pour afficher Groupe en tant que choix de rapport dans la liste Utilisation d'Internet par. **Remarque :** pour que Groupe apparaisse dans la liste Utilisation d'Internet par, plusieurs groupes doivent exister. De même, pour que Domaine apparaisse dans la liste Utilisation d'Internet par, plusieurs domaines doivent exister. Il n'existe pas de valeur maximale pour les domaines.

Paramètre	Description
maxUsersDrilldown	Ce paramètre fonctionne avec le paramètre warnTooManyHits pour contrôler les moments où l'option Utilisateur doit s'afficher en rouge. L'affichage en rouge indique que le choix de l'option Utilisateur entraîne la production d'un rapport très volumineux dont l'exécution peut être longue. Si le nombre d'utilisateurs est supérieur à cette valeur (par défaut, 5 000), et le nombre d'accès supérieur à la valeur warnTooManyHits, l'option Utilisateur s'affiche en rouge dans les différentes listes déroulantes et de valeurs. Si le nombre d'utilisateurs est supérieur à cette valeur mais que le nombre d'accès est inférieur à la valeur warnTooManyHits, l'option Utilisateur s'affiche dans sa couleur habituelle, le rapport produit étant de taille plus raisonnable.
maxGroupsDrilldown	L'option Groupe s'affiche en rouge pendant l'exploration verticale si le nombre de groupes est supérieur à ce nombre dans le rapport proposé (par défaut, 2 000). L'affichage en rouge indique que le choix de l'option Groupe entraîne la production d'un rapport très volumineux dont l'exécution peut être longue.
warnTooManyHits	Ce paramètre fonctionne avec le paramètre maxUsersDrilldown pour contrôler le moment où l'option Utilisateur doit s'afficher en rouge. Si le nombre d'utilisateurs est supérieur à la valeur maxUsersDrilldown, mais que le nombre d'accès est inférieur à cette valeur (par défaut, 10 000), l'option Utilisateur ne s'affiche *pas* en rouge. Si le nombre d'utilisateurs est supérieur à la valeur maxUsersDrilldown et que le nombre d'accès est supérieur à cette valeur, l'option Utilisateur s'affiche en rouge. L'affichage en rouge indique que le choix de l'option Utilisateur entraîne la production d'un rapport très volumineux dont l'exécution peut être longue.
hitsPerPage	Ce paramètre détermine le nombre maximal d'éléments (par défaut, 100) affichés par page. (Ce paramètre n'affecte pas les rapports imprimés.)
maxOutputBufferSize	Ce paramètre correspond à la quantité maximale de données (en octets) pouvant être affichée sur la page principale des rapports d'investigation. Si les données demandées dépassent cette limite (par défaut 4 000 000, ou 4 millions d'octets), un message apparaît en rouge à la fin du rapport pour indiquer que certains résultats ne sont pas affichés. Si cela pose un problème, des valeurs supérieures permettent d'afficher une plus grande quantité de données dans un rapport. Toutefois, si des erreurs de mémoire surviennent, pensez à réduire cette valeur.

Paramètre	Description
sendMulti	Cette option est désactivée (0) par défaut. Définissez-la sur 1 (activée) pour diviser les très grands rapports détaillés planifiés en plusieurs fichiers de 10 000 lignes chacun. Les fichiers représentant un même rapport sont compressés et envoyés aux destinataires par courrier électronique. Les fichiers du rapport peuvent ensuite être extraits avec des utilitaires de compression courants.
maxSlices	Ce paramètre correspond au nombre maximal de secteurs distincts (par défaut, 6) d'un graphique en secteurs, y compris le secteur Autre, qui combine toutes les valeurs non représentées dans des secteurs individuels.
timelineCompressionThreshold	Cette option est utilisée uniquement pour l'Activité utilisateur par jour ou par mois, lorsque l'option 'Regrouper les accès similaires/Afficher tous les accès' est disponible. Le rapport réduit tous les accès de la même catégorie survenant au cours du nombre de secondes définies ici (par défaut, 10).
PageSize	Pour simplifier la diffusion ou l'impression, les rapports d'investigation peuvent être publiés au format PDF (Portable Document Format). La taille des pages (par défaut, Lettre) peut être : • A4 (21,59 x 27,49 cm) • Lettre (21,59 x 27,94 cm)

Rapports sur activité propre

Rubriques connexes :

- *Configuration des préférences de génération de rapports*, page 308
- *Rapports sur activité propre*, page 144
- *Rapports d'investigation*, page 118

Vous pouvez activer cette fonction pour permettre aux utilisateurs d'afficher des rapports d'investigation sur leur propre activité Internet. Cela leur permet de voir quels types d'informations sont collectés à leur propos, afin de respecter la législation en vigueur dans la plupart des pays. De plus, l'affichage de leur propre activité peut

encourager certains utilisateurs à modifier leurs habitudes de navigation afin de respecter la politique Internet de l'organisation.

> **Remarque**
> La fonction de rapport sur l'activité propre n'est disponible que si Websense Manager et les composants de génération de rapports sont installés sur un système d'exploitation Windows. Reportez-vous au *Guide de déploiement* pour plus d'informations.

Pour activer la fonction de rapport sur activité propre :

1. Ouvrez la page **Paramètres > Général > Services d'annuaire** et configurez le service d'annuaire utilisé pour authentifier les utilisateurs qui accèdent à Websense Manager avec leurs identifiants réseau. Il est possible que cette opération ait déjà été effectuée précédemment pour activer le filtrage par noms d'utilisateur et de groupe. Voir *Services d'annuaire*, page 63.

   Si votre installation comprend plusieurs serveurs Policy Server, vous devez vous connecter à chacun d'eux et configurer la page Services d'annuaire avec les informations destinées au service d'annuaire approprié.
2. Ouvrez la page **Paramètres > Génération de rapports > Préférences** et cochez la case **Permettre aux utilisateurs de générer des rapports sur leur propre activité**. Voir *Configuration des préférences de génération de rapports*, page 308.

Après avoir activé cette option, assurez-vous de fournir aux utilisateurs les informations dont ils ont besoin pour exécuter les rapports :

- L'URL permettant d'accéder à l'interface de rapport sur activité propre. Rappelez aux utilisateurs qu'ils peuvent enregistrer l'URL sous forme de favori ou de signet en vue d'une utilisation future.

  Voir ci-dessous pour obtenir des informations détaillées sur l'URL.
- Le serveur Policy Server à sélectionner lors de la connexion.

  Lorsque le réseau ne comprend qu'un serveur Policy Server, cela n'est pas nécessaire. Si votre réseau comprend plusieurs serveurs Policy Server, donnez aux utilisateurs l'adresse IP de celui qui est configuré pour communiquer avec le service d'annuaire qui authentifie leur connexion réseau. Il s'agit également du serveur Policy Server spécifié lors de l'installation de Log Server.
- Le nom d'utilisateur et le mot de passe à utiliser pour la connexion.

  Les utilisateurs du rapport sur l'activité propre doivent saisir leur nom d'utilisateur et leur mot de passe réseau lors de la connexion.

L'**URL** permettant d'accéder à l'interface des rapports sur activité propre est :

```
https://<IPserveur>:9443/mng/login/pages/
   selfReportingLogin.jsf
```

Remplacez <IPserveur>, par l'adresse IP de l'ordinateur exécutant Websense Manager.

Les administrateurs et les utilisateurs peuvent également accéder à la page de connexion des rapports sur activité propre en ouvrant la page de connexion de Websense Manager et en cliquant sur le lien Rapports sur activité propre.

Si votre réseau comprend **plusieurs serveurs Policy Server**, vous devez indiquer aux utilisateurs celui qu'ils doivent choisir lors de la connexion aux rapports sur activité propre.

14 Configuration du réseau

Rubriques connexes :

- *Configuration matérielle*, page 344
- *Configuration de Network Agent*, page 345
- *Vérification de la configuration de Network Agent*, page 352

Lorsque vous exécutez Websense en mode autonome (sans intégration à un proxy ou un pare-feu), Websense Network Agent permet d'effectuer les opérations suivantes :

- Le filtrage du contenu Internet
- La gestion des protocoles réseau et des applications Internet
- La gestion de la bande passante
- La journalisation du volume d'octets transféré

Dans un déploiement intégré de Websense, un produit tiers peut gérer l'acheminement des requêtes des utilisateurs vers Websense pour le filtrage et le renvoi des pages de blocage vers le client. Dans cet environnement, Network Agent peut tout de même être utilisé pour filtrer les requêtes non HTTP, fournir plus de détails sur la journalisation ou les deux.

Network Agent surveille en permanence l'utilisation globale du réseau, y compris les octets transférés via le réseau. L'agent envoie des résumés d'utilisation à Websense à intervalles prédéfinis. Chaque résumé comprend l'heure de début et de fin, l'ensemble des octets transférés et les octets utilisés par protocole.

Par défaut, Network Agent fournit également des données d'utilisation de la bande passante à Policy Server et des données de journalisation du filtrage au service Filtering Service.

Network Agent est généralement configuré de manière à voir tout le trafic du réseau. Il distingue :

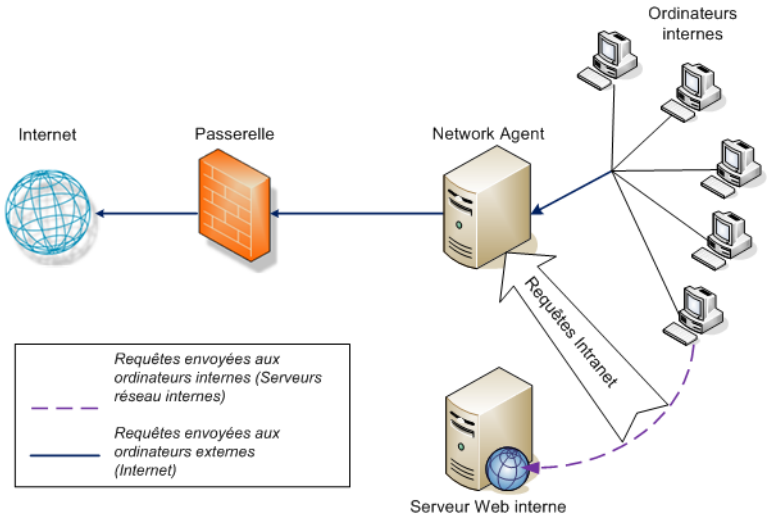
- Les requêtes envoyées par des ordinateurs internes à des ordinateurs internes (accès à un serveur intranet, par exemple)
- Les requêtes envoyées par des ordinateurs internes à des ordinateurs externes (requêtes Internet d'utilisateur, par exemple)

Ces dernières constituent le principal problème dans la surveillance de l'utilisation Internet par les employés.

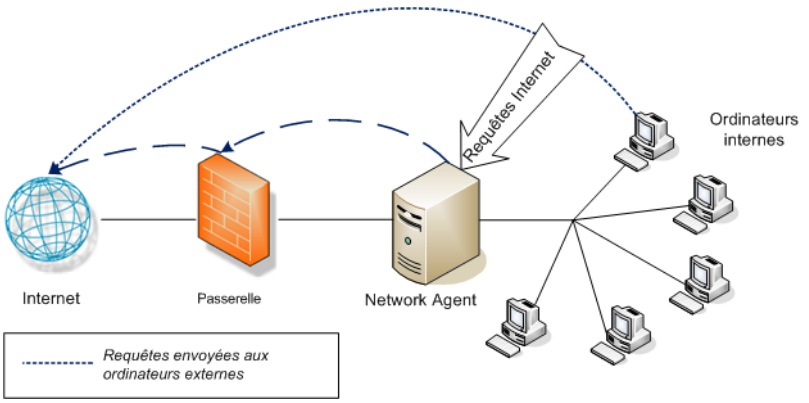
Configuration matérielle

Chaque instance de Network Agent surveille le trafic **provenant** des ordinateurs identifiés comme appartenant à votre réseau. Par défaut, il surveille uniquement le trafic **destiné** aux ordinateurs internes que vous spécifiez (par exemple, les serveurs Web internes).

Vous pouvez choisir quels ordinateurs internes (segments réseau) sont surveillés par chaque instance de Network Agent, ou même par chaque carte réseau sur un ordinateur Network Agent.



Surveillance des requêtes envoyées aux ordinateurs internes



Surveillance des requêtes envoyées aux ordinateurs externes

Chaque instance de Network Agent doit :

- Être placée de façon appropriée dans le réseau afin de détecter le trafic destiné à tous les ordinateurs surveillés et qui en provient.
- Disposer d'au moins 1 carte réseau dédiée à la surveillance du trafic.

Network Agent peut être installé sur un ordinateur équipé de plusieurs cartes réseau et peut utiliser plusieurs cartes réseau pour surveiller les requêtes et envoyer les pages de blocage. Si vous ajoutez une nouvelle carte réseau dans l'ordinateur Network Agent, redémarrez le service Network Agent, puis configurez la nouvelle carte (voir *Configuration des paramètres des cartes réseau*, page 349).

> **Remarque**
> Pour vérifier que Network Agent peut voir le trafic d'un segment du réseau, employez l'utilitaire Détecteur de trafic réseau. Voir *Vérification de la configuration de Network Agent*, page 352.

Pour plus d'informations sur le placement de Network Agent et les exigences relatives aux cartes réseau, reportez-vous au *Guide de déploiement*.

Pour plus d'informations sur la configuration de Network Agent pour la surveillance des requêtes réseau internes, l'utilisation de cartes réseau spécifiques et la journalisation améliorée, consultez la section *Configuration de Network Agent*, page 345.

Configuration de Network Agent

Rubriques connexes :

- *Configuration matérielle*, page 344
- *Configuration des paramètres globaux*, page 346
- *Configuration des paramètres locaux*, page 347
- *Configuration des paramètres des cartes réseau*, page 349
- *Ajout ou modification des adresses IP*, page 351

Après l'installation de Network Agent, utilisez Websense Manager pour configurer son comportement pour la surveillance du réseau. Les paramètres de Network Agent sont divisés en deux sections principales :

- Les **Paramètres globaux** affectent toutes les instances de Network Agent. Utilisez-les pour :
  - Identifier les ordinateurs de votre réseau
  - Définir la liste des ordinateurs de votre réseau pour lesquels Network Agent doit surveiller les requêtes **entrantes** (par exemple les serveurs Web internes)
  - Définir le calcul de la bande passante et le comportement de la journalisation des protocoles

- Les **Paramètres locaux** ne s'appliquent qu'à l'instance de Network Agent sélectionnée. Utilisez-les pour :
  - Identifier l'instance de Filtering Service associée à chaque Network Agent
  - Noter les proxies et les caches utilisés par les ordinateurs surveillés par cette instance de Network Agent
  - Configurer l'utilisation de chaque carte réseau de l'ordinateur Network Agent (pour surveiller les requêtes, envoyer les pages de blocage, ou les deux)

    Les paramètres des cartes réseau déterminent également quel segment du réseau est surveillé par chaque instance de Network Agent.

Configuration des paramètres globaux

Rubriques connexes :

- *Configuration matérielle*, page 344
- *Configuration des paramètres locaux*, page 347
- *Configuration des paramètres des cartes réseau*, page 349
- *Ajout ou modification des adresses IP*, page 351

La page **Paramètres > Network Agent > Global** permet de définir le comportement de base de surveillance et de journalisation de toutes les instances de Network Agent.

La liste **Définition du réseau interne** identifie les ordinateurs qui font partie de votre réseau. Par défaut, Network Agent ne surveille pas le trafic (communications réseau internes) circulant entre ces ordinateurs.

Un jeu d'entrées initial est fourni par défaut. Vous pouvez ajouter des entrées, ou modifier ou supprimer des entrées existantes.

La liste **Trafic interne à surveiller** comprend les ordinateurs inclus dans la Définition du réseau interne pour lesquels Network Agent doit **surveiller** le trafic. Elle peut par exemple inclure des serveurs Web internes pour vous aider à effectuer le suivi des connexions internes.

Toutes les requêtes envoyées depuis le réseau vers les ordinateurs internes spécifiés sont surveillées. Par défaut, cette liste est vide.

- Cliquez sur **Ajouter** pour ajouter une adresse IP ou une plage d'adresses IP dans la liste appropriée. Pour plus d'informations, consultez *Ajout ou modification des adresses IP*, page 351.
- Pour modifier une entrée de la liste, cliquez sur la plage ou sur l'adresse IP. Pour plus d'informations, consultez *Ajout ou modification des adresses IP*, page 351.
- Pour supprimer une entrée de la liste, cochez la case accolée à la plage ou à l'adresse IP, puis cliquez sur **Supprimer**.

Les options **Paramètres supplémentaires** vous permettent de déterminer la fréquence à laquelle Network Agent calcule l'utilisation de la bande passante et si le trafic de protocoles est journalisé et à quelle fréquence.

Champ	Procédure
Intervalle de calcul de la bande passante	Entrez un nombre compris entre 1 et 300 pour spécifier la fréquence, en secondes, à laquelle Network Agent doit calculer l'utilisation de la bande passante. Une entrée de 300, par exemple, indique à Network Agent de calculer la bande passante toutes les 5 minutes. La valeur par défaut est 10 secondes.
Journaliser régulièrement le trafic de protocoles	Cochez cette option pour activer le champ Intervalle de journalisation.
Intervalle de journalisation	Entrez un nombre compris entre 1 et 300 pour spécifier la fréquence, en minutes, à laquelle Network Agent doit journaliser les protocoles. Une entrée de 60, par exemple, indique à Network Agent d'écrire dans le fichier journal toutes les heures. La valeur par défaut est 1 minute.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Configuration des paramètres locaux

Rubriques connexes :

- *Configuration matérielle*, page 344
- *Configuration des paramètres globaux*, page 346
- *Configuration des paramètres des cartes réseau*, page 349

La page **Paramètres > Network Agent > Paramètres locaux** permet de configurer le comportement du filtrage, les informations du proxy et les autres paramètres de l'instance de Network Agent sélectionnée. L'adresse IP de l'instance de Network Agent sélectionnée s'affiche dans la barre de titre du panneau de contenu et est mise en surbrillance dans le panneau de navigation à gauche.

Servez-vous des paramètres **Définition de Filtering Service** pour spécifier quel service Filtering Service est associé à l'instance de Network Agent sélectionnée, et

préciser comment répondre aux requêtes Internet lorsque Filtering Service n'est pas disponible.

Champ	Procédure
Adresse IP de Filtering Service	Sélectionnez l'instance de Filtering Service associée à cette instance de Network Agent.
Si Filtering Service n'est pas disponible	Sélectionnez **Autoriser** pour autoriser toutes les requêtes ou sélectionnez **Bloquer** pour bloquer toutes les requêtes jusqu'à ce que Filtering Service soit de nouveau disponible. La valeur par défaut est Autoriser.

Pour s'assurer que les requêtes des utilisateurs soient correctement surveillées, filtrées et journalisées, utilisez la liste **Proxies et caches** pour spécifier l'adresse IP d'un serveur proxy ou cache communiquant avec Network Agent.

- Cliquez sur **Ajouter** pour ajouter une adresse IP ou une plage d'adresses IP dans la liste. Pour plus d'informations, consultez *Ajout ou modification des adresses IP*, page 351.
- Pour modifier une entrée de la liste, cliquez sur la plage ou sur l'adresse IP.
- Pour supprimer une entrée de la liste, cochez la case accolée à la plage ou à l'adresse IP, puis cliquez sur **Supprimer**.

Utilisez la liste **Cartes réseau** pour configurer des cartes réseau individuelles. Cliquez sur une carte réseau dans la colonne **Nom**, puis passez à la section *Configuration des paramètres des cartes réseau*, page 349 pour d'autres instructions.

Si les requêtes HTTP de votre réseau passent par un port non standard, cliquez sur **Paramètres avancés de Network Agent** pour définir les ports que Network Agent doit surveiller. Par défaut, les **Ports utilisés pour le trafic HTTP** sont les ports **8080, 80**.

Ne modifiez pas les autres paramètres de cette section à moins d'y être invité(e) par le support technique de Websense.

Champ	Description
Mode	• Aucun (par défaut) • Général • Erreur • Détail • Bande passante
Sortie	• Fichier (par défaut) • Fenêtre
Port	55870 (par défaut)

Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Configuration des paramètres des cartes réseau

Rubriques connexes :

- *Configuration matérielle*, page 344
- *Configuration de Network Agent*, page 345
- *Configuration des paramètres de surveillance pour une carte réseau*, page 350
- *Ajout ou modification des adresses IP*, page 351

La page **Network Agent > Paramètres locaux > Configuration de carte réseau** permet de spécifier comment Network Agent se sert de chaque carte réseau disponible pour surveiller et gérer l'utilisation du réseau.

La section **Informations sur la carte réseau** présente le contexte des modifications apportées, en indiquant l'**Adresse IP**, une brève **Description** de la carte réseau et son **Nom**. Ces informations vous permettent de vérifier que vous configurez bien la carte réseau appropriée.

Surveillance

Dans une configuration à plusieurs cartes réseau, vous pouvez définir l'une d'elles pour la surveillance du trafic et une autre pour l'envoi des pages de blocage. Une carte réseau au moins doit être utilisée pour la surveillance, mais plusieurs peuvent l'être.

Servez-vous de la section **Surveillance** pour indiquer à Network Agent s'il doit ou non **Utiliser cette carte réseau pour surveiller le trafic**.

- Si cette carte réseau n'est pas utilisée pour la surveillance, désactivez la case à cocher et passez à la section suivante.
- Si la carte réseau est utilisée pour la surveillance, cochez la case et cliquez sur **Configurer**. La page Configuration du comportement de la surveillance apparaît. Reportez-vous à la section *Configuration des paramètres de surveillance pour une carte réseau*, page 350 pour obtenir des instructions.

Autres options des cartes réseau

Outre la configuration des options de surveillance, vous pouvez également déterminer d'autres comportements pour les cartes réseau :

1. Sous Blocage, assurez-vous que la carte réseau appropriée apparaît bien dans le champ **Carte réseau de blocage**. Si vous configurez plusieurs cartes réseau, les paramètres de chacune d'elles doivent correspondre à ceux de ce champ. En d'autres termes, une seule carte réseau est utilisée pour le blocage.
2. Si vous exécutez Websense en mode **Autonome**, l'option **Filtrer et journaliser les demandes HTTP** est activée et ne peut pas être modifiée.

3. Si vous avez intégré Websense à une application ou un périphérique tiers, utilisez les options **Intégrations** pour préciser comment cette instance de Network Agent doit filtrer et journaliser les requêtes HTTP. Les options qui ne s'appliquent pas à votre environnement sont désactivées.
   - Sélectionnez **Journaliser les demandes HTTP** pour améliorer la précision des rapports Websense.
   - Sélectionnez **Filtrer toutes les demandes non envoyées sur les ports HTTP** pour utiliser Network Agent pour filtrer uniquement les requêtes HTTP qui ne passent pas par le produit d'intégration.
4. Sous Gestion des protocoles, indiquez si Network Agent doit utiliser cette carte réseau pour filtrer les protocoles non HTTP :
   - Activez l'option **Filtrer les demandes de protocole non HTTP** pour activer la fonction de gestion des protocoles. Cela permet à Websense de filtrer les applications Internet et les méthodes de transfert de données, telles que celles utilisées pour la messagerie instantanée, la diffusion multimédia, le partage de fichiers, la messagerie Internet, etc. Pour plus d'informations, consultez *Filtrage des catégories et des protocoles*, page 38 et *Fonctionnement des protocoles*, page 184.
   - Activez l'option **Mesurer l'utilisation de bande passante par protocole** pour activer la fonction Bandwidth Optimizer. Network Agent utilise cette carte réseau pour surveiller l'utilisation de la bande passante du réseau par chaque protocole ou application. Pour plus d'informations, consultez *Utilisation de Bandwidth Optimizer pour gérer la bande passante*, page 191.

Configuration des paramètres de surveillance pour une carte réseau

La page **Paramètres locaux > Configuration de carte réseau > Liste de surveillance** permet de spécifier quels ordinateurs sont surveillés par Network Agent via la carte réseau sélectionnée.

1. Sous Liste de surveillance, spécifiez les requêtes surveillées par Network Agent :
   - **Tous** : Network Agent surveille les requêtes de tous les ordinateurs qu'il voit utiliser la carte réseau sélectionnée. En général, cela comprend tous les ordinateurs situés sur le même segment de réseau que la carte réseau ou l'ordinateur Network Agent en cours.
   - **Aucun** : Network Agent ne surveille aucune requête.
   - **Spécifique** : Network Agent surveille uniquement les segments réseau inclus dans la Liste de surveillance.

2. Si vous sélectionnez Spécifique, cliquez sur **Ajouter**, puis spécifiez les adresses IP des ordinateurs que Network Agent doit surveiller. Pour plus d'informations, consultez *Ajout ou modification des adresses IP*, page 351.

   > **Remarque**
   > Vous ne pouvez pas entrer de plages d'adresses IP qui se chevauchent. Si les plages se chevauchent, les mesures de la bande passante du réseau risquent d'être imprécises et le filtrage basé sur la bande passante peut ne pas s'appliquer correctement.

   Pour supprimer une adresse IP ou une plage réseau, cochez l'élément approprié dans la liste, puis cliquez sur **Supprimer**.

3. Sous Exceptions de liste de surveillance, identifiez tous les ordinateurs internes que Network Agent doit exclure de la surveillance.

   Par exemple, Network Agent peut ignorer les requêtes provenant du serveur CPM Server. De cette façon, ce dernier ne viendra pas encombrer le journal Websense ni les résultats du moniteur d'état.

   a. Pour identifier un ordinateur, cliquez sur **Ajouter**, puis entrez son adresse IP.

   b. Répétez le processus pour identifier d'autres ordinateurs.

4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Configuration de carte réseau. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ajout ou modification des adresses IP

Rubriques connexes :

- *Configuration des paramètres globaux*, page 346
- *Configuration des paramètres locaux*, page 347
- *Configuration des paramètres des cartes réseau*, page 349

Utilisez la page **Ajouter des adresses IP** ou **Modifier des adresses IP** pour apporter des modifications dans les listes suivantes de Network Agent : Définition du réseau interne, Trafic interne à surveiller, Proxies et caches, Liste de surveillance ou Exceptions de liste de surveillance.

- Lorsque vous ajoutez ou modifiez une plage d'adresses IP, assurez-vous qu'elle n'empiète pas sur une entrée existante (adresse IP unique ou plage d'adresses) dans la liste.
- Lorsque vous ajoutez ou modifiez une seule adresse IP, assurez-vous qu'elle n'entre pas dans une plage apparaissant déjà dans la liste.

Pour ajouter une nouvelle adresse IP ou plage d'adresses IP :

1. Sélectionnez le bouton radio **Adresse IP** ou **Plage d'adresses IP**.

2. Entrez une plage ou une adresse IP valide.
3. Cliquez sur **OK** pour revenir à la page précédente des paramètres de Network Agent. La nouvelle plage ou adresse IP s'affiche dans le tableau approprié.

   Pour revenir à la page précédente sans mettre vos modifications en cache, cliquez sur **Annuler**.
4. Au besoin, répétez ce processus pour chaque adresse IP supplémentaire.

Lorsque vous modifiez une plage ou une adresse IP existante, la page Modifier des adresses IP affiche l'élément sélectionné avec le bouton radio approprié déjà activé. Effectuez les modifications nécessaires, puis cliquez sur **OK** pour revenir à la page précédente.

Lorsque vos modifications sont terminées, cliquez sur **OK** dans la page des paramètres de Network Agent. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Vérification de la configuration de Network Agent

Après avoir configuré Network Agent dans Websense Manager, servez-vous de l'outil Détecteur de trafic réseau pour vérifier que Websense voit bien les ordinateurs de votre réseau.

1. Sélectionnez **Démarrer > Tous les programmes > Websense > Utilitaires > Détecteur de trafic réseau** pour lancer cet outil.
2. Sélectionnez une carte réseau dans la liste déroulante **Adaptateur réseau**.
3. Examinez les adresses qui s'affichent dans la liste **Plages réseau surveillées** pour vérifier que tous les sous-réseaux appropriés y apparaissent.
4. Servez-vous des boutons **Ajouter un sous-réseau** et **Supprimer un sous-réseau** pour modifier les parties du réseau testées.
5. Cliquez sur **Démarrer la surveillance**.

   Le Détecteur de trafic réseau repère les ordinateurs du réseau en surveillant les informations qu'ils envoient. La liste **Nombre d'ordinateurs détectés** présente le nombre actuel d'ordinateurs détectés.
6. Pour afficher des informations spécifiques sur les ordinateurs détectés par l'outil, sélectionnez un sous-réseau dans la liste Plages réseau surveillées, puis cliquez sur **Afficher les ordinateurs détectés**.

   Si un ordinateur spécifique n'apparaît pas dans la liste, assurez-vous qu'il génère du trafic réseau. Pour ce faire, accédez à cet ordinateur, ouvrez un navigateur et visitez un site Web. Reprenez ensuite l'outil Détecteur de trafic réseau et voyez si l'ordinateur s'affiche dans la boîte de dialogue **Ordinateurs détectés**.
7. Lorsque le test de la visibilité du trafic réseau est terminé, cliquez sur **Arrêter la surveillance**.

Si certains ordinateurs ne sont pas visibles :

- Revoyez la configuration du réseau et les exigences de placement des cartes réseau (voir *Configuration matérielle*, page 344).
- Revoyez les informations détaillées sur la configuration du réseau dans le *Guide d'installation* de votre logiciel Websense.
- Vérifiez que vous avez correctement configuré la carte réseau de surveillance (*Configuration des paramètres des cartes réseau*, page 349).

15 Dépannage

Servez-vous de cette section pour trouver des solutions aux problèmes courants avant de contacter le support technique.

Le site Web de Websense propose une vaste base de connaissances disponible à l'adresse www.websense.com/global/en/SupportAndKB/. Lancez des recherches par mot-clé ou par numéro de référence, ou consultez les articles les plus populaires.

Les instructions relatives au dépannage sont regroupées dans les sections suivantes :

Problèmes d'installation et d'abonnement

Etat Websense indiquant un problème d'abonnement

Une clé d'abonnement valide est nécessaire pour télécharger la base de données principale Websense et effectuer un filtrage Internet. Lorsque votre abonnement expire ou est invalide et que la base de données principale n'a pas été téléchargée depuis plus de 2 semaines, le moniteur d'état de Websense affiche un avertissement.

- Vérifiez que vous avez saisi votre clé d'abonnement exactement telle que vous l'avez reçue. La clé d'abonnement respecte la casse.
- Vérifiez que votre abonnement n'est pas arrivé à expiration. Voir *Clé d'abonnement*, page 358.
- Vérifiez que la base de données principale a bien été téléchargée avec succès au cours des 2 dernières semaines. Vous pouvez vérifier l'état du téléchargement dans Websense Manager : cliquez sur **Téléchargement de la base de données** à la page État > Aujourd'hui.

  Pour résoudre les problèmes de téléchargement de bases de données, consultez la section *La base de données principale ne se télécharge pas*, page 358.

Si vous avez saisi la clé correctement mais que l'erreur d'état persiste, ou si votre abonnement est arrivé à expiration, contactez Websense, Inc. ou votre revendeur agréé.

Lorsque votre abonnement expire, les paramètres de Websense Manager déterminent si tous les utilisateurs obtiennent un accès Internet non filtré ou si toutes les requêtes Internet sont bloquées. Pour plus d'informations, consultez *Votre abonnement*, page 28.

Utilisateurs manquants dans Websense Manager après une mise à niveau

Si vous avez défini Active Directory comme service d'annuaire, certains noms d'utilisateur peuvent ne pas apparaître dans Websense Manager après une mise à niveau de Websense. Cela se produit lorsque les noms d'utilisateur comprennent des caractères n'appartenant pas au jeu de caractères UTF-8.

Pour prendre en charge LDAP 3.0, le programme d'installation de Websense remplace le jeu de caractères MBCS par le jeu UTF-8 pendant la mise à niveau. Par conséquent, les noms d'utilisateur qui comprennent des caractères non UTF-8 ne sont pas reconnus correctement.

Pour résoudre ce problème, définissez manuellement le jeu de caractères sur MBCS :

1. Dans Websense Manager, sélectionnez **Paramètres** > **Services d'annuaire**.
2. Assurez-vous que **Active Directory (Native Mode)** soit sélectionné sous Annuaires, en haut de la page.
3. Cliquez sur **Paramètres de l'annuaire avancés**.
4. Sous Jeu de caractères, cliquez sur **MBCS**. Il vous faudra peut-être faire défiler les éléments pour voir cette option.
5. Cliquez sur **OK** pour mettre la modification en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Problèmes de la base de données principale

- *Utilisation de la base de données de filtrage initiale*, page 357
- *La base de données principale date de plus d'une semaine.*, page 357

- *La base de données principale ne se télécharge pas*, page 358
- *La base de données principale ne se télécharge pas à l'heure définie.*, page 362
- *Contact du support technique pour les problèmes de téléchargement de la base de données*, page 362

Utilisation de la base de données de filtrage initiale

La base de données principale Websense héberge les définitions de catégories et de protocoles qui constituent la base du filtrage du contenu Internet.

Une version partielle de la base de données principale est installée en même temps que Websense sur chaque ordinateur Filtering Service. Cette base de données partielle est utilisée pour activer la fonction de filtrage de base dès que vous entrez votre clé d'abonnement.

Vous devez télécharger la base de données dans son intégralité pour qu'un filtrage complet soit effectué. Pour plus d'informations, consultez *Base de données principale Websense*, page 32.

Le téléchargement de la base de données complète peut prendre quelques minutes ou plus d'une heure, selon la vitesse de la connexion Internet, la bande passante, la mémoire et l'espace disque disponibles.

La base de données principale date de plus d'une semaine.

La base de données principale Websense héberge les définitions de catégories et de protocoles qui constituent la base du filtrage du contenu Internet. Websense télécharge les modifications apportées à la base de données principale en fonction du planning défini dans Websense Manager. Par défaut, le téléchargement est programmé pour s'exécuter une fois par jour.

Pour déclencher manuellement le téléchargement de la base de données :

1. Dans Websense Manager, ouvrez la page **État > Aujourd'hui**, puis cliquez sur **Téléchargement de la base de données**.
2. Cliquez sur **Mettre à jour** à côté de l'instance de Filtering Service appropriée pour démarrer le téléchargement de la base de données ou cliquez sur **Tout mettre à jour** pour démarrer le téléchargement sur tous les ordinateurs Filtering Service.

   Remarque

   Après le téléchargement des mises à jour de la base de données principale, l'utilisation du processeur peut être de 90 % ou plus pendant quelques minutes pendant le chargement de la base de données dans la mémoire locale. Il est généralement préférable de programmer les téléchargements en dehors des heures de pointe.

3. Pour continuer à travailler pendant le téléchargement de la base de données, cliquez sur **Fermer**.

Cliquez sur le bouton **Téléchargement de la base de données** à tout moment pour afficher l'état du téléchargement.

Si une nouvelle version de la base de données principale ajoute ou supprime des catégories ou des protocoles, les administrateurs qui exécutent des tâches de gestion de stratégies liées aux catégories ou aux protocoles (par exemple qui modifient un jeu de catégories) au moment du téléchargement peuvent recevoir des erreurs. Bien que de telles mises à jour soient assez rares, il est préférable d'éviter, dans la mesure du possible, de modifier des éléments liés aux catégories et aux protocoles pendant la mise à jour d'une base de données.

La base de données principale ne se télécharge pas

Si vous n'arrivez pas à télécharger la base de données principale Websense :

- Vérifiez que vous avez correctement saisi votre clé d'abonnement dans Websense Manager et que cette clé n'est pas arrivée à expiration (*Clé d'abonnement*, page 358).
- Vérifiez que l'ordinateur Filtering Service peut accéder à Internet (*Accès Internet*, page 359).
- Vérifiez les paramètres du pare-feu ou du serveur proxy pour vous assurer que Filtering Service peut se connecter au serveur de téléchargement de Websense (*Vérification des paramètres du pare-feu ou du serveur proxy*, page 359).
- Vérifiez que l'ordinateur de téléchargement dispose de suffisamment d'espace disque (*Espace disque insuffisant*, page 360) et de mémoire (*Mémoire insuffisante*, page 361).
- Recherchez la présence sur le réseau d'une application ou d'un dispositif, par exemple un logiciel anti-virus, susceptible d'empêcher la connexion du téléchargement (*Applications restrictives*, page 362).

Clé d'abonnement

Pour vérifier que la clé d'abonnement a été saisie correctement et n'est pas arrivée à expiration :

1. Dans Websense Manager, sélectionnez **Paramètres > Compte**.
2. Comparez la clé que Websense, Inc. ou votre revendeur vous a envoyée avec celle qui apparaît dans le champ **Clé d'abonnement**. La clé doit reproduire la même combinaison de majuscules/minuscules que votre document.
3. Vérifier la date accolée à **Date d'expiration de la clé**. Si cette date est dépassée, contactez votre revendeur ou Websense, Inc., afin de renouveler votre abonnement.
4. Si vous avez modifié la clé dans la boîte de dialogue Paramètres, cliquez sur **OK** pour activer la clé et le téléchargement de la base de données.

Pour démarrer manuellement un téléchargement de la base de données, ou pour vérifier l'état du dernier téléchargement, cliquez sur **Téléchargement de la base de données** dans la barre d'outils située en haut de la page État > Aujourd'hui.

Accès Internet

Pour télécharger la base de données principale, l'ordinateur Filtering Service envoie une commande **HTTP post** aux serveurs de téléchargement aux URL suivantes :

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com

Pour vérifier que Filtering Service peut accéder à Internet pour communiquer avec le serveur de téléchargement :

1. Ouvrez un navigateur sur l'ordinateur exécutant Filtering Service.
2. Entrez l'URL suivante :

   http://download.websense.com/

   Si l'ordinateur peut ouvrir une connexion HTTP au site, une page de redirection s'affiche et le navigateur affiche la page d'accueil de Websense.

   Si ce n'est pas le cas, assurez-vous que l'ordinateur :

   - Peut communiquer sur le port 80, ou sur le port désigné dans votre réseau pour le trafic HTTP
   - Est configuré de manière à effectuer correctement les recherches DNS
   - Est configuré pour utiliser les serveurs proxy éventuellement nécessaires (voir *Vérification des paramètres du pare-feu ou du serveur proxy*, page 359)

   Assurez-vous également que certaines règles de votre passerelle ne bloquent pas le trafic HTTP provenant de l'ordinateur Filtering Service.
3. Pour vérifier que l'ordinateur peut communiquer avec le site de téléchargement, utilisez l'une des méthodes suivantes :
   - À l'invite de commande, entrez la commande suivante :

     ```
     ping download.websense.com
     ```

     Vérifiez que le ping obtienne une réponse du serveur de téléchargement.
   - Utilisez telnet pour vous connecter à **download.websense.com 80**. Si vous voyez un curseur et aucun message d'erreur, vous pouvez vous connecter au serveur de téléchargement.

Vérification des paramètres du pare-feu ou du serveur proxy

Si la base de données principale est téléchargée via un pare-feu ou un serveur proxy nécessitant une authentification, assurez-vous qu'un navigateur de l'ordinateur Filtering Service puisse charger correctement les pages Web. Si les pages s'ouvrent normalement mais que la base de données principale n'est pas téléchargée, vérifiez les paramètres du serveur proxy dans le navigateur Web.

Microsoft Internet Explorer :

1. Sélectionnez **Outils > Options Internet**.

2. Ouvrez l'onglet **Connexions**.
3. Cliquez sur **Paramètres du réseau local**. Les informations relatives à la configuration du serveur proxy s'affichent sous **Serveur proxy**.

   Notez les paramètres du proxy.

Mozilla Firefox :

1. Sélectionnez **Outils > Options > Avancé**.
2. Ouvrez l'onglet **Réseau**.
3. Cliquez sur **Paramètres**. La boîte de dialogue Paramètres de connexion indique si le navigateur est configuré pour se connecter à un serveur proxy.

   Notez les paramètres du proxy.

Ensuite, assurez-vous que Websense soit configuré pour utiliser le même serveur proxy pour effectuer le téléchargement.

1. Dans Websense Manager, sélectionnez **Paramètres > Téléchargement de la base de données**.
2. Vérifiez que l'option **Utiliser un serveur proxy ou un pare-feu** est activée et que le serveur et le port appropriés apparaissent.
3. Vérifiez l'exactitude de tous les paramètres d'**Authentification**. Vérifier le nom d'utilisateur et le mot de passe, en respectant l'orthographe et la casse.

   Si Websense doit fournir des informations d'authentification, le pare-feu ou le serveur proxy doit être configuré pour accepter l'authentification de base ou en texte clair. Les informations relatives à l'activation de l'authentification de base sont disponibles dans la Base de connaissances de Websense.

Si un pare-feu limite l'accès à Internet au moment où Websense Express télécharge habituellement la base de données, ou limite la taille d'un fichier pouvant être transféré via HTTP, Websense ne peut pas télécharger la base de données. Pour déterminer si le pare-feu est la cause du problème de téléchargement, regardez si une règle du pare-feu est susceptible de bloquer le téléchargement, puis modifiez au besoin les heures de téléchargement dans Websense Manager (*Configuration des téléchargements de la base de données*, page 33).

Espace disque insuffisant

La base de données principale Websense est stockée dans le répertoire **bin** de Websense (/opt/Websense/bin ou C:\Program Files\Websense\bin, par défaut). Le lecteur sur lequel est situé ce répertoire doit disposer de suffisamment d'espace disque pour télécharger la base de données compressée et pour la décompresser ensuite.

L'espace disque disponible sur l'ordinateur doit être au moins égal à deux fois la taille de la base de données principale. Au fur et à mesure de l'augmentation du nombre d'entrées dans la base de données principale, la taille nécessaire pour un téléchargement réussi s'accroît également. En règle générale, Websense, Inc. recommande un espace disque disponible d'au moins 3 Go sur le lecteur de téléchargement.

Sous Windows, utilisez l'Explorateur de Windows pour vérifier l'espace disque disponible :

1. Ouvrez **Poste de travail** dans l'Explorateur Windows (pas dans Internet Explorer).
2. Sélectionnez le lecteur sur lequel Websense est installé. Par défaut, Websense est situé sur le lecteur C.
3. Cliquez du bouton droit et choisissez **Propriétés** dans le menu contextuel.
4. Dans l'onglet Général, vérifiez que l'espace disque disponible est supérieur ou égal à 3 Go. Si l'espace disponible sur le lecteur est insuffisant, supprimez les fichiers inutiles pour libérer l'espace requis.

Dans les systèmes Linux, utilisez la commande **df** pour vérifier la quantité d'espace disponible dans le système de fichiers sur lequel Websense est installé :

1. Ouvrez une session sur le terminal.
2. À l'invite, entrez :

   ```
   df -h /opt
   ```

   Websense est généralement installé dans le répertoire /opt/Websense/bin. S'il est installé en un autre emplacement, utilisez ce chemin.
3. Assurez-vous que l'espace disque disponible soit supérieur ou égal à 3 Go. Si l'espace disponible sur le lecteur est insuffisant, supprimez les fichiers inutiles pour libérer l'espace requis.

Si, après vérification, l'espace disque disponible est suffisant mais que les problèmes de téléchargement persistent, tentez d'arrêter tous les services Websense (voir *Arrêt et démarrage des services Websense*, page 286), de supprimer les fichiers **Websense.xfr** et **Websense** (sans extension), de redémarrer les services, puis de télécharger manuellement une nouvelle base de données.

Mémoire insuffisante

La mémoire nécessaire pour exécuter Websense et télécharger la base de données principale dépend de la taille du réseau. Par exemple, dans le cas d'un petit réseau, 2 Go de mémoire sont conseillés pour toutes les plates-formes.

Reportez-vous au *Guide de déploiement* pour les recommandations système.

Pour vérifier la mémoire disponible dans un système Windows :

1. Ouvrez le Gestionnaire des tâches.
2. Sélectionnez l'onglet **Performances**.
3. Vérifiez la **Mémoire physique** totale disponible.
4. Si la mémoire disponible est inférieure à 2 Go, augmentez la quantité de RAM de l'ordinateur.

Vous pouvez également sélectionner **Panneau de configuration > Outils d'administration > Performances** pour obtenir ces informations.

Pour vérifier la mémoire disponible dans un système Linux :

1. Ouvrez une session sur le terminal.
2. À l'invite, entrez :

   ```
   top
   ```
3. Calculez la mémoire totale disponible en ajoutant **Mem: av** et **Swap: av**.
4. Si la mémoire disponible est inférieure à 2 Go, augmentez la quantité de RAM de l'ordinateur.

Applications restrictives

Certaines applications restrictives, telles que les logiciels antivirus, les applications de limite de taille ou les systèmes de détection des intrusions, peuvent interférer avec les téléchargements de la base de données. Dans la mesure du possible, configurez Websense pour qu'il passe directement à la dernière passerelle de sorte qu'il n'ait pas besoin de se connecter à ces applications ou dispositifs. Vous pouvez également :

1. Désactivez les restrictions liées à l'ordinateur Filtering Service et à l'emplacement de téléchargement de la base de données principale.

   Pour obtenir des instructions sur la modification de la configuration du périphérique ou du dispositif, consultez sa documentation.
2. Tentez de télécharger la Base de données principale.

Si cette modification n'a aucun effet, reconfigurez l'application ou le dispositif pour inclure l'ordinateur exécutant Filtering Service.

La base de données principale ne se télécharge pas à l'heure définie.

Il est possible que l'heure et la date du système ne soient pas définis correctement sur l'ordinateur Filtering Service. Websense utilise l'horloge du système pour déterminer l'heure de téléchargement de la base de données principale.

Si le téléchargement ne s'effectue pas du tout, consultez *La base de données principale ne se télécharge pas*, page 358.

Contact du support technique pour les problèmes de téléchargement de la base de données

Si les problèmes de téléchargement de la base de données principale persistent à la fin de la procédure de dépannage de cette section d'aide, envoyez les informations suivantes au support technique de Websense :

1. Le message d'erreur exact qui s'affiche dans la boîte de dialogue Téléchargement de la base de données
2. Les adresses IP externes des ordinateurs qui tentent de télécharger la base de données

3. Votre clé d'abonnement Websense
4. La date et l'heure de la dernière tentative
5. Le nombre d'octets transférés, le cas échéant
6. Ouvrez une fenêtre d'invite de commande et exécutez la commande **nslookup** sur **download.websense.com**. Si la connexion au serveur de téléchargement est établie, envoyez les adresses IP renvoyées au service technique.
7. Ouvrez une fenêtre d'invite de commande et exécutez la commande **tracert** sur **download.websense.com**. Si la connexion au serveur de téléchargement est établie, envoyez le suivi du routage au Support technique.
8. Un suivi de paquets ou une capture de paquets exécuté(e) sur le serveur de téléchargement Websense pendant une tentative de téléchargement
9. Un suivi de paquets ou une capture de paquets exécuté(e) sur la passerelle réseau pendant la même tentative de téléchargement
10. Les fichiers suivants du répertoire **bin** de Websense : **websense.ini**, **eimserver.ini** et **config.xml**.

Pour obtenir les coordonnées du support technique, accédez au site www.websense.com/SupportPortal/default.aspx.

Problèmes de filtrage

Dysfonctionnement de Filtering Service

Lorsque le service Filtering Service ne fonctionne pas, les requêtes Internet ne peuvent être ni filtrées ni journalisées.

Filtering Service peut s'arrêter dans les cas suivants :

- L'ordinateur Filtering Service ne dispose pas de suffisamment d'espace disque.

- Un téléchargement de la base de données principale a échoué du fait d'un manque d'espace disque (voir *La base de données principale ne se télécharge pas*, page 358).
- Le fichier **websense.ini** est manquant ou corrompu.
- Vous avez arrêté le service (par exemple après la création de pages de blocage personnalisés) et vous ne l'avez pas redémarré.

Filtering Service peut également sembler arrêté si vous avez redémarré plusieurs services Websense sans les redémarrer dans l'ordre approprié. Lorsque vous redémarrez plusieurs services, n'oubliez pas de démarrer la base de données de stratégies, Policy Broker et Policy Server avant les autres services Websense.

Pour résoudre ces problèmes :

- Vérifiez que l'ordinateur Filtering Service dispose d'au moins 3 Go d'espace disque disponible. Vous pouvez éventuellement supprimer des fichiers inutiles ou ajouter des capacités supplémentaires.
- Naviguez jusqu'au répertoire **bin** (par défaut, C:\Program Files\Websense\bin ou /opt/Websense/bin), et vérifiez que vous pouvez ouvrir le fichier **websense.ini** dans un éditeur de texte. Si ce fichier est corrompu, remplacez-le par un fichier de sauvegarde.
- Regardez dans l'Observateur d'événements de Windows ou dans le fichier **websense.log** si des messages d'erreur sont liés au service Filtering Service (voir *Outils de dépannage*, page 399).
- Déconnectez-vous de Websense Manager, redémarrez Websense Policy Server, puis le service Websense Filtering Service (voir *Arrêt et démarrage des services Websense*, page 286).

  Patientez 1 minute, puis reconnectez-vous à Websense Manager.

User Service indisponible

Lorsque User Service ne fonctionne pas, ou lorsque Policy Server ne peut pas communiquer avec ce service, Websense ne peut pas appliquer correctement les stratégies de filtrage à base d'utilisateurs.

User Service peut sembler arrêté si vous avez redémarré Policy Server après avoir redémarré d'autres services Websense. Pour résoudre ce problème :

1. Redémarrez le service Websense Policy Server (voir *Arrêt et démarrage des services Websense*, page 286).
2. Démarrez ou redémarrez Websense User Service.
3. Fermez Websense Manager.

   Patientez 1 minute, puis reconnectez-vous à Websense Manager.

Si le problème n'est pas résolu à la fin de la procédure précédente :

- Regardez dans l'Observateur d'événements de Windows ou dans le fichier **websense.log** si des messages d'erreur sont liés au service User Service (voir *Outils de dépannage*, page 399).

- Naviguez jusqu'au répertoire **bin** de Websense (par défaut, C:\Program Files\Websense\bin ou /opt/Websense/bin), et vérifiez que vous pouvez ouvrir le fichier **websense.ini** dans un éditeur de texte. Si ce fichier est corrompu, remplacez-le par un fichier de sauvegarde.

Problème de classement des sites dans la catégorie Technologies de l'information

Les versions 4.0 et ultérieures d'Internet Explorer acceptent les recherches saisies dans la barre d'adresse. Lorsque cette option est activée, si l'utilisateur entre uniquement un nom de domaine dans la barre d'adresse (**websense** au lieu de **http://www.websense.com**, par exemple), Internet Explorer considère l'entrée comme une requête de recherche et non comme une requête de site. Il affiche le site le plus ressemblant recherché par l'utilisateur, et la liste des sites les plus proches.

Par conséquent, Websense autorise, bloque ou limite la requête en fonction de l'état de la catégorie Informatique/Moteurs de recherche et portails de la stratégie active, pas en fonction de la catégorie du site demandé. Pour que Websense filtre en fonction de la catégorie du site demandé, désactivez les recherches à partir de la barre d'adresse :

1. Sélectionnez **Outils > Options Internet**.
2. Ouvrez l'onglet **Avancé**.
3. Dans la section Rechercher de la barre d'adresse, sélectionnez **Ne pas effectuer de recherche à partir de la barre d'adresse**.
4. Cliquez sur **OK**.

> **Remarque**
> Cette procédure convient pour les versions 5, 6 et 7 d'Internet Explorer.

Mots-clés non bloqués

Les causes potentielles de ce problème sont les suivantes : l'option **Désactiver le blocage par mot-clé** est activée, ou le site dont l'URL contient le mot-clé utilise une commande **post** pour envoyer des données à votre serveur Web.

Pour vérifier que le blocage par mot-clé est activé :

1. Dans Websense Manager, sélectionnez **Paramètres > Filtrage**.
2. Dans l'onglet Filtrage général, vérifiez la liste **Options de recherche de mots-clés**. Si **Désactiver le blocage par mot-clé** apparaît, sélectionnez une autre option dans la liste. Pour plus d'informations sur les options disponibles, consultez *Configuration des paramètres de filtrage de Websense*, page 56.
3. Cliquez sur **OK** pour mettre la modification en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Si un site utilise une commande **post** pour envoyer des données à votre serveur Web, Websense ne reconnaît pas les paramètres de filtrage par mot-clé pour cette URL. À

moins que votre produit d'intégration ne reconnaisse les données envoyées via la commande post, les utilisateurs peuvent toujours accéder aux URL contenant des mots-clés bloqués.

Pour vérifier si un site Web utilise une commande post, affichez la source du site dans votre navigateur. Si le code source contient la chaîne **<method=post>**, la commande post est utilisée pour charger ce site.

Problème de filtrage des URL de filtre d'accès limité ou personnalisé

Si une URL HTTPS d'un filtre d'accès limité ou d'une liste d'URL personnalisée (recatégorisées ou non filtrées) n'est pas filtrée comme prévu, il se peut qu'un produit d'intégration convertisse l'URL en un format non reconnu par Filtering Service.

Les produits d'intégration non proxy convertissent les URL du format domaine au format IP. Par exemple, l'URL **https://<domaine>** est lue sous la forme **https://<adresse IP>:443**. Lorsque cela se produit, Filtering Service ne peut pas associer l'URL envoyée par le produit d'intégration à l'URL personnalisée ou au filtre d'accès limité, et ne filtre donc pas le site de façon appropriée.

Pour contourner ce problème, ajoutez à la fois les adresses IP et les URL des sites que vous souhaitez filtrer à l'aide d'URL personnalisées ou de filtres d'accès limité.

Un utilisateur ne peut pas accéder à un protocole ou à une application comme prévu.

Si votre réseau comprend Microsoft ISA Server, certaines configurations de méthode d'authentification peuvent entraîner l'abandon des connexions aux applications de messagerie.

Si une autre méthode que l'authentification anonyme est active, le serveur proxy tente d'identifier les paquets de données reçus lorsque les utilisateurs demandent à se connecter aux applications. Le serveur proxy n'arrive pas à identifier le paquet de données et la connexion est abandonnée. Ce problème peut éventuellement fausser l'activité de filtrage des protocoles de Websense.

L'accès à un protocole ou à une application Internet peut également être bloqué si le port utilisé par l'application est lui-même bloqué. Cela se produit dans les cas suivants :

- Le port est bloqué par un pare-feu.
- L'un des identificateurs du protocole personnalisé bloqué inclut le port (sous forme de port individuel ou dans une plage de ports).

Une requête FTP n'est pas bloquée comme prévu.

Dans le cas d'une intégration aux pare-feu Check Point®, Websense requiert l'activation de **l'affichage des dossiers** dans le navigateur du client pour reconnaître et filtrer les requêtes FTP.

Lorsque l'affichage des dossiers n'est pas activé, les requêtes FTP envoyées au proxy FireWall-1 sont envoyées à Websense avec un préfixe « http:// ». Websense filtre donc ces requêtes en tant que requêtes HTTP et non FTP.

Websense n'applique pas les stratégies de groupe ou d'utilisateur

Si Websense applique les stratégies d'ordinateur ou de réseau, ou la stratégie **Par défaut**, alors que des stratégies d'utilisateur ou de groupe ont été attribuées, consultez la section *Problèmes liés à l'identification des utilisateurs*, page 370. Des informations supplémentaires sont disponibles dans la Base de connaissances.

Les utilisateurs distants ne sont pas filtrés par la stratégie appropriée.

Si un utilisateur distant se connecte à l'aide des informations d'identification du domaine (informations de connexion réseau), Websense applique la stratégie attribuée à cet utilisateur, ou au groupe ou au domaine de l'utilisateur, le cas échéant. Si aucune stratégie n'est attribuée à l'utilisateur, au groupe ou au domaine, ou si l'utilisateur se connecte à l'ordinateur avec un compte utilisateur local, Websense applique la stratégie Par défaut.

Il peut cependant arriver qu'un utilisateur ne soit pas filtré par une stratégie d'utilisateur ou de groupe ou par la stratégie Par défaut. Cela se produit lorsque l'utilisateur se connecte à l'ordinateur distant avec un compte utilisateur local et que la dernière partie de l'adresse MAC (Media Access Control) de l'ordinateur distant chevauche une adresse IP réseau à laquelle une stratégie a été attribuée. Dans ce cas, la stratégie attribuée à cette adresse IP particulière est appliquée à l'utilisateur distant.

Problèmes liés à Network Agent

Network Agent n'est pas installé.

Network Agent doit être installé pour que le filtrage par protocole puisse s'effectuer. Avec certaines intégrations, Network Agent permet également une journalisation plus précise.

Si vous utilisez un produit d'intégration et que vous n'avez pas besoin de la journalisation ni du filtrage par protocole de Network Agent, vous pouvez masquer le message d'état « Aucun agent Network Agent n'est installé ». Reportez-vous à la section *Vérification de l'état du système en cours*, page 294 pour obtenir des instructions.

Dans le cas d'une installation autonome, Network Agent doit être installé pour surveiller et filtrer le trafic réseau. Pour des instructions sur leur installation, consultez le *Guide d'installation*, puis la section *Configuration de Network Agent*, page 345.

Network Agent n'est pas en cours d'exécution.

Network Agent doit être installé pour que le filtrage par protocole puisse s'effectuer. Avec certaines intégrations, Network Agent permet également une journalisation plus précise.

Dans le cas d'une installation autonome, Network Agent doit s'exécuter pour surveiller et filtrer le trafic réseau.

Pour résoudre le problème :

1. Ouvrez la boîte de dialogue Services de Windows (voir *Boîte de dialogue Services de Windows*, page 399) pour voir si le service **Websense Network Agent** est démarré.
2. Redémarrez les services **Websense Policy Broker** et **Websense Policy Server** (voir *Arrêt et démarrage des services Websense*, page 286).
3. Démarrez ou redémarrez le service **Websense Network Agent**.
4. Fermez Websense Manager.
5. Patientez 1 minute, puis reconnectez-vous à Websense Manager.

Si le problème n'est pas résolu :

- Regardez dans l'**Observateur d'événements de Windows** si des messages d'erreur sont liés au service Network Agent (voir *Observateur d'événements de Windows*, page 400).
- Regardez dans le fichier **Websense.log** si des messages d'erreur sont liés au service Network Agent (voir *Fichier journal Websense*, page 400).

Network Agent ne surveille aucune carte réseau.

Pour surveiller le trafic réseau, Network Agent doit être associé à au moins une carte réseau.

Si vous ajoutez ou retirez des cartes réseau de l'ordinateur Network Agent, vous devez actualiser votre configuration Network Agent.

1. Dans Websense Manager, sélectionnez **Paramètres**.
2. Dans le panneau de navigation, sous Network Agent, sélectionnez l'adresse IP de l'ordinateur Network Agent.
3. Assurez-vous que toutes les cartes réseau de l'ordinateur sélectionné apparaissent dans la liste.
4. Assurez-vous qu'une carte réseau au moins soit configurée pour surveiller le trafic réseau.

Pour plus d'informations, consultez *Configuration de Network Agent*, page 345.

Network Agent ne peut pas communiquer avec Filtering Service.

Network Agent doit pouvoir communiquer avec Filtering Service pour appliquer vos stratégies d'utilisation d'Internet.

- Avez-vous modifié l'adresse IP de l'ordinateur Filtering Service ou réinstallé Filtering Service ?

  Dans l'affirmative, consultez la section *Mise à jour des informations d'ID unique ou de l'adresse IP de Filtering Service*, page 369.
- L'ordinateur Network Agent contient-il plus de 2 cartes réseau ?

  Dans l'affirmative, consultez la section *Configuration du réseau*, page 343 pour vérifier vos paramètres Websense.
- Avez-vous reconfiguré le commutateur connecté à l'ordinateur Network Agent ?

  Dans l'affirmative, reportez-vous au *Guide d'installation* pour vérifier votre configuration matérielle, et à la section *Configuration de Network Agent*, page 345 pour vérifier vos paramètres Websense.

Si aucune de ces solutions ne s'applique, consultez la section *Configuration des paramètres locaux*, page 347 pour plus d'informations sur l'association entre Network Agent et Filtering Service.

Mise à jour des informations d'ID unique ou de l'adresse IP de Filtering Service

Lorsque Filtering Service à été désinstallé puis réinstallé, Network Agent n'actualise pas automatiquement l'identificateur interne (ID unique) de Filtering Service. Websense Manager tente alors d'interroger Filtering Service avec l'ancien ID unique, qui n'existe plus.

De même, lorsque vous modifiez l'adresse IP de l'ordinateur Filtering Service, cette modification n'est pas automatiquement enregistrée.

Pour rétablir la connexion à Filtering Service :

1. Ouvrez Websense Manager.

Un message d'état indique qu'une instance de Network Agent ne peut pas se connecter à Filtering Service.

2. Cliquez sur **Paramètres** en haut du panneau de navigation situé à gauche.
3. Dans le panneau de navigation, sous Network Agent, sélectionnez l'adresse IP de l'ordinateur Network Agent.
4. En haut de la page, sous Définition de Filtering Service, développez la liste **Adresse IP du serveur**, puis sélectionnez l'adresse IP de l'ordinateur Filtering Service.
5. Cliquez sur **OK** en bas de la page pour mettre la mise à jour en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Problèmes liés à l'identification des utilisateurs

Rubriques connexes :

- *Problèmes de filtrage*, page 363
- *Les utilisateurs distants ne sont pas invités à s'authentifier manuellement.*, page 380
- *Les utilisateurs distants ne sont pas filtrés correctement.*, page 380

Si Websense utilise des stratégies d'ordinateur ou de réseau, ou la stratégie **Par défaut**, pour filtrer les requêtes Internet alors même que des stratégies d'utilisateur ou de groupe ont été attribuées, ou lorsqu'une stratégie d'utilisateur ou de groupe inappropriée est appliquée, procédez comme suit pour cerner le problème :

- Si vous utilisez Microsoft ISA Server et que vous avez modifié la méthode d'authentification, assurez-vous que le service Proxy Web à redémarré.
- Si vous utilisez des groupes imbriqués dans Windows Active Directory, les stratégies attribuées à un groupe parent s'appliquent aux utilisateurs appartenant à un sous-groupe, et non directement au groupe parent. Pour plus d'informations sur la hiérarchie des utilisateurs et des groupes, consultez la documentation de votre service d'annuaire.
- Le cache de User Service peut être obsolète. User Service met en cache les correspondances nom d'utilisateur/adresse IP pendant 3 heures. Vous pouvez obliger le cache de User Service à se mettre à jour en mettant en cache les modifications dans Websense Manager et en cliquant sur **Enregistrer tout**.
- Si l'utilisateur qui n'est pas filtré correctement travaille sur un ordinateur fonctionnant sous Windows XP SP2, le problème peut provenir du Pare-feu de connexion Internet (ICF) de Windows, inclus et activé par défaut sous Windows XP SP2. Pour plus d'informations sur Windows ICF, consultez l'Article #320855 de la Base de connaissances de Microsoft.

Pour que DC Agent ou Logon Agent obtienne les informations de connexion des utilisateurs d'un ordinateur fonctionnant sous Windows XP SP2 :

1. Dans le menu **Démarrer** de l'ordinateur client, sélectionnez **Paramètres** > **Panneau de configuration** > **Centre de sécurité** > **Pare-feu Windows**.
2. Ouvrez l'onglet **Exceptions**.
3. Activez l'option **Partage de fichiers et d'imprimantes**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue Pare-feu de connexion Internet (ICF), puis fermez toutes les autres fenêtres ouvertes.

Si vous utilisez un agent d'identification transparente Websense, consultez la section de dépannage appropriée :

- *Dépannage de DC Agent*, page 371.
- *Dépannage de Logon Agent*, page 373.
- *Dépannage d'eDirectory Agent*, page 376.
- *Dépannage de RADIUS Agent*, page 378.

Dépannage de DC Agent

Pour résoudre les problèmes d'identification des utilisateurs liés à DC Agent :

1. Vérifiez toutes les connexions réseau.
2. Vérifiez les messages d'erreur dans l'Observateur d'événements de Windows (voir *Observateur d'événements de Windows*, page 400).
3. Vérifiez les informations d'erreur détaillées dans le fichier journal de Websense (Websense.log) (voir *Fichier journal Websense*, page 400).

Les causes courantes des problèmes d'identification d'utilisateur liés à DC Agent comprennent :

- Les services réseau ou Windows communiquent avec le contrôleur de domaine de telle sorte que DC Agent voie le service comme un nouvel utilisateur, pour lequel aucune stratégie n'a été définie. Voir *La stratégie Par défaut ne filtre pas correctement les utilisateurs.*, page 372.
- DC Agent ou User Service a pu être installé sous forme de service à l'aide du compte Invité, ce qui correspond pour le contrôleur de domaine à un utilisateur anonyme. Si le contrôleur de domaine a été configuré pour ne pas donner la liste des utilisateurs et des groupes à un utilisateur anonyme, DC Agent n'est pas autorisé à télécharger la liste. Voir *Modification manuelle des autorisations de DC Agent et User Service*, page 372.
- Le cache de User Service est obsolète. User Service met en cache les correspondances nom d'utilisateur/adresse IP pendant 3 heures, par défaut. Le cache est également mis à jour chaque fois que vous effectuez des modifications et que vous cliquez sur **Enregistrer tout** dans Websense Manager.

La stratégie Par défaut ne filtre pas correctement les utilisateurs.

Lorsque le réseau ou Microsoft Windows 200x contacte le contrôleur de domaine, le nom du compte utilisé peut faire croire à Websense qu'un utilisateur non identifié accède à Internet à partir de l'ordinateur filtré. Comme aucune stratégie d'utilisateur ou de groupe n'a été attribuée à cet utilisateur, la stratégie d'ordinateur ou de réseau, ou la stratégie Par défaut, s'applique.

- Les services réseau peuvent éventuellement avoir besoin de privilèges de domaine pour accéder aux données du réseau et utiliser le nom d'utilisateur de domaine sur lequel ils s'exécutent pour contacter le contrôleur de domaine.

  Pour résoudre ce problème, consultez la section *Configuration d'un agent pour qu'il ignore certains noms d'utilisateur*, page 234.

- Les services Windows 200x contactent régulièrement le contrôleur de domaine avec un nom d'utilisateur composé du nom de l'ordinateur suivi du signe dollar (jdoe-ordinateur$). DC Agent confond le service avec le nouvel utilisateur auquel aucune stratégie n'a été attribuée.

  Pour résoudre le problème, configurez DC Agent pour qu'il ignore toute connexion de forme **ordinateur$**.

  1. Sur l'ordinateur DC Agent, localisez le répertoire Websense **bin** (par défaut, **C:\Program Files\Websense\bin**).
  2. Ouvrez le fichier **transid.ini** dans un éditeur de texte.
  3. Ajoutez l'entrée suivante dans le fichier :

     ```
     IgnoreDollarSign=true
     ```

  4. Enregistrez et fermez le fichier.
  5. Redémarrez DC Agent (voir *Arrêt et démarrage des services Websense*, page 286).

Modification manuelle des autorisations de DC Agent et User Service

Sur l'ordinateur exécutant le contrôleur de domaine :

1. Créez un compte utilisateur, par exemple **Websense**. Vous pouvez utiliser un compte existant, mais un compte Websense est préférable car il vous permet de définir le mot de passe pour qu'il n'expire pas. Aucun privilège spécial n'est nécessaire.

   Définissez le mot de passe pour qu'il n'expire jamais. Ce compte fournit uniquement un contexte de sécurité pour l'accès aux objets de l'annuaire.

   Notez le nom d'utilisateur et le mot de passe définis pour ce compte puisqu'ils seront nécessaires aux étapes 6 et 7.
2. Ouvrez la boîte de dialogue Services de Windows sur chaque ordinateur Websense DC Agent (**Démarrer > Tous les programmes > Outils d'administration > Services**).
3. Sélectionnez l'entrée **Websense DC Agent**, puis cliquez sur **Arrêter**.
4. Double-cliquez sur l'entrée **Websense DC Agent**.
5. Dans l'onglet **Connexion**, sélectionnez l'option **Ce compte**.

6. Entrez le nom d'utilisateur du compte Websense DC Agent créé à l'étape 1. Par exemple : **DomainName\websense**.
7. Entrez et confirmez le mot de passe Windows de ce compte.
8. Cliquez sur **OK** pour refermer la boîte de dialogue.
9. Sélectionnez l'entrée **Websense DC Agent** dans la boîte de dialogue Services, puis cliquez sur **Démarrer**.
10. Répétez cette procédure pour chaque instance de Websense User Service.

Dépannage de Logon Agent

Si certains utilisateurs de votre réseau sont filtrés par la stratégie **Par défaut** parce que Logon Agent ne parvient pas à les identifier :

- Assurez-vous que les Objets de stratégie de groupe (GPO) s'appliquent correctement aux ordinateurs de ces utilisateurs (voir *Objets de stratégie de groupe*, page 373).
- Si User Service est installé sur un ordinateur Linux et que vous utilisez Windows Active Directory (Native Mode), vérifiez la configuration de votre service d'annuaire (voir *User Service sous Linux*, page 374).
- Vérifiez que l'ordinateur client peut communiquer avec le contrôleur de domaine à partir duquel le script de connexion est exécuté (voir *Visibilité du contrôleur de domaine*, page 374).
- Assurez-vous que NetBIOS soit activé sur l'ordinateur client (voir *NetBIOS*, page 374).
- Vérifiez que le profil d'utilisateur sur l'ordinateur client n'est pas corrompu (voir *Problèmes des profils utilisateur*, page 375).

Objets de stratégie de groupe

Après avoir vérifié que votre environnement répond aux conditions requises décrites dans le *Guide d'installation* de Websense, vérifiez que les Objets de stratégie de groupe sont appliqués correctement :

1. Sur l'ordinateur Active Directory, ouvrez le Panneau de configuration de Windows, puis sélectionnez **Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
2. Cliquez du bouton droit sur l'entrée du domaine, puis choisissez **Propriétés**.
3. Cliquez sur l'onglet **Stratégie de groupe**, puis sélectionnez la stratégie de domaine dans la liste Liens des objets de la stratégie de domaine du groupe.
4. Cliquez sur **Modifier**, puis développez le nœud Configuration utilisateur dans l'arborescence.
5. Développez le nœud Paramètres Windows et sélectionnez **Scripts**.
6. Dans le volet droit, double-cliquez sur **Connexion** et vérifiez que **logon.bat** est répertorié dans la boîte de dialogue Propriétés de connexion.

   Ce script est requis par l'application d'ouverture de session cliente.

- Si **logon.bat** n'est pas dans le script, reportez-vous au chapitre *Configuration initiale* de votre *Guide d'installation* de Websense.
- Si **logon.bat** apparaît bien dans le script mais que Logon Agent ne fonctionne pas, utilisez les autres procédures de dépannage de cette section pour vérifier la présence éventuelle d'un problème de connectivité réseau, ou consultez la Base de connaissances de Websense.

User Service sous Linux

Lorsque vous utilisez Logon Agent pour l'identification transparente des utilisateurs, et que User Service est installé sur un ordinateur Linux, vous devez configurer temporairement Websense pour qu'il communique avec Active Directory en mode mixte.

1. Dans Websense Manager, sélectionnez **Paramètres > Services d'annuaire**.
2. Notez les paramètres actuels de votre annuaire.
3. Sous Annuaires, sélectionnez **Annuaire Windows NT/Active Directory (Mixed Mode)**.
4. Cliquez sur **OK** pour mettre en cache vos modifications, puis cliquez sur **Enregistrer tout**.
5. Sous Annuaires, sélectionnez **Active Directory (Native Mode)**. Si votre configuration originale n'apparaît pas, servez-vous des notes relevées à l'étape 2 pour redéfinir vos paramètres d'annuaire. Reportez-vous à la section *Windows Active Directory (Native Mode)*, page 63 pour obtenir des instructions détaillées.
6. Lorsque vos modifications sont terminées, cliquez sur **OK**, puis sur **Enregistrer tout**.

Visibilité du contrôleur de domaine

Pour vérifier que l'ordinateur client peut communiquer avec le contrôleur de domaine :

1. Tentez d'associer un lecteur de l'ordinateur client au lecteur partagé racine du contrôleur de domaine. C'est dans cet emplacement que s'exécute habituellement le script de connexion et que réside **LogonApp.exe**.
2. Sur l'ordinateur client, ouvrez une invite de commande Windows et exécutez la commande suivante :

   ```
   net view /domain:<nom de domaine>
   ```

Si l'un de ces tests échoue, recherchez des solutions potentielles dans la documentation du système d'exploitation Windows. Le problème est lié à la connectivité du réseau et non à Websense.

NetBIOS

Pour que le script de connexion Websense s'exécute sur l'ordinateur de l'utilisateur, NetBIOS pour TCP/IP doit être activé et le service Assistance TCP/IP NetBIOS doit s'exécuter.

Vérifiez que NetBIOS pour TCP/IP est activé sur l'ordinateur client.

1. Cliquez du bouton droit sur **Favoris réseau** et choisissez **Propriétés**.
2. Cliquez du bouton droit sur **Connexion au réseau local** et choisissez **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** et cliquez sur **Propriétés**.
4. Cliquez sur **Avancé**.
5. Sélectionnez l'onglet **WINS** et vérifiez que l'option NetBIOS appropriée est définie.
6. Si vous modifiez un élément, cliquez sur **OK**, puis sur **OK** à deux reprises pour fermer les différentes boîtes de dialogue Propriétés et enregistrer vos modifications.

   Si aucune modification n'était nécessaire, cliquez sur **Annuler** pour fermer chacune des boîtes de dialogue sans apporter de modification.

Servez-vous de la boîte de dialogue Services de Windows pour vérifier que le service **Assistance TCP/IP NetBIOS** s'exécute sur l'ordinateur client (voir *Boîte de dialogue Services de Windows*, page 399). Le service Assistance TCP/IP NetBIOS s'exécute sous Windows 2000, Windows XP, Windows Server 2003 et Windows NT.

Problèmes des profils utilisateur

Si le profil utilisateur est corrompu sur l'ordinateur client, le script de connexion Websense (et les paramètres GPO de Windows) ne peuvent pas s'exécuter. Pour résoudre ce problème, recréez le profil utilisateur.

Lorsque vous recréez un profil utilisateur, le dossier Mes documents existant de l'utilisateur, ses Favoris et d'autres données et paramètres personnalisés ne sont pas automatiquement transférés vers le nouveau profil. Ne supprimez pas le profil corrompu existant avant d'avoir vérifié que le nouveau permet de résoudre le problème ni avant d'avoir copié les données existantes de l'utilisateur dans le nouveau profil.

Pour recréer le profil utilisateur :

1. Ouvrez une session sur l'ordinateur client avec des droits d'administrateur local.
2. Renommez le répertoire contenant le profil utilisateur :

   ```
   C:\Documents and Settings\<nom d'utilisateur>
   ```

3. Redémarrez l'ordinateur.
4. Ouvrez une session sur l'ordinateur sous le nom de l'utilisateur filtré. Un nouveau profil utilisateur est créé automatiquement.
5. Vérifiez que l'utilisateur est filtré comme prévu.
6. Copiez les données personnalisées (par exemple le contenu du dossier Mes documents) de l'ancien profil vers le nouveau. N'utilisez pas l'Assistant Transfert de fichiers et de paramètres qui pourrait transférer la corruption au nouveau profil.

Dépannage d'eDirectory Agent

Rubriques connexes :

- *Activation des diagnostics eDirectory Agent*, page 377
- *eDirectory Agent ne compte pas correctement les connexions au serveur eDirectory.*, page 377
- *Exécution d'eDirectory Agent en mode console*, page 378

Il arrive qu'un utilisateur ne soit pas filtré correctement si son nom d'utilisateur n'est pas transmis à eDirectory Agent. Si l'utilisateur ne se connecte pas au serveur Novell eDirectory, eDirectory Agent ne peut pas détecter la connexion. Cela se produit dans les cas suivants :

- L'utilisateur se connecte à un domaine qui n'est pas inclus dans le contexte racine par défaut pour les sessions de connexion d'utilisateur eDirectory. Ce contexte racine est défini à l'installation et doit correspondre au contexte racine spécifié pour Novell eDirectory à la page **Paramètres** > **Services d'annuaire**.
- L'utilisateur tente d'éviter l'invite de connexion pour contourner le filtrage Websense.
- L'utilisateur n'a pas de compte défini dans le serveur eDirectory.

Si l'utilisateur ne se connecte pas au serveur eDirectory, les stratégies utilisateur ne peuvent pas s'appliquer à cet utilisateur. La stratégie **Par défaut** est alors appliquée. Si des utilisateurs se connectent de façon anonyme sur des stations de travail partagées de votre réseau, configurez une stratégie de filtrage pour ces ordinateurs particuliers.

Pour déterminer si eDirectory Agent reçoit un nom d'utilisateur et identifie ce dernier :

1. Activez la journalisation eDirectory Agent selon les descriptions de la section *Activation des diagnostics eDirectory Agent*, page 377.
2. Ouvrez le fichier journal spécifié dans un éditeur de texte.
3. Recherchez l'entrée de l'utilisateur qui n'est pas filtré correctement.
4. Une entrée telle que celle présentée ci-dessous indique qu'eDirectory Agent a identifié un utilisateur :

   ```
   WsUserData::WsUserData()
   User: cn=Admin,o=novell (10.202.4.78)
   WsUserData::~WsUserData()
   ```

   Dans l'exemple ci-dessus, l'utilisateur **Admin** s'est connecté au serveur eDirectory et a bien été identifié.
5. Si l'utilisateur est identifié mais n'est toujours pas filtré comme prévu, vérifiez la configuration des stratégies pour vous assurer que la stratégie appropriée s'applique bien à cet utilisateur et que son nom dans Websense Manager correspond à son nom dans Novell eDirectory.

   Si l'utilisateur n'est *pas* identifié, vérifiez que :

   - L'utilisateur a un compte Novell eDirectory.

- L'utilisateur se connecte à un domaine inclus dans le contexte racine par défaut pour les ouvertures de session eDirectory.
- L'utilisateur ne contourne pas l'invite de connexion.

Activation des diagnostics eDirectory Agent

eDirectory Agent possède des capacités de diagnostic intégrées qui ne sont pas activées par défaut. Vous pouvez activer la journalisation et le débogage pendant l'installation ou au moment de votre choix.

1. Arrêtez eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 286).
2. Sur l'ordinateur eDirectory Agent, localisez le répertoire d'installation d'eDirectory Agent.
3. Ouvrez le fichier **wsedir.ini** dans un éditeur de texte.
4. Localisez la section **[eDirAgent]**.
5. Pour activer la journalisation et le débogage, définissez la valeur de **DebugMode** sur **On** :

   ```
   DebugMode=On
   ```

6. Pour définir le niveau de détails du journal, modifiez la ligne suivante :

   ```
   DebugLevel=<N>
   ```

   N peut être une valeur comprise entre 0 et 3, où 3 correspond au niveau le plus détaillé.
7. Modifiez la ligne **LogFile** pour spécifier le nom du fichier journal :

   ```
   LogFile=nomdufichier.txt
   ```

   Par défaut, la sortie du journal est envoyée à la console eDirectory Agent. Si vous exécutez l'agent en mode console (voir *Exécution d'eDirectory Agent en mode console*, page 378), vous pouvez conserver la valeur par défaut.
8. Enregistrez et fermez le fichier **wsedir.ini**.
9. Démarrez le service eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 286).

eDirectory Agent ne compte pas correctement les connexions au serveur eDirectory.

Si eDirectory Agent surveille plus de 1 000 utilisateurs du réseau alors qu'il n'affiche que 1 000 connexions au serveur Novell eDirectory, il est possible que le problème soit dû à une limite de l'API Windows chargée de transmettre les informations du serveur eDirectory à Websense eDirectory Agent. Cela ne se produit que très rarement.

Pour résoudre ce problème, ajoutez un paramètre dans le fichier **wsedir.ini** qui compte avec précision les connexions au serveur (Windows uniquement) :

1. Arrêtez le service Websense eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 286).

2. Localisez le répertoire Websense **bin** (par défaut, **C:\Program Files\Websense\bin**).
3. Ouvrez le fichier **wsedir.ini** dans un éditeur de texte.
4. Insérez une ligne vide, puis entrez :

   ```
   MaxConnNumber = <NNNN>
   ```

   Ici, *<NNNN>* correspond au nombre maximal de connexions potentielles au serveur Novell eDirectory. Par exemple, si votre réseau a 1 950 utilisateurs, vous pouvez entrer 2000 comme nombre maximal.
5. Enregistrez le fichier.
6. Redémarrez eDirectory Agent.

Exécution d'eDirectory Agent en mode console

1. Procédez de l'une des manières suivantes :
   - À l'invite de commande Windows (**Démarrer > Exécuter > cmd**), entrez la commande suivante :

     ```
     eDirectoryAgent.exe -c
     ```
   - À l'invite de commande Linux, entrez la commande :

     ```
     eDirectoryAgent -c
     ```
2. Lorsque vous êtes prêt(e) à arrêter l'agent, appuyez sur **Entrée**. L'exécution de l'agent s'arrête en quelques secondes.

Dépannage de RADIUS Agent

RADIUS Agent possède des capacités de diagnostic intégrées qui ne sont pas activées par défaut. Pour activer la journalisation et le débogage de RADIUS Agent :

1. Arrêtez le service RADIUS Agent (voir *Arrêt et démarrage des services Websense*, page 286).
2. Sur l'ordinateur RADIUS Agent, localisez le répertoire d'installation de l'agent (par défaut, **Websense\bin**).
3. Ouvrez le fichier **wsradius.ini** dans un éditeur de texte.
4. Localisez la section **[RADIUSAgent]**.
5. Pour activer la journalisation et le débogage, définissez la valeur de **DebugMode** sur **On** :

   ```
   DebugMode=On
   ```
6. Pour définir le niveau de détails du journal, modifiez la ligne suivante :

   ```
   DebugLevel=<N>
   ```

   N peut être une valeur comprise entre 0 et 3, où 3 correspond au niveau le plus détaillé.
7. Modifiez la ligne **LogFile** pour spécifier le nom du fichier de sortie :

   ```
   LogFile=nomdufichier.txt
   ```

Par défaut, la sortie du journal est envoyée à la console RADIUS Agent. Si vous exécutez l'agent en mode console (voir *Exécution de RADIUS Agent en mode console*, page 379), vous pouvez conserver la valeur par défaut.

8. Enregistrez et fermez le fichier **wsradius.ini**.
9. Démarrez le service RADIUS Agent (voir *Arrêt et démarrage des services Websense*, page 286).

Si des utilisateurs distants ne sont pas identifiés et filtrés comme prévu, la cause probable est un problème de communication entre RADIUS Agent et votre serveur RADIUS. Pour en déterminer la cause, examinez les erreurs dans les journaux de RADIUS Agent.

Exécution de RADIUS Agent en mode console

Pour démarrer RADIUS Agent en mode console (comme une application), entrez les éléments suivants :

- À l'invite de commande de Windows :

  ```
  RadiusAgent.exe -c
  ```

- À l'invite de commande de Linux :

  ```
  ./RadiusAgent -c
  ```

Pour arrêter l'agent à tout moment, appuyez de nouveau sur **Entrée**. L'arrêt de l'exécution de l'agent peut demander quelques secondes.

RADIUS Agent accepte les paramètres de ligne de commande suivants :

> **Remarque**
> Sous Linux, Websense, Inc. recommande d'utiliser le script fourni pour démarrer ou arrêter Websense RADIUS Agent (**WsRADIUSAgent start|stop**), au lieu des paramètres -r et -s.

Paramètre	Description
-i	Installe le service/démon RADIUS Agent.
-r	Exécute le service/démon RADIUS Agent.
-s	Arrête le service/démon RADIUS Agent.
-c	Exécute RADIUS Agent sous forme de processus d'application et non pas sous forme de service ou de démon. En mode console, RADIUS Agent peut être configuré pour envoyer la sortie du journal vers la console ou dans un fichier texte.
-v	Affiche le numéro de version de RADIUS Agent.
-? -h -help <*sans option*>	Affiche des informations d'utilisation sur la ligne de commande. Répertorie et décrit tous les paramètres de ligne de commande possibles.

Les utilisateurs distants ne sont pas invités à s'authentifier manuellement.

Si vous avez configuré les utilisateurs distants de sorte qu'ils s'authentifient manuellement lorsqu'ils accèdent à Internet, il peut arriver que certains d'entre eux ne soient pas invités à s'authentifier. Cela se produit lorsque des adresses IP du réseau ont été configurées pour ignorer l'authentification manuelle.

Lorsqu'un utilisateur distant accède au réseau, Websense lit la dernière partie de l'adresse MAC (Media Access Control) de l'ordinateur. Si celle-ci correspond à une adresse IP du réseau configurée pour ignorer l'authentification manuelle, l'utilisateur distant n'est pas invité à s'authentifier manuellement lorsqu'il accède à Internet.

La solution consiste à reconfigurer l'adresse IP réseau pour qu'elle utilise l'authentification manuelle. Une autre solution consiste à désactiver l'authentification manuelle pour l'utilisateur distant concerné.

Les utilisateurs distants ne sont pas filtrés correctement.

Si certains utilisateurs distants ne sont pas filtrés, ou pas filtrés par les stratégies qui leur sont attribuées, recherchez dans les journaux de RADIUS Agent le message **Error receiving from server: 10060** (Windows) ou **Error receiving from server: 0** (Linux).

Cela se produit généralement lorsque le serveur RADIUS ne reconnaît pas RADIUS Agent comme un client (source des requêtes RADIUS). Vérifiez que votre serveur RADIUS est correctement configuré (voir *Configuration de l'environnement RADIUS*, page 221).

Vous pouvez utiliser l'outil de diagnostic intégré de RADIUS Agent pour résoudre les problèmes de filtrage (voir *Dépannage de RADIUS Agent*, page 378).

Si vous avez implémenté la fonction Remote Filtering (voir *Filtrage des clients distants*, page 157), les utilisateurs distants ne sont pas filtrés si le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering sur le réseau.

Pour obtenir des instructions sur la configuration de Remote Filtering, consultez le document technique *Remote Filtering*.

Problèmes de messages de blocage

- *Un message de blocage de protocole s'affiche à la place de la page de blocage.*, page 383

Aucune page de blocage ne s'affiche pour un type de fichier bloqué.

Lorsque le blocage de types de fichiers est utilisé, le message de blocage n'est pas toujours visible pour l'utilisateur. Par exemple, lorsqu'un fichier téléchargeable fait partie d'une trame interne (IFRAME) dans un site autorisé, le message de blocage envoyé à cette trame n'est pas visible car la taille de la trame est égale à zéro.

Le problème provient uniquement de l'affichage. L'utilisateur ne peut pas accéder au fichier bloqué ni le télécharger.

Les utilisateurs reçoivent une erreur du navigateur à la place de la page de blocage.

Si les utilisateurs reçoivent un message d'erreur à la place d'une page de blocage, les deux causes les plus probables sont les suivantes :

- Le navigateur de l'utilisateur est configuré pour utiliser un proxy externe. La plupart des navigateurs permettent d'utiliser un proxy externe. Assurez-vous que le navigateur n'est pas configuré avec cette option.
- Il existe un problème d'identification ou de communication avec l'ordinateur Filtering Service.

Si les paramètres du navigateur de l'utilisateur sont corrects, vérifiez que l'adresse IP de l'ordinateur Filtering Service est correctement répertoriée dans le fichier **eimserver.ini**.

1. Arrêtez **Websense Filtering Service** (voir *Arrêt et démarrage des services Websense*, page 286).
2. Localisez le répertoire Websense **bin** (C:\Program Files\Websense\bin ou /opt/Websense/bin par défaut).
3. Ouvrez le fichier **eimserver.ini** dans un éditeur de texte.
4. Sous [WebsenseServer], insérez une ligne vide, puis entrez :

   ```
   BlockMsgServerName = <Adresse IP de Filtering Service>
   ```

   Par exemple, si l'adresse IP de Filtering Service est 10.201.72.15, entrez :

   ```
   BlockMsgServerName = 10.201.72.15
   ```

5. Enregistrez et fermez le fichier.
6. Redémarrez Filtering Service.

Si l'ordinateur Filtering Service a plusieurs cartes réseau et que la page de blocage ne s'affiche toujours pas correctement après la modification du fichier **eimserver.ini**, tentez d'utiliser les adresses IP des autres cartes réseau pour le paramètre **BlockMsgServerName**.

Si la page de blocage ne s'affiche toujours pas, assurez-vous que les utilisateurs puissent accéder en lecture aux fichiers des répertoires de pages de blocage de Websense :

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

Si le problème de page de blocage persiste, recherchez d'autres conseils de dépannage dans la Base de connaissances de Websense.

Une page blanche s'affiche à la place de la page de blocage.

Lorsque des publicités sont bloquées, ou lorsqu'un navigateur ne détecte pas correctement le code associé à une page de blocage, l'utilisateur peut recevoir une page blanche à la place de la page de blocage. Les causes potentielles de ce problème sont les suivantes :

- Lorsque la catégorie Publicités est bloquée, Websense confond parfois les requêtes de fichier graphique avec les requêtes de publicité, et affiche une image vierge à la place du message de blocage (méthode de blocage des publicités standard). Si l'URL demandée se termine par .gif ou toute autre extension similaire, l'utilisateur doit la saisir une nouvelle fois en ignorant la partie *.gif.
- Certains navigateurs plus anciens peuvent ne pas détecter l'encodage des pages de blocage. Pour que les caractères soient correctement détectés, configurez votre navigateur pour qu'il affiche le jeu de caractères approprié (UTF-8 pour le français, l'allemand, l'italien, l'espagnol, le Brésilien, le portugais, le chinois simplifié, le chinois traditionnel ou le coréen ; et Shift_JIS pour le japonais). Consultez la documentation de votre navigateur pour obtenir des instructions, ou mettez-le à niveau avec une version plus récente.

Les messages de blocage de protocole ne s'affichent pas comme prévu.

Les messages de blocage de protocoles peuvent ne pas apparaître, ou apparaître après un certain délai, pour les raisons suivantes :

- User Service doit être installé sur un ordinateur Windows pour que les messages de blocage de protocole s'affichent correctement. Pour plus d'informations, consultez le *Guide d'installation*.
- Les messages de blocage de protocole peuvent ne pas atteindre les ordinateurs client si Network Agent est installé sur un ordinateur disposant de plusieurs cartes réseau et que l'une d'elles ne surveille pas le même segment réseau que Filtering Service. Vérifiez que l'ordinateur Filtering Service dispose d'un accès par les protocoles NetBIOS et SMB (Server Message Block) aux ordinateurs client, et que le port 15871 n'est pas bloqué.
- Un message de blocage de protocole peut être légèrement retardé ou apparaître sur un ordinateur interne d'où proviennent les données de protocole demandées (et

non sur l'ordinateur client), lorsque Network Agent est configuré pour surveiller les requêtes **envoyées** aux ordinateurs internes.

- Si le client filtré ou l'ordinateur de filtrage Websense exécute Windows 200x, le service Windows **Messenger** doit s'exécuter pour que le message de blocage de protocole s'affiche. Dans la boîte de dialogue Services de Windows de l'ordinateur client ou du serveur, vérifiez que le service Messenger s'exécute (voir *Boîte de dialogue Services de Windows*, page 399). Même si le message de blocage ne s'affiche pas, les demandes de protocole restent bloquées.

Un message de blocage de protocole s'affiche à la place de la page de blocage.

Si votre produit d'intégration n'envoie pas d'informations HTTPS à Websense, ou si Websense s'exécute en mode autonome, Network Agent peut confondre une requête de site HTTPS bloquée par les paramètres des catégories avec une requête de protocole. Par conséquent, un message de blocage de protocole apparaît. La requête HTTPS est également journalisée en tant que requête de protocole.

Problèmes liés aux journaux, aux messages d'état et aux alertes

Où puis-je trouver les messages d'erreur liés aux composants de Websense ?

Lorsque des erreurs ou des avertissements sont liés aux principaux composants de Websense, de brefs messages d'alerte s'affichent dans la liste **Résumé sur les alertes d'état**, en haut de la page **État > Aujourd'hui** de Websense Manager (voir *Alertes d'état de Websense*, page 384).

- Cliquez sur un message d'alerte pour obtenir des informations détaillées dans la page **État > Alertes**.
- Cliquez sur **Solutions** à côté d'un message de la page État > Alertes pour obtenir de l'aide au dépannage.

Les erreurs, les avertissements et les messages provenant des composants de Websense, ainsi que les messages d'état du téléchargement de la base de données, sont stockés dans le fichier **websense.log** dans le répertoire **bin** de Websense (C:\Program Files\Websense\bin ou /opt/Websense/bin, par défaut). Voir *Fichier journal Websense*, page 400.

Dans le cas de composants Websense installés sur des ordinateurs Windows, vous pouvez également consulter l'Observateur d'événements de Windows. Voir *Observateur d'événements de Windows*, page 400.

Alertes d'état de Websense

Le Résumé sur les alertes d'état de Websense présente la liste des problèmes éventuellement rencontrés par les composants de Websense. Cela comprend :

- Filtering Service n'est pas en cours d'exécution.
- User Service n'est pas disponible.
- Log Server n'est pas en cours d'exécution.
- Aucun Log Server n'est configuré pour un serveur Policy Server.
- La base de données d'activité n'est pas disponible.
- Network Agent n'est pas en cours d'exécution.
- Aucun Network Agent n'est configuré pour un serveur Policy Server.
- Aucune carte réseau de surveillance n'est configurée pour un agent Network Agent.
- Aucun Filtering Service n'est configuré pour un agent Network Agent.
- La base de données de filtrage initial est utilisée.
- La base de données principale est téléchargée pour la première fois.
- Une mise à jour de la base de données principale est en cours.
- La base de données principale date de plus d'une semaine.
- Le téléchargement de la base de données principale a échoué.
- WebCatcher n'est pas actif.
- Il existe un problème d'abonnement.
- La clé d'abonnement arrive à expiration.
- Aucune clé d'abonnement n'a été saisie.

La page Alertes fournit des informations de base sur la condition de l'erreur ou de l'avertissement. Cliquez sur **Solutions** pour obtenir des informations sur la résolution du problème.

Dans certains cas, si vous recevez des messages d'erreur ou d'état relatifs à un composant que vous n'utilisez pas, ou que vous avez désactivé, vous pouvez choisir de masquer les messages d'alerte. Pour plus d'informations, consultez *Vérification de l'état du système en cours*, page 294.

Deux enregistrements de journal sont générés pour une seule requête.

Lorsque le Planificateur de paquets QoS de Windows est installé sur le même ordinateur que Network Agent, deux requêtes sont journalisées pour chaque requête

HTTP ou de protocole provenant de l'ordinateur Network Agent. (Cette duplication ne se produit pas avec les requêtes provenant des ordinateurs client de votre réseau.)

Pour résoudre ce problème, désactivez le Planificateur de paquets QoS de Windows sur l'ordinateur Network Agent.

Ce problème ne se produit pas si vous utilisez Network Agent pour toutes les journalisations. Pour plus d'informations, consultez la section *Configuration des paramètres des cartes réseau*, page 349.

Problèmes liés à Policy Server et à la base de données de stratégies

J'ai oublié mon mot de passe.

Si vous êtes un Super administrateur ou un administrateur délégué qui utilise un compte utilisateur Websense pour se connecter à Policy Server via Websense Manager, tout Super administrateur inconditionnel peut réinitialiser le mot de passe.

- Le mot de passe WebsenseAdministrator est défini à la page **Paramètres > Compte**.
- Les autres mots de passe de compte administrateur sont définis à la page **Administration déléguée > Gérer les comptes utilisateur Websense**.

Si vous n'utilisez pas l'administration déléguée et que vous avez oublié le mot de passe WebsenseAdministrator, connectez-vous à MyWebsense pour le réinitialiser.

- La clé d'abonnement associée au compte MyWebsense doit correspondre à votre actuelle clé d'abonnement Websense Web Security ou Websense Web Filter.
- Si vous avez plusieurs clés d'abonnement, vous devez sélectionner la clé Websense Web Security ou Websense Web Filter appropriée pour pouvoir réinitialiser le mot de passe.
- Vous devez accéder à l'ordinateur Websense Manager pour mener à bien le processus de réinitialisation.

Je ne peux pas me connecter à Policy Server.

Vérifiez que l'adresse IP du serveur Policy Server sélectionné est correcte. Si l'adresse de l'ordinateur Policy Server a changé depuis son ajout à Websense Manager, vous devrez vous connecter à un autre Policy Server, supprimer l'ancienne adresse IP dans Websense Manager, puis ajouter la nouvelle adresse IP de Policy Server. Voir *Ajout et modification des instances de Policy Server*, page 278.

Si Websense Manager s'est arrêté soudainement, ou a été arrêté via les commandes kill (Linux) ou Fin de tâche (Windows), attendez quelques minutes avant de vous reconnecter. Websense détecte et ferme la session terminée en moins de 3 minutes.

Le service Websense Policy Database ne démarre pas.

Le service Websense Policy Database s'exécute en tant que compte spécial : **WebsenseDBUser**. Si ce compte rencontre des problèmes de connexion, la base de données de stratégies ne peut pas démarrer.

Pour résoudre ce problème, modifiez le mot de passe WebsenseDBUser.

1. Ouvrez une session sur l'ordinateur Policy Database avec des droits d'administrateur local.
2. Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Gestion de l'ordinateur**.
3. Dans le panneau de navigation, sous Outils système, développez **Utilisateurs et groupes locaux**, puis sélectionnez **Utilisateurs**. Les informations de l'utilisateur apparaissent dans le panneau de contenu.
4. Cliquez du bouton droit sur **WebsenseDBUser** et sélectionnez **Définir le mot de passe**.
5. Entrez et confirmez le nouveau mot de passe de ce compte utilisateur, puis cliquez sur **OK**.
6. Fermez la boîte de dialogue Gestion de l'ordinateur.
7. Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Services**.
8. Cliquez du bouton droit sur **Websense Policy Database** et choisissez **Propriétés**.
9. Dans l'onglet Connexion de la boîte de dialogue Propriétés, entrez les nouvelles informations du mot de passe WebsenseDBUser, puis cliquez sur **OK**.
10. Cliquez de nouveau du bouton droit sur Websense Policy Database et sélectionnez **Démarrer**.

    Lorsque le service a démarré, fermez la boîte de dialogue Services.

Problèmes d'administration déléguée

- *Les clients gérés ne peuvent pas être supprimés du rôle.*, page 387
- *Une erreur de connexion indique que quelqu'un d'autre est connecté à mon ordinateur.*, page 387
- *Certains utilisateurs ne peuvent pas accéder à un site de la liste URL non filtrées.*, page 387
- *Les sites recatégorisés ne sont pas filtrés par la catégorie appropriée.*, page 387
- *Je ne peux pas créer de protocole personnalisé.*, page 388

Les clients gérés ne peuvent pas être supprimés du rôle.

Les clients ne peuvent pas être supprimés directement de la liste des clients gérés de la page Administration déléguée >Modifier le rôle si :

- L'administrateur a appliqué une stratégie au client.
- L'administrateur a appliqué une stratégie à un ou plusieurs membres d'un réseau, d'un groupe, d'un domaine ou d'une unité d'organisation.

Des problèmes peuvent également survenir si, lors de la connexion à Websense Manager, le Super administrateur choisit un autre serveur Policy Server que celui qui communique avec le service d'annuaire contenant les clients à supprimer. Dans ce cas, le serveur Policy Server et le service d'annuaire en cours ne reconnaissent pas les clients.

Pour plus d'informations sur la suppression de clients gérés, consultez la section *Suppression de clients gérés*, page 265.

Une erreur de connexion indique que quelqu'un d'autre est connecté à mon ordinateur.

Lorsque vous tentez de vous connecter à Websense Manager, il peut arriver que vous receviez l'erreur « Échec de la connexion. Le rôle <nom du rôle> est utilisé par <nom d'utilisateur>, depuis <date, heure>, sur l'ordinateur 127.0.0.1. ». L'adresse IP 127.0.0.1 est également appelée adresse de bouclage et désigne généralement l'ordinateur local.

Ce message signifie que quelqu'un est connecté à l'ordinateur d'installation de Websense Manager, dans le rôle même que vous demandez. Vous pouvez alors sélectionner un autre rôle (si vous en administrez plusieurs), vous connecter pour la génération de rapports uniquement, ou attendre que l'autre administrateur se déconnecte.

Certains utilisateurs ne peuvent pas accéder à un site de la liste URL non filtrées.

Les URL non filtrées n'affectent que les clients gérés par le rôle dans lequel les URL sont ajoutées. Par exemple, si un Super administrateur ajoute des URL non filtrées, les clients gérés par les rôles d'administration déléguée ne peuvent pas accéder à ces sites.

Pour que le site soit accessible aux clients d'autres rôles, le Super administrateur peut passer à chaque rôle et ajouter les sites appropriés dans leur liste URL non filtrées.

Les sites recatégorisés ne sont pas filtrés par la catégorie appropriée.

Les URL recatégorisées n'affectent que les clients gérés par le rôle dans lequel les URL sont ajoutées. Par exemple, si un Super administrateur ajoute des URL

recatégorisées, les clients gérés par les rôles d'administration déléguée continuent à être filtrés selon la catégorie Base de données principale de ces sites.

Pour appliquer la recatégorisation aux clients d'autres rôles, le Super administrateur peut passer à chaque rôle et recatégoriser leurs sites.

Je ne peux pas créer de protocole personnalisé.

Seuls les Super administrateurs peuvent créer des protocoles personnalisés. Les administrateurs délégués peuvent cependant définir des actions de filtrage pour les protocoles personnalisés.

Lorsque des Super administrateurs créent des protocoles personnalisés, ils doivent définir l'action par défaut appropriée pour la plupart des clients. Ils doivent ensuite signaler le nouveau protocole aux administrateurs délégués de sorte qu'ils puissent mettre à jour les filtres de leur rôle, le cas échéant.

Problèmes liés à la génération de rapports

Log Server n'est pas en cours d'exécution.

Si Log Server ne fonctionne pas, ou si d'autres composants de Websense ne peuvent pas communiquer avec Log Server, les informations d'utilisation Internet ne sont pas stockées et il est possible que vous ne puissiez pas générer de rapports sur l'utilisation d'Internet.

Log Server peut être indisponible dans les cas suivants :

- L'ordinateur Log Server ne dispose pas de suffisamment d'espace disque.
- Vous avez modifié le mot de passe Microsoft SQL Server ou MSDE sans mettre à jour la configuration ODBC ou Log Server.
- Il s'est écoulé plus de 14 jours depuis le dernier téléchargement réussi de la base de données principale.
- Le fichier logserver.ini est manquant ou corrompu.
- Vous avez arrêté Log Server pour éviter la journalisation des informations de l'utilisation d'Internet.

Pour résoudre le problème :

- Vérifiez la quantité d'espace disque disponible et supprimez au besoin les fichiers devenus inutiles.
- Si vous pensez que la modification du mot de passe est à l'origine du problème, consultez la section *Mise à jour du mot de passe de connexion à Log Server*, page 393.
- Naviguez jusqu'au répertoire **bin** de Websense (par défaut, C:\Program Files\Websense\bin), et vérifiez que vous pouvez ouvrir le fichier **logserver.ini** dans un éditeur de texte. Si ce fichier est corrompu, remplacez-le par un fichier de sauvegarde.
- Ouvrez la boîte de dialogue Services de Windows pour vérifier que Log Server s'exécute et, si nécessaire, redémarrez le service (voir *Arrêt et démarrage des services Websense*, page 286).
- Regardez dans l'Observateur d'événements de Windows ou dans le fichier **websense.log** si des messages d'erreur sont liés au service Log Server (voir *Outils de dépannage*, page 399).

Aucun Log Server n'est installé pour un serveur Policy Server.

Websense Log Server collecte des informations sur l'utilisation Internet et les stocke dans la base de données d'activité en vue de leur utilisation dans les rapports d'investigation et de présentation et les graphiques et résumés des pages Aujourd'hui et Historique de Websense Manager.

Pour pouvoir générer des rapports, Log Server doit être installé.

Ce message peut s'afficher si :

- Log Server n'est pas installé sur le même ordinateur que Policy Server et l'adresse IP de Log Server n'est pas correctement définie sur localhost dans Websense Manager.

- Log Server est installé sur un ordinateur Linux.
- Vous n'utilisez pas les outils de génération de rapports de Websense.

Pour vérifier que l'adresse IP de Log Server IP est bien définie dans Websense Manager :

1. Cliquez sur l'onglet **Paramètres** dans le panneau de navigation, puis sur **Général > Journalisation**.
2. Entrez l'adresse IP ou le nom de l'ordinateur Log Server dans le champ **Adresse IP ou nom de Log Server**.
3. Cliquez sur **OK** pour mettre vos modifications en cache, puis cliquez sur **Enregistrer tout**.

Si Log Server est installé sur un ordinateur Linux, ou si vous n'utilisez pas les outils de génération de rapports de Websense, vous pouvez masquer le message d'alerte dans Websense Manager.

1. Cliquez sur l'onglet Principal dans le panneau de navigation, puis sur **État > Alertes**.
2. Sous Alertes actives, cliquez sur **Avancé**.
3. Activez l'option **Masquer cette alerte** pour le message « Aucun serveur Log Server installé ».
4. Cliquez sur **Enregistrer maintenant**. Les modifications sont implémentées immédiatement.

La base de données d'activité n'a pas été créée.

Il arrive parfois que le programme d'installation ne puisse pas créer la base de données d'activité. La liste suivante décrit les causes et les solutions les plus courantes.

Problème :	Un ou des fichiers existants utilisent les noms employés par Websense pour la base de données d'activité (wslogdb70 et wslogdb70_1). Cependant, les fichiers ne sont pas correctement connectés au moteur de base de données et ne peuvent donc pas être utilisés par le programme d'installation de Websense.
Solution :	Supprimez ou renommez les fichiers existants, puis exécutez de nouveau le programme d'installation.
Problème :	Le compte utilisé pour l'installation ne dispose pas des autorisations adéquates sur le lecteur où est installée la base de données.
Solution :	Actualisez le compte de connexion pour qu'il dispose d'autorisations de lecture et d'écriture sur l'emplacement d'installation, ou connectez-vous avec un autre compte qui dispose de ces autorisations. Réexécutez ensuite le programme d'installation.
Problème :	L'emplacement spécifié ne contient pas suffisamment d'espace disque pour créer et gérer la base de données d'activité.

Solution :	Libérez suffisamment d'espace sur le disque sélectionné pour installer et gérer la base de données d'activité. Réexécutez ensuite le programme d'installation. Vous pouvez également choisir un autre emplacement.
Problème :	Le compte de connexion utilisé pour l'installation ne dispose pas des autorisations SQL Server adéquates pour créer une base de données.
Solution :	Actualisez le compte de connexion ou connectez-vous avec un compte qui dispose déjà des autorisations requises. Réexécutez ensuite le programme d'installation. Les autorisations nécessaires dépendent de la version de Microsoft SQL Server : ■ SQL Server 2000 ou MSDE : autorisations **dbo** (propriétaire de la base de données) requises ■ SQL Server 2005 : autorisations **dbo** et **SQLServerAgentReader** requises

La base de données d'activité n'est pas disponible.

La base de données d'activité Websense stocke les informations sur l'utilisation Internet en vue de leur utilisation dans les rapports d'investigation et de présentation et les graphiques et résumés des pages Aujourd'hui et Historique de Websense Manager.

Si Websense ne peut pas se connecter à la base de données d'activité, commencez par vérifier que le moteur de base de données (Microsoft SQL Server ou Microsoft SQL Server Desktop Engine [MSDE]) s'exécute sur l'ordinateur Log Database.

1. Dans la boîte de dialogue Services de Windows (voir *Boîte de dialogue Services de Windows*, page 399), vérifiez que les services suivants s'exécutent :
   - Microsoft SQL Server :
     - MSSQLSERVER
     - SQLSERVERAGENT
   - Microsoft SQL Desktop Engine (MSDE) :
     - MSSQL$WEBSENSE (si vous avez obtenu MSDE par Websense, Inc.)
     - SQLAgent$WEBSENSE
2. Si un service est arrêté, cliquez du bouton droit sur son nom et cliquez sur **Démarrer**.

   Si le service ne redémarre pas, regardez dans l'Observateur d'événements de Windows (voir *Observateur d'événements de Windows*, page 400) si des erreurs et des avertissements sont liés à Microsoft SQL Server ou MSDE.

Si le moteur de base de données s'exécute :

- Vérifiez que SQL Server Agent s'exécute sur l'ordinateur où s'exécute le moteur de base de données.
- Dans la boîte de dialogue Services de Windows, vérifiez que le service **Websense Log Server** s'exécute.

- Si Log Server et la base de données d'activité sont installés sur des ordinateurs différents, assurez-vous que ces deux ordinateurs s'exécutent et que la connexion réseau qui les relie fonctionne.
- Assurez-vous qu'il y ait suffisamment d'espace disque sur l'ordinateur de la base de données d'activité et que suffisamment d'espace disque ait été alloué à celle-ci (voir *Log Server n'enregistre rien dans la base de données d'activité.*, page 392).
- Vérifiez que le mot de passe Microsoft SQL Server ou MSDE n'a pas été modifié. Si le mot de passe a été modifié, vous devez actualiser les informations de mot de passe utilisées par Log Server pour se connecter à la base de données. Voir *Mise à jour du mot de passe de connexion à Log Server*, page 393.

Taille de la base de données d'activité

La taille de la base de données d'activité est toujours un problème. Si vous avez déjà généré des rapports Websense avec succès et que vous remarquez à présent que l'affichage des rapports est plus long, ou si votre navigateur Web commence à vous envoyer des messages d'expiration, envisagez de désactiver certaines partitions de la base de données.

1. Dans Websense Manager, sélectionnez **Paramètres > Génération de rapports > Base de données d'activité**.
2. Localisez la section **Partitions disponibles** de la page.
3. Désactivez la case à cocher **Activer** des partitions non nécessaires pour les opérations de génération de rapports en cours.
4. Cliquez sur **Enregistrer maintenant** pour implémenter les modifications.

Log Server n'enregistre rien dans la base de données d'activité.

De façon générale, si Log Server ne peut pas écrire de données dans la base de données d'activité, c'est que celle-ci ne dispose plus de suffisamment d'espace disque. Cela se produit lorsque le disque est plein ou, dans le cas de Microsoft SQL Server, si une taille maximale a été définie pour la croissance de la base de données.

Si le lecteur qui héberge la base de données d'activité est plein, vous devez accroître l'espace disque de l'ordinateur pour restaurer la journalisation.

Si votre administrateur de base de données SQL Server a défini une taille maximale de croissance potentielle pour une base de données individuelle dans Microsoft SQL Server, effectuez l'une des opérations suivantes :

- Demandez à votre administrateur de bases de données SQL Server d'augmenter la taille maximale.
- Identifiez la taille maximale et ouvrez la page **Paramètres > Génération de rapports > Base de données d'activité** pour configurer la base de données d'activité de sorte qu'elle utilise le remplacement lorsqu'elle atteint environ 90 % de la taille maximale. Voir *Configuration des options de remplacement*, page 325.

Si votre service informatique a défini une quantité d'espace disque maximale pour les opérations SQL Server, demandez-leur de l'aide.

Mise à jour du mot de passe de connexion à Log Server

Si vous modifiez le mot de passe du compte utilisé par Websense pour se connecter à la base de données d'activité, vous devez également actualiser Log Server pour qu'il utilise le nouveau mot de passe.

1. Sur l'ordinateur Log Server, sélectionnez **Démarrer > Tous les programmes > Websense > Utilitaires > Configuration de Log Server**. L'utilitaire Configuration de Log Server apparaît.
2. Cliquez sur l'onglet **Base de données** et vérifiez que la base de données appropriée (par défaut, **wslogdb70**) s'affiche dans le champ Nom de la source de données ODBC (DSN).
3. Cliquez sur **Connexion**. La boîte de dialogue Sélectionner la source de données apparaît.
4. Cliquez sur l'onglet **Source de données machine**, puis double-cliquez sur **wslogdb70** (ou sur le nom de votre base de données d'activité). La boîte de dialogue Connexion SQL Server apparaît.
5. Vérifiez que le champ ID de connexion contient le nom du compte approprié (généralement **sa**), puis entrez le nouveau mot de passe.
6. Cliquez sur **OK** puis sur **Appliquer** dans la boîte de dialogue Configuration de Log Server.
7. Sélectionnez l'onglet **Connexion**, puis arrêtez et redémarrez Log Server.
8. Lorsque Log Server s'exécute à nouveau, cliquez sur **OK** pour fermer l'utilitaire.

Configuration des autorisations d'utilisateur pour Microsoft SQL Server 2005

Microsoft SQL Server 2005 définit desrôles SQL Server Agent qui gèrent l'accès à la structure des travaux. Les travaux SQL Server Agent pour SQL Server 2005 sont stockés dans la base de données SQL Server msdb.

Pour installer Websense Log Server avec succès, le compte utilisateur qui possède la base de données Websense doit appartenir à l'un des rôles suivants dans la base de données msdb :

- Rôle SQLAgentUser
- Rôle SQLAgentReader
- Rôle SQLAgentOperator

> **Remarque**
> Le compte utilisateur SQL doit également être membre du rôle de serveur fixe *DBCreator*.

Ouvrez Microsoft SQL Server 2005 pour accorder au compte utilisateur SQL Server les autorisations nécessaires pour installer les composants de la génération de rapports de Websense.

1. Sur l'ordinateur SQL Server, sélectionnez **Démarrer > Tous les programmes > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**.
2. Sélectionnez l'arborescence **Explorateur d'objets**.
3. Sélectionnez **Sécurité > Connexions**.
4. Sélectionnez le compte de connexion à utiliser pour l'installation.
5. Cliquez du bouton droit sur le compte de connexion et sélectionnez **Propriétés** pour cet utilisateur.
6. Sélectionnez **Mappage utilisateur** et procédez comme suit :
   a. Sélectionnez **msdb** dans le mappage des bases de données.
   b. Accordez l'appartenance à l'un des rôles suivants :
      - Rôle SQLAgentUser
      - Rôle SQLAgentReader
      - Rôle SQLAgentOperator
   c. Cliquez sur **OK**.
7. Sélectionnez **Rôles du serveur**, puis **dbcreator**. Le rôle dbcreator est créé.
8. Cliquez sur **OK**.

Log Server ne peut pas se connecter au service d'annuaire.

Si l'une des erreurs énumérée ci-dessous ce produit, Log Server ne peut pas accéder au service d'annuaire, alors que cet accès est nécessaire pour la mise à jour des correspondances utilisateur/groupe pour les rapports. Ces erreurs s'affichent dans l'Observateur d'événements de Windows (voir *Observateur d'événements de Windows*, page 400).

- EVENT ID:4096 - Impossible d'initialiser le service d'annuaire. Websense Server est peut-être inactif ou inaccessible.
- EVENT ID:4096 - Impossible de se connecter au service d'annuaire. Les groupes pour cet utilisateur ne seront pas résolus pour l'instant. Vérifiez que ce processus peut accéder au service d'annuaire.

La cause la plus courante est que Websense Log Server et Websense User Service sont installés de part et d'autre d'un pare-feu qui limite l'accès.

Pour résoudre ce problème, configurez le pare-feu de sorte qu'il autorise l'accès par les ports utilisés pour la communication entre ces composants.

Les données des rapports du temps de navigation sur Internet sont déréglées.

N'oubliez pas que la consolidation peut dérégler les données des rapports de Temps de navigation sur Internet. Ces rapports indiquent le temps passé par les utilisateurs sur Internet et peuvent détailler le temps consacré à chaque site. Le temps de navigation sur Internet est calculé à partir d'un algorithme spécial et l'activation de la consolidation peut dérégler la précision des calculs pour ces rapports.

La bande passante est plus importante que prévu.

La plupart des intégrations Websense, mais pas toutes, fournissent des informations sur la bande passante. Si votre intégration ne fournit pas d'informations sur la bande passante, vous pouvez configurer Network Agent pour qu'il exécute la journalisation en incluant les données de bande passante.

Lorsqu'un utilisateur demande à télécharger un fichier autorisé, le produit d'intégration ou Network Agent envoie la taille complète du fichier, que Websense enregistre sous forme d'octets reçus.

Si l'utilisateur annule ensuite le téléchargement, ou si le fichier n'est pas téléchargé dans son intégralité, la valeur des octets reçus dans la base de données d'activité représente toujours la taille complète du fichier. Dans ce cas, le nombre d'octets rapportés est supérieur au nombre d'octets véritablement reçus.

Cela affecte également les valeurs de bande passante indiquée, qui représentent une combinaison des octets reçus et des octets envoyés.

Certaines requêtes de protocoles ne sont pas enregistrées.

Quelques protocoles, tels que ceux qu'utilisent ICQ et AOL, invitent les utilisateurs à se connecter à un serveur disposant d'une adresse IP, puis envoient une adresse IP d'identification et un numéro de port différents au client pour la messagerie. Dans ce cas, il est possible que tous les messages envoyés et reçus ne soient pas surveillés et enregistrés par Websense Network Agent car le serveur de messagerie est inconnu lors de l'échange des messages.

Par conséquent, le nombre de requêtes enregistrées peut ne pas correspondre au nombre de requêtes réellement envoyées. La précision des rapports produits par les outils de Websense en est affectée.

Tous les rapports sont vides.

Si vos rapports ne contiennent aucune donnée, vérifiez que :

- Les partitions de base de données actives comprennent des informations pour les dates incluses dans les rapports. Voir *Partitions de base de données*, page 395.
- Le travail SQL Server Agent est actif dans Microsoft SQL Server ou MSDE. Voir *Travail SQL Server Agent*, page 396.
- Log Server est configuré pour recevoir les informations de journal de Filtering Service. Voir *Configuration de Log Server*, page 396.

Partitions de base de données

Tous les enregistrements de journal Websense sont stockés dans des partitions de la base de données. De nouvelles partitions peuvent être créées en fonction de la taille ou de la date, selon votre configuration et votre moteur de base de données.

Vous pouvez activer ou désactiver des partitions individuelles dans Websense Manager. Si vous tentez de générer un rapport à partir des informations stockées dans des partitions désactivées, aucune information n'est détectée et le rapport sera vide.

Pour vérifier que les partitions de base de données appropriées sont actives :

1. Sélectionnez **Paramètres > Génération de rapports > Base de données d'activité**.
2. Localisez la section **Partitions disponibles**.
3. Cochez la case **Activer** de chaque partition contenant des données à inclure dans les rapports.
4. Cliquez sur **Enregistrer maintenant** pour implémenter les modifications.

Travail SQL Server Agent

Il est possible que le travail de base de données SQL Server Agent ait été désactivé. Ce travail doit s'exécuter pour que les enregistrements de journal soient traités dans la base de données par le travail de base de données ETL.

Si vous utilisez MSDE :

1. Sélectionnez **Démarrer > Outils d'administration > Services**.
2. Assurez vous que SQL Server et SQL Server Agent soient en cours d'exécution. Si vous avez obtenu MSDE auprès de Websense, Inc., ces services sont appelés MSSQL$WEBSENSE et SQLAgent$WEBSENSE.

Si vous exécutez l'application Microsoft SQL Server complète, demandez à votre administrateur de base de données de vérifier que le travail SQL Server Agent s'exécute.

Configuration de Log Server

Pour être certain que Log Server reçoive des informations de journal de Filtering Service, les paramètres de configuration doivent être corrects dans Websense Manager et dans Log Server. Si ce n'est pas le cas, les données de journal ne sont jamais traitées dans la base de données d'activité.

D'abord, vérifiez que Websense Manager parvient à se connecter à Log Server.

1. Connectez-vous à Websense Manager avec des autorisations de Super administrateur inconditionnel.
2. Sélectionnez **Paramètres > Général > Journalisation**.
3. Entrez le **nom de la machine** ou **l'adresse IP** sur lequel est situé Log Server.
4. Entrez le **port** surveillé par Log Server (par défaut, 55805).
5. Cliquez sur **Vérifier l'état** pour déterminer si Websense Manager peut communiquer avec le Log Server spécifié.

   Un message indique si le test de la connexion a réussi. Actualisez l'adresse IP ou le nom d'ordinateur et le port, le cas échéant, jusqu'à ce que le test réussisse.

6. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Ces modifications ne seront pas implémentées tant que vous ne cliquez pas sur **Enregistrer tout**.

Ensuite, vérifiez les paramètres dans l'utilitaire de configuration de Log Server.

1. Sur l'ordinateur Log Server, sélectionnez **Démarrer > Tous les programmes > Websense > Utilitaires > Configuration de Log Server**.
2. Dans l'onglet **Connexions**, vérifiez que le Port correspond à la valeur saisie dans Websense Manager.
3. Cliquez sur **OK** pour enregistrer vos modifications.
4. Utilisez le bouton de l'onglet **Connexions** pour arrêter, puis démarrer Log Server.
5. Cliquez sur **Quitter** pour fermer l'utilitaire de configuration de Log Server.

Aucun graphique ne s'affiche dans les pages Aujourd'hui ou Historique.

Lorsque l'organisation utilise l'administration déléguée, examinez les autorisations de génération de rapports pour le rôle d'administrateur délégué. Si l'option **Afficher des rapports dans les pages Aujourd'hui et Historique** n'est pas activée, ces graphiques ne s'affichent pas pour les administrateurs délégués de ce rôle.

Dans les environnements qui utilisent plusieurs serveurs Policy Server, le serveur Log Server est installé de manière à ne communiquer qu'avec un seul serveur Policy Server. Vous devez vous connecter à ce serveur Policy Server pour afficher les graphiques sur les pages Aujourd'hui ou Historique ou pour accéder aux autres fonctions de rapports.

Impossible d'accéder à certaines fonctions de génération de rapports

Si les paramètres de blocage des fenêtres contextuelles de votre navigateur Web sont très stricts, ils peuvent bloquer certaines fonctions de la génération de rapports. Pour utiliser ces fonctions, vous devez réduire le niveau de blocage ou désactiver complètement le blocage des fenêtres contextuelles.

Certaines données de rapport n'apparaissent pas dans le document Microsoft Excel.

Le plus grand nombre de lignes pouvant être ouvert dans une feuille de calcul Microsoft Excel est 65 536. Si vous exportez un rapport contenant plus d'enregistrements au format Microsoft Excel, le 65 537ème enregistrement et les suivants ne sont pas disponibles dans la feuille de calcul.

Pour pouvoir accéder à toutes les informations dans le rapport exporté, effectuez l'une des opérations suivantes :

- Dans le cas de rapports de présentation, modifiez le filtre de manière à définir un rapport plus petit, éventuellement en réduisant la plage de dates, en sélectionnant moins d'utilisateurs et de groupes ou en sélectionnant moins d'actions.
- Dans le cas de rapports d'investigation, explorez les données de manière à définir un rapport plus petit.
- Sélectionnez un autre format d'exportation de rapport.

Enregistrement du résultat des rapports de présentation au format HTML

Si vous générez un rapport directement à partir de la page Génération de rapports > Rapports de présentation, vous avez le choix entre 3 formats d'affichage : HTML, PDF et XLS. Si vous choisissez le format HTML, vous pouvez afficher le rapport dans la fenêtre de Websense Manager.

L'impression et l'enregistrement des rapports de présentation à partir du navigateur ne sont pas conseillés. La sortie imprimée comprend l'intégralité de la fenêtre du navigateur et l'ouverture d'un fichier enregistré lance Websense Manager.

Pour imprimer ou enregistrer des rapports plus efficacement, choisissez le format PDF ou XLS. Vous pouvez ouvrir ces types de fichier immédiatement si le logiciel correspondant (Adobe Reader ou Microsoft Excel) est installé sur l'ordinateur local. Vous pouvez également enregistrer le fichier sur le disque (votre seule possibilité si le logiciel correspondant n'est pas disponible).

Après avoir ouvert un rapport dans Adobe Reader ou Microsoft Excel, servez-vous des options d'impression et d'enregistrement de ce programme pour obtenir le résultat désiré.

Problèmes de recherche dans les rapports d'investigation

Deux problèmes potentiels sont liés à la recherche dans les rapports d'investigation.

- Il est impossible de saisir des caractères ASCII étendus.
- Le modèle de recherche n'est pas détecté.

Caractères ASCII étendus

Les champs de recherche situés au-dessus du graphique à barres dans la page principale des rapports d'investigation vous permettent de rechercher un terme ou une chaîne de texte spécifique dans l'élément graphique sélectionné.

Si vous utilisez Mozilla Firefox sur un serveur Linux pour accéder à Websense Manager, vous ne pouvez pas saisir de caractères ASCII étendus dans ces champs. Il s'agit d'une limite connue de Firefox sous Linux.

Si vous devez rechercher une chaîne de texte comprenant des caractères ASCII étendus dans un rapport d'investigation, accédez à Websense Manager à partir d'un serveur Windows et utilisez un navigateur pris en charge.

Modèle de recherche introuvable

Il arrive parfois que des rapports d'investigation ne puissent pas trouver les URL associées à un modèle saisi dans les champs de recherche de la page principale des rapports d'investigation. Si cela se produit, et si vous êtes pratiquement certain(e) que ce modèle existe dans les URL rapportées, tentez de saisir un modèle différent qui vous permette également de trouver les URL recherchées.

Problèmes généraux liés aux rapports d'investigation

- Certaines requêtes sont très longues. Vous pouvez dans ce cas obtenir un écran vide ou un message indiquant que votre requête a expiré. Cela peut se produire pour les raisons suivantes :
  - Le serveur Web a expiré.
  - MSDE ou Microsoft SQL Server a expiré.
  - Le serveur proxy ou de mise en cache a expiré.

  Vous devrez peut-être augmenter manuellement le délai d'expiration de ces composants.
- Si les utilisateurs n'appartiennent à aucun groupe, ils n'apparaîtront pas non plus dans un domaine. Les choix Groupe et Domaine seront inactifs.
- Même si Log Server enregistre les visites à la place des accès, les rapports d'investigation appellent ces informations de journal des **Accès**.

Outils de dépannage

- *Boîte de dialogue Services de Windows*, page 399
- *Observateur d'événements de Windows*, page 400
- *Fichier journal Websense*, page 400

Boîte de dialogue Services de Windows

Sur les ordinateurs Microsoft Windows, Filtering Service, Network Agent, Policy Server, User Service et tous les agents de l'identification transparente de Websense s'exécutent en tant que services. Vous pouvez donc utiliser la boîte de dialogue Services de Windows pour vérifier leur état de fonctionnement.

1. Dans le Panneau de configuration de Windows, ouvrez le dossier **Outils d'administration**.
2. Double-cliquez sur **Services**.
3. Parcourez la liste des services pour localiser le service que vous souhaitez dépanner.

   L'entrée du service comprend le nom de ce dernier, une brève description, l'état du service (démarré ou arrêté), comment le service démarre et le compte utilisé par le service pour effectuer ses tâches.

4. Double-cliquez sur un nom de service pour ouvrir une boîte de dialogue de propriétés présentant davantage d'informations sur le service.

Observateur d'événements de Windows

L'Observateur d'événements de Windows enregistre les messages d'erreur relatifs aux événements Windows, y compris les activités des services. Ces messages peuvent vous aider à identifier des erreurs de réseau ou de service à l'origine de problèmes de filtrage Internet ou d'identification d'utilisateurs.

1. Dans le Panneau de configuration de Windows, ouvrez le dossier **Outils d'administration**.
2. Double-cliquez sur **Observateur d'événements**.
3. Dans l'Observateur d'événements, cliquez sur **Application** pour obtenir la liste des messages d'erreur, des avertissements et des messages d'information.
4. Parcourez la liste pour identifier les erreurs ou les avertissements provenant de services Websense.

Fichier journal Websense

Websense inscrit les messages d'erreur dans le fichier **websense.log**, situé dans le répertoire **bin** de Websense (C:\Program Files\Websense\bin ou /opt/Websense/bin, par défaut).

Les informations de ce fichier sont comparables à celles de l'Observateur d'événements de Windows. Dans les environnements Windows, l'Observateur d'événements présente les messages de façon plus conviviale. Le fichier **websense.log**, toutefois, est disponible sur les systèmes Linux et peut être envoyé au support technique de Websense si vous avez besoin d'aide pour résoudre un problème.

Index

B

C

F

G

H

I

J

N

O

R

S

T

W