Didacticiel de démarrage rapide pour les utilisateurs procédant à une mise à niveau

Solutions Websense® Web Security

v7.7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Publié en 2012
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.

Marques déposées

Websense est une marque déposée et TRITON est une marque commerciale 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 appartiennent à leurs propriétaires respectifs.

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

Oracle et Java sont des marques déposées d'Oracle et/ou de ses filiales. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

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 commerciales ou déposées d'Adobe Systems Incorporated aux États-Unis et/ou dans d'autres pays.

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 comporte un logiciel distribué par Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000. Apache Software Foundation. Tous droits réservés.

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

Table des matières

Rubrique 1 **Bienvenue 7**

Console TRITON™ Unified Security Center 7
Termes et concepts de référence. 10
Recherche d'informations dans TRITON - Web Security 12
Prise en charge des produits tiers 12

Rubrique 2 **Nouveautés de la Version 7 . . . . . 13**

Surveillance de l'état de Web Security 13
Vérification de la configuration de votre filtrage Websense 14
Création de rapports dans TRITON - Web Security 14
Gestion centralisée des informations des stratégies 15
Sauvegarde et restauration des informations des stratégies 16
Connexions simultanées des administrateurs 16
Identification des Super administrateurs conditionnels 17
Création d'exceptions aux paramètres d'identification des utilisateurs 17
Intégration à Websense Web Security Gateway 18

Rubrique 3 **Nouveautés de la Version 7.1 . . . . . 19**

Alertes d'état étendues 19
Protection de la fonction Save and Deploy (Enregistrer et déployer) 20
Modification des rapports de présentation 20
Nouveaux rapports de Websense Web Security Gateway 21

Rubrique 4 **Nouveautés de la Version 7.5 . . . . . 23**

Websense Web Security Gateway Anywhere 23
Sécurité Web hybride 24
Prévention des pertes de données via Internet 25
Présentation de TRITON - Web Security. 25
Priorités de la sécurité 26
Amélioration de la génération des rapports de présentation 27
Amélioration du résumé de l'historique 27
Nouveaux paramètres de Websense Web Security Gateway 28
Nouveaux rapports de Websense Web Security Gateway 29

Rubrique 5 **Nouveautés de la Version 7.6 . . . . . 31**

Amélioration de TRITON Unified Security Center 31

Présentation de Real-Time Monitor 32
Nouvelles plateformes pour la base de données d'activité. 33
Administration déléguée et génération de rapports 33
Nouvelles alertes de fonctionnement de DC Agent 35
Pages de blocage. 35
Filtrage basé sur l'état de la catégorie Risques de sécurité 36
Surveillance de l'état de Web Security 37
Prise en charge du Client Remote Filtering 64 bits 37
Gestion des clés de Policy Server. 37
Mise en cache de User Service. 38
Filtrage IPv6 38
Modification des alertes d'utilisation 38
Prise en charge des noms de domaine internationaux (IDN) 39
Accès à Content Gateway et alertes 39

Rubrique 6 **Nouveautés de la Version 7.7 . . . . . 41**

Amélioration du Tableau de bord de Web Security 42
Outils de protection contre le contenu malveillant avancé. 43
Déclenchement d'alertes en fonction de la gravité de l'activité Internet suspecte . . . 44
Exceptions : Listes blanche et noire d'URL. 44
Amélioration des rapports de présentation 45
Temps de navigation disponible dans les rapports d'investigation détaillés 46
Amélioration du blocage des types de fichiers. 47
Informations supplémentaires dans les pages de blocage 48
Configuration centralisée de Log Server 48
Amélioration de la configuration de la Base de données d'activité 49
Prise en charge étendue des ports SQL Server non standard 49
Prise en charge du cryptage SSL avec SQL Server 50
Amélioration de la configuration de DC Agent 50
Nouvelle identification transparente et journalisation des alertes de fonctionnement 51
Actions dépendant du temps dans les déploiements Filtering Service multiples. 52
Intégration aux solutions SIEM tierces 52
Filtrage des URL et des clients IPv6 53
Accès direct du Super administrateur à Content Gateway Manager 53
Amélioration de la configuration de Directory Agent 53
Génération de rapports d'agent utilisateur hybride et authentification personnalisée 54
Basculement vers le service hybride 55
Autres améliorations du service hybride 55

Rubrique 7 **Où puis-je trouver...? 57**

Ma stratégie Global 57
Mes jeux de catégories et de protocoles Default Settings 58
Pages Aujourd'hui et Historique 58
Mes listes d'acceptation 59
Mes URL personnalisées 59
Mes URL non filtrées 59
Mes objets d'annuaire. 59
Websense Explorer 60
Websense Reporter 60
Utilitaire de configuration de Log Server. 60
Mes rapports 60
Real-Time Analyzer 63
Mes paramètres de serveurs 63
Mes paramètres Network Agent locaux 63
Gestion des comptes d'administrateur 63
Détecteur de trafic réseau (Outil de visibilité du trafic) 64
Gestion des clés d'abonnement 64

Rubrique 8 **Procédures 67**

Téléchargement de la base de données principale 67
Ajout de clients. 68
Création d'une stratégie 69
Attribution d'une stratégie aux clients 69
Vérification de l'application de la stratégie appropriée 70
Création d'un rapport de présentation 70
Création d'un rapport d'investigation 71
Création ou modification d'une catégorie personnalisée 71
Recatégorisation d'une URL 72
Autorisation d'une URL pour tous les clients 72
Définition de mots-clés. 73
Utilisation des types de fichiers 73
Création de comptes Websense pour les administrateurs. 73
Connexion des administrateurs à l'aide des comptes réseau 74
Déplacement de clients d'un rôle à un autre 75
Gestion des paramètres du journal d'audit 76
Configuration du filtrage Web hybride 76
Prévention des pertes de données sur Internet 77

1 Bienvenue

Ce didacticiel de démarrage rapide vous permet de découvrir les nouvelles fonctionnalités et fonctions de votre logiciel Websense Web Security.

La section d'introduction présente les modifications de base importantes, quelles que soient les versions précédemment utilisées. Par exemple, au lieu de séparer les glossaires de chaque version, les termes ajoutés ou révisés dans chaque version depuis la version 7.0 sont présentés dans un même tableau.

Même si vous effectuez une mise à niveau à partir d'une version très récente, consultez les informations relatives aux modifications d'URL et aux plateformes prises en charge indiquées dans la présentation :

- *Console TRITON™ Unified Security Center*
- *Termes et concepts de référence*
- *Recherche d'informations dans TRITON - Web Security*
- *Prise en charge des produits tiers*

Les rubriques suivantes sont susceptibles de vous intéresser :

- *Nouveautés de la Version 7*
- *Nouveautés de la Version 7.1*
- *Nouveautés de la Version 7.5*
- *Nouveautés de la Version 7.6*
- *Nouveautés de la Version 7.7*
- *Où puis-je trouver...?*
- *Procédures*

Console TRITON™ Unified Security Center

TRITON Unified Security Center est une console de type navigateur qui permet d'exécuter des tâches de configuration, d'administration et de génération de rapports pour les logiciels et dispositifs Websense Web Security, Data Security et Email Security.

Pour accéder à la console TRITON depuis n'importe quel emplacement du réseau, ouvrez un navigateur pris en charge (Microsoft Internet Explorer 8 ou 9, Mozilla Firefox 4.x, 5.x ou 6.x ou Google Chrome 13 ou versions ultérieures) et saisissez l'URL suivante :

```
https://<adresse IP ou nom d'hôte>:9443/triton/
```

Remplacez <adresse IP ou nom d'hôte> par le nom ou l'emplacement de l'ordinateur TRITON - Web Security.

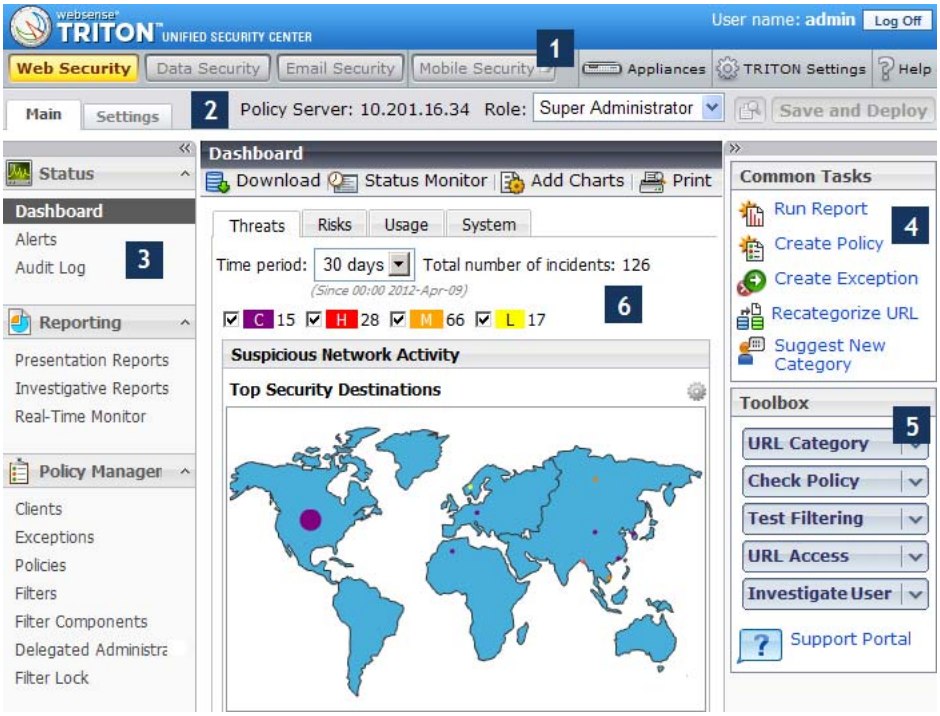
Tout administrateur disposant d'un accès Web Security à la console TRITON est dirigé vers la page **État > Tableau de bord** de Web Security après sa connexion. (Avant que le tableau de bord ne s'affiche, l'administrateur peut être invité à saisir une clé d'abonnement ou à lancer un didacticiel de démarrage rapide.)

Le tableau de bord Menaces présente des informations sur l'activité suspecte éventuellement liée à du contenu malveillant avancé dans votre réseau.

- Les Super administrateurs définissent les administrateurs délégués éventuellement autorisés à accéder au tableau de bord Menaces.
- Les administrateurs qui ne peuvent pas accéder au tableau de bord Menaces peuvent tout de même être autorisés à accéder aux tableaux de bord Risques, Usage et Système.
- Même les administrateurs non autorisés à consulter les informations des rapports du Tableau de bord Web Security ont accès à des informations d'état système limitées dans le tableau de bord Système.

Pour plus d'informations sur le Tableau de bord Web Security, consultez la section *Surveillance de l'état de Web Security*, page 13.

Comme les versions précédentes, TRITON - Web Security permet d'accéder aux outils de gestion des stratégies et aux paramètres de configuration de votre déploiement. Si vous avez effectué une mise à niveau à partir de la version 6.3.x ou d'une version antérieure, notez que cette console permet également d'accéder à tous les outils de génération de rapports. Voir *Création de rapports dans TRITON - Web Security*, page 14.



Légende

1 Dans la partie supérieure de l'écran :

- La **bannière** donne des informations sur votre session de connexion.
- La **barre d'outils TRITON** vous permet de passer aisément d'un module TRITON à l'autre, d'accéder aux dispositifs V-Series de votre réseau, de configurer les paramètres TRITON et d'obtenir de l'aide.

  Cliquez sur Aide > **Expliquer cette page** pour obtenir des informations détaillées sur les fonctions affichées dans le panneau de contenu. Le menu Aide permet également d'accéder au système d'aide de TRITON - Web Security, aux didacticiels de démarrage rapide destinés aux nouveaux utilisateurs et à ceux qui effectuent une mise à niveau, et à la Base de connaissances et aux forums Websense.

2 Juste au-dessous de la barre d'outils TRITON, la **barre d'outils Web Security** permet d'accéder aux fonctions disponibles, où que vous soyez dans l'interface :

- L'adresse IP de l'instance de Policy Server à laquelle vous êtes connecté est indiquée. Si votre déploiement comprend plusieurs instances de Policy Server, servez-vous de la liste déroulante pour passer d'une instance à l'autre.
- En général, les modifications sont mises en cache lorsque vous cliquez sur OK. Le bouton **Save and Deploy (Enregistrer et déployer)** change de couleur pour indiquer si des modifications mises en cache sont en attente d'enregistrement. Cliquez sur l'icône en forme de loupe (Afficher les modifications en attente) pour voir la liste des modifications actuellement mises en cache avant de procéder à leur enregistrement.

3 Servez-vous du panneau de navigation gauche pour accéder aux fonctionnalités et aux fonctions de TRITON - Web Security :

- L'onglet **Principal** permet d'accéder à toutes les tâches de gestion des stratégies et aux informations d'état, y compris aux journaux d'alertes et d'audit et aux outils de génération de rapports (si vous avez installé la génération de rapports sous Windows).
- L'onglet **Paramètres** permet d'accéder à la plupart des tâches de configuration de Websense, précédemment accessibles via le menu Serveur > Paramètres.

4 Les listes **Tâches communes** proposent des liens rapides vers les pages des tâches les plus fréquemment effectuées dans TRITON - Web Security. Le dernier lien, Suggérer une nouvelle catégorie, permet d'accéder au site MyWebsense où, après connexion, vous pouvez suggérer la recatégorisation d'un site dans la base de données principale.

5 La **Boîte à outils** permet d'identifier rapidement la catégorie d'un site, la stratégie appliquée à un client spécifique ou le type de filtrage appliqué à la requête spécifique d'un client donné, de savoir si une URL a été consultée depuis le réseau au cours des 14 derniers jours et d'identifier les sites demandés par un utilisateur au cours des 14 derniers jours. Les deux dernières requêtes génèrent un rapport d'investigation (appelé auparavant rapport Websense Explorer) avec des informations détaillées. Voir *Vérification de la configuration de votre filtrage Websense*, page 14.

6 Chaque fois que vous ouvrez TRITON - Web Security, la page **Tableau de bord > Menaces** présente l'activité suspecte éventuellement liée à la présence de contenu malveillant avancé dans votre réseau.

Termes et concepts de référence

Dans le cadre de notre effort permanent pour rendre TRITON Unified Security Center et ses modules plus intuitifs et cohérents, plusieurs concepts, composants de stratégie et fonctionnalités de Web Security ont été renommés. Par exemple, les jeux de catégories, les listes d'acceptation et les jeux de protocoles ayant des rôles similaires dans l'identification des stratégies de filtrage appliquées aux demandes des clients, ont été renommés respectivement filtres de catégories, filtres d'accès limité et filtres de protocoles, et sont appelés collectivement « filtres ».

Le tableau suivant présente une liste de références rapides qui vous aidera à identifier les fonctions dont le nom a changé. Cette liste comprend les modifications apportées dans les versions 7.0 à 7.7.

Ancien terme	Nouveau terme
Toujours bloquer (jeu de catégories)	Bloquer tout (filtre de catégories)
Jeu de catégories	Filtre de catégories
Continuer (option de filtrage)	Confirmer (action)
URL personnalisées (non filtrées)	Exceptions autorisées
URL personnalisées (recatégorisées)	URL recatégorisées
Rôle de génération de rapports délégué	Rôle de génération de rapports d'investigation
Objets d'annuaire	Utilisateurs ou clients d'annuaire (toutes les entrées d'annuaire—utilisateurs, groupes et domaines [unités d'organisation)—pouvant être ajoutées en tant que clients du filtrage)
Disposition	Action
Définitions des filtres	• Stratégies • Filtres (filtres de catégories, filtres de protocoles et filtres d'accès limité) • Filtrer les composants (catégories, protocoles, URL personnalisées, mots-clés et types de fichiers)
Option de filtrage	Action *ou* action de filtrage
Stratégie *Global	Stratégie Par défaut
page Historique	Tableau de bord Web Security (incluant également l'ancienne page Aujourd'hui)
Accès (utilisés dans les rapports)	Accès, *également* Requêtes ou demandes (termes génériques désignant les accès et les visites)
Utilitaire de configuration de Log Server	[abandonné], *remplacé par* Paramètres > Génération de rapports > Log Server (page de TRITON - Web Security)
Détecteur de trafic réseau (*ou* Outil de visibilité du trafic)	[abandonné]

Ancien terme	Nouveau terme
Ne jamais bloquer (jeu de catégories)	Autoriser tout (filtre de catégories)
Modèle	Expression régulière
Jeu de protocoles	Filtre de protocoles
Real-Time Analyzer	[abandonné], *remplacé par* Real-Time Monitor
Remote Administrator	Super administrateur conditionnel (Certaines autorisations d'administrateur ont été modifiées. Voir *Administration déléguée et génération de rapports*, page 33.)
Enregistrer tout (*ou* Enregistrer les modifications)	Save and Deploy (Enregistrer et déployer)
Enregistrer les modifications (*ou* Enregistrer tout)	Save and Deploy (Enregistrer et déployer)
Super administrateur	Super administrateur inconditionnel (accès à Web Security uniquement), *ou* Administrateur de la sécurité globale (accès à tous les modules TRITON)
page Aujourd'hui	Tableau de bord Web Security (incluant également l'ancienne page Historique)
Outil de visibilité du trafic (*ou* Détecteur de trafic réseau)	[abandonné]
URL non filtrées	Exceptions (autorisées)
Modèle d'URL	Expression régulière
Visites	Visites, *également* Requêtes ou demandes (termes génériques désignant les accès et les visites)
Web Filter Lock	Verrouillage du filtre
WebsenseAdministrator	admin (Administrateur de sécurité globale)
Websense Explorer	Rapports d'investigation
Websense Manager	TRITON - Web Security (module de TRITON Unified Security Center)
Websense Reporter	[abandonné], *remplacé par* Rapports de présentation
Station de travail (client)	Ordinateur
Liste d'acceptation	Filtre d'accès limité

Recherche d'informations dans TRITON - Web Security

Pour vous permettre d'exploiter au mieux votre logiciel Websense, TRITON - Web Security comprend 5 types d'Aide :

1	Une icône accompagne toutes les fonctions importantes du produit. Placez votre souris sur cette icône pour obtenir une brève description de la fonction.
2	Dans le cas des tâches complexes ou avancées, un texte d'aide s'affiche directement sur la page et fournit des directives ou d'autres conseils sur l'utilisation d'un outil ou d'un champ.
3	Des informations détaillées sur chaque page de TRITON - Web Security, comprenant souvent des instructions pour les procédures, sont également disponibles. Cliquez sur **Aide** dans la barre d'outils TRITON, puis sélectionnez **Expliquer cette page**.
4	Pour parcourir l'Aide de TRITON - Web Security, cliquez sur **Aide**, puis sur **Sommaire**. Le système d'aide s'affiche dans une nouvelle fenêtre de votre navigateur. Pour obtenir une version imprimée du système d'aide au format PDF, cliquez sur l'icône Adobe PDF située en haut et à gauche de toute page d'Aide. (Pour ouvrir ce fichier, Adobe Reader doit être installé.)
5	Si vous ne trouvez pas les informations nécessaires dans TRITON - Web Security, le menu **Aide** comprend des liens conduisant au Portail de support de Websense et à la source en ligne de toutes les ressources d'assistance techniques, des produits et des clients, y compris à la base de connaissances et aux forums des clients.

Prise en charge des produits tiers

Websense Web Security s'exécute sur un certain nombre de plateformes et communique avec divers produits tiers pour assurer les fonctions de gestion, le filtrage des URL, la gestion des stratégies basées sur l'utilisateur et la génération des rapports.

Des informations complètes sur l'intégration et l'interaction avec les produits tiers sont disponibles dans le Centre Installation et déploiement (disponible sur le site support.websense.com). Cette section présente brièvement les produits récemment ajoutés et les plateformes prises en charge.

Prise en charge des navigateurs

Dans la version 7.7, TRITON Unified Security Center (et tous les outils de génération de rapports) sont accessibles via les navigateurs suivants :

- Microsoft Internet Explorer versions 8 et 9
- Mozilla Firefox versions 4.x, 5.x et 6.x
- Google Chrome 13 et versions ultérieures

2 Nouveautés de la Version 7

Websense Web Security et Websense Web Filter versions 7.0 et ultérieures comprennent une interface de type navigateur qui simplifie la configuration et la gestion de votre logiciel Websense à partir de tout emplacement du réseau.

Si vous êtes habitué à une version précédente de Websense Manager, vous pouvez commencer par une présentation de la nouvelle interface :

- *Console TRITON™ Unified Security Center*, page 7
- *Termes et concepts de référence*, page 10

Votre logiciel Websense comprend également un certain nombre de nouvelles fonctions :

- *Surveillance de l'état de Web Security*, page 13
- *Vérification de la configuration de votre filtrage Websense*, page 14
- *Création de rapports dans TRITON - Web Security*, page 14
- *Gestion centralisée des informations des stratégies*, page 15
- *Sauvegarde et restauration des informations des stratégies*, page 16
- *Connexions simultanées des administrateurs*, page 16
- *Identification des Super administrateurs conditionnels*, page 17
- *Création d'exceptions aux paramètres d'identification des utilisateurs*, page 17
- *Intégration à Websense Web Security Gateway*, page 18

Surveillance de l'état de Web Security

Lorsque vous ouvrez TRITON - Web Security, la page **État > Tableau de bord** présente le tableau de bord **Menaces** qui résume les activités suspectes éventuellement liées à la présence de contenu malveillant avancé dans votre réseau.

Le Tableau de bord de Web Security comprend 3 autres onglets :

- L'onglet **Risques** donne des informations sur les requêtes autorisées et bloquées de la classe Risques de sécurité.
- L'onglet **Usage** présente l'activité Internet de votre réseau.
- L'onglet **Système** donne des informations générales sur le fonctionnement et l'état de votre déploiement.

Les Super administrateurs contrôlent les administrateurs délégués autorisés à accéder aux informations des rapports du tableau de bord.

Le Tableau de bord de la version 7.7 de Web Security ayant été profondément remanié, reportez-vous à la section *Nouveautés de la Version 7.7*, page 41, pour plus d'informations.

Vérification de la configuration de votre filtrage Websense

Le panneau de raccourcis placé à droite comprend une **Boîte à outils** qui vous permet de voir rapidement comment les sites sont catégorisés, comment les utilisateurs sont filtrés et d'autres informations sur la configuration du filtrage actuel.

Outil	Description
Catégorie d'URL	Découvrez comment un site est catégorisé. Entrez une URL, puis cliquez sur **Aller**. La catégorie du site s'affiche. Si l'URL a été recatégorisée, la nouvelle catégorie est affichée.
Vérifier la stratégie	Identifiez les stratégies actuellement appliquées à un client individuel. (Plusieurs stratégies peuvent être imposées lorsque l'utilisateur appartient à plusieurs groupes.) Entrez un nom d'utilisateur complet ou une adresse IP, puis cliquez sur **Aller**. La liste des stratégies s'affiche.
Tester le filtrage	Découvrez ce qu'il se passe lorsqu'un client spécifique demande un site particulier. Entrez d'abord une URL, puis le nom d'utilisateur complet ou l'adresse IP, et cliquez sur **Aller**. La catégorie du site, l'action appliquée à la catégorie et son motif s'affichent.
Accès à l'URL	Découvrez si des utilisateurs ont tenté d'accéder à un site au cours des deux dernières semaines. Entrez une URL, puis cliquez sur **Aller**. Un rapport d'investigation montre si des utilisateurs ont accédé à ce site et, dans l'affirmative, lesquels et quand. 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	Examinez l'historique de l'usage Internet d'un utilisateur au cours des 14 derniers jours. Saisissez un nom d'utilisateur complet ou partiel (si le filtrage par utilisateur s'applique) ou l'adresse IP (pour les requêtes provenant d'ordinateurs auxquels le filtrage par utilisateur ne s'applique pas), puis cliquez sur **Aller**. L'historique de l'utilisation du client apparaît dans un rapport d'investigation.

Création de rapports dans TRITON - Web Security

Tous les outils de génération de rapports de Websense Web Security ont été intégrés à la console TRITON. Comme les graphiques du Tableau de bord, les rapports d'investigation et de présentation exigent l'installation de Log Server, un composant réservé à Windows. (Real-Time Monitor, introduit avec la version 7.6, n'a pas besoin de Log Server mais obtient les informations relatives à l'activité du filtrage Internet de Usage Monitor. Voir *Présentation de Real-Time Monitor*, page 32.)

La page **Génération de rapports > Rapports de présentation** remplace l'application Websense Reporter. Cette page présente la liste des graphiques prédéfinis et des rapports tabulaires, illustrant chacun des informations spécifiques issues de la base de données d'activité.

- Exécutez un rapport de la liste des rapports prédéfinis.
- Servez-vous du bouton 'Enregistrer sous' pour copier un rapport prédéfini, puis modifiez son filtre pour spécifier les clients, les catégories, les protocoles et les actions à y inclure.
- Servez-vous du bouton Modifier pour actualiser le filtre appliqué à un rapport personnalisé.
- Désignez un rapport comme Favori pour pouvoir le retrouver plus rapidement dans la liste.
- Planifiez l'exécution ultérieure ou périodique des rapports, en choisissant un ou plusieurs destinataires pour le courrier électronique.

La page **Génération de rapports > Rapports d'investigation** remplace Websense Explorer. Cette page présente un graphique à barres résumé (présentant par défaut les accès par classe de risques). Cet outil fonctionne de la même façon que Websense Explorer, si ce n'est que vous y accédez depuis la console TRITON. Par exemple :

- Approfondissez certains détails en les sélectionnant directement dans le graphique.
- Développez le graphique à barres pour faire apparaître 2 niveaux de données.
- Servez-vous de la vue détaillée pour générer et modifier vos propres rapports tabulaires.
- Enregistrez un rapport sous forme de favori pour en planifier l'exécution régulière ou périodique.
- Examinez l'activité Internet d'un utilisateur particulier par jour ou par mois.

Gestion centralisée des informations des stratégies

Dans les versions précédentes de Websense, chaque serveur Policy Server stockait ses propres informations de configuration des stratégies et des clients. Dans les environnements à plusieurs serveurs Policy Server, les outils Distribution de la stratégie centrale et Distribution de la configuration centrale permettaient de synchroniser les différents serveurs Policy Server.

À présent, une **base de données de stratégies** stocke les informations de configuration des stratégies et des clients pour plusieurs serveurs Policy Server.

- La Base de données des stratégies est associée à TRITON - Web Security.
- Pour vous connecter à un serveur Policy Server connecté à la base de données des stratégies, servez-vous de TRITON - Web Security.
- Tous les serveurs Policy Server connectés à la base de données des stratégies partagent les informations relatives aux administrateurs, aux clients et aux stratégies, ajoutées ou modifiées dans un serveur Policy Server.

Les informations spécifiques à une seule instance de Policy Server, par exemple les informations de connexion de Filtering Service ou de Network Agent, sont stockées séparément par chaque serveur Policy Server.

Sauvegarde et restauration des informations des stratégies

L'utilitaire de sauvegarde de Websense simplifie la sauvegarde des données des stratégies et des paramètres Websense et permet de restaurer une configuration spécifique. Servez-vous de cet utilitaire pour :

- Sauvegarder immédiatement ou planifier des sauvegardes automatiques de Websense
- Restaurer votre configuration Websense
- Importer une configuration existante

L'utilitaire de sauvegarde enregistre et restaure :

- Les informations de la configuration globale, y compris les données des clients et des stratégies, stockées dans la base de données des stratégies
- Les informations de la configuration locale, telles que les paramètres de Filtering Service et de Log Server, stockées par Policy Server
- Les fichiers d'initialisation et de configuration des composants de Websense

L'utilitaire de sauvegarde de Websense est accessible à partir de la ligne de commande et doit être exécuté dans chaque ordinateur comprenant des composants Websense. Pour plus d'informations sur l'exploitation de cet outil, consultez l'Aide de TRITON - Web Security.

Connexions simultanées des administrateurs

Comme dans les versions précédentes, vous pouvez utiliser l'administration déléguée pour autoriser certains administrateurs à gérer les informations des stratégies ou à exécuter des rapports pour une liste définie de clients.

Dorénavant, plusieurs administrateurs peuvent se connecter simultanément au même serveur Policy Server pour gérer les stratégies ou générer des rapports.

- Un seul administrateur à la fois peut se connecter à chaque rôle avec des autorisations **de stratégie**.
- Plusieurs administrateurs peuvent se connecter simultanément au même rôle incluant des autorisations **génération de rapports** ou **auditor (vérificateur)** (*versions 7.6 et ultérieures*).

Si vous tentez de vous connecter à un rôle actuellement utilisé par un autre administrateur disposant d'autorisations de stratégie, vous avez la possibilité de vous connecter au rôle sélectionné avec :

- Des autorisations de génération de rapports uniquement
- Des autorisations de lecture seule (vérificateur temporaire) (*versions 7.6 et ultérieures*)
- Un accès à la surveillance de l'état (pages État > Tableau de bord et Alertes, plus Real-Time Monitor)

Vous pouvez aussi vous connecter à un autre rôle que vous êtes autorisé à gérer.

Identification des Super administrateurs conditionnels

Les jeux d'autorisations suivants peuvent être attribués aux administrateurs du rôle Super administrateur :

- Les Super administrateurs inconditionnels disposent d'un accès complet à tous les paramètres de configuration, de génération de rapports et de gestion des stratégies.

  Les Global Security Administrators (Administrateurs de la sécurité globale) (*versions 7.6 et ultérieures*) disposent automatiquement d'un accès Super Administrateur inconditionnel au module Web Security.
- Les Super administrateurs conditionnels disposent d'un accès plus limité aux paramètres de configuration.

  Comme les Administrateurs à distance des versions 6.x et antérieures, les Super administrateurs conditionnels peuvent exécuter la plupart des fonctions de gestion des stratégies, mais ne peuvent pas modifier le verrouillage du filtre ni configurer la plupart des pages Paramètres.

Création d'exceptions aux paramètres d'identification des utilisateurs

Outre les options d'identification transparente des utilisateurs et d'authentification manuelle disponibles dans les versions précédentes de Websense, il existe à présent une option d'**authentification sélective** qui permet de définir des options d'authentification spécifiques pour certaines adresses IP.

L'authentification sélective permet de déterminer si les utilisateurs qui demandent un accès à Internet à partir d'un ordinateur spécifique sont identifiés de façon transparente, sont invités à saisir leurs identifiants de connexion via le navigateur (authentification manuelle) ou ne sont jamais invités à s'authentifier. 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
- Assurer que les utilisateurs d'un ordinateur de salle d'examen situé dans un cabinet médical soient toujours identifiés avant d'accéder à Internet

Dans la page **Paramètres > Général > Identification utilisateur**, cliquez sur **Exceptions** pour définir les paramètres d'identification d'utilisateur spécifiques de certains ordinateurs du réseau.

Intégration à Websense Web Security Gateway

Websense Web Security Gateway élève le niveau de protection de Websense Web Security et vous permet désormais d'activer l'analyse avancée des fichiers en ligne et du contenu des sites Web demandés. Lorsqu'elle est activée, cette analyse ne concerne que les sites non bloqués par Websense Web Security.

- L'option **Catégorisation du contenu** vérifie le contenu des sites autorisés et renvoie la catégorie à utiliser pour le filtrage.
- L'option **Content security (Sécurité du contenu)** recherche des menaces pour la sécurité dans le contenu Web, par exemple des risques de phishing, de redirection d'URL, d'exploits Web et d'antiblocage par proxy.
- L'option **File analysis (Analyse des fichiers)** examine le contenu des fichiers pour détecter les menaces potentielles (par exemple la présence d'un virus, d'un cheval de Troie ou d'un ver).

3 Nouveautés de la Version 7.1

La version 7.1 introduit :

- De nouveaux messages d'alerte d'état dans le Tableau de bord de Web Security (voir *Alertes d'état étendues*, page 19)
- Une fonctionnalité **Save and Deploy (Enregistrer et déployer)** étendue (voir *Protection de la fonction Save and Deploy (Enregistrer et déployer)*, page 20)
- Un processus simplifié pour la création et la modification des rapports de présentation personnalisés (voir *Modification des rapports de présentation*, page 20)
- De nouveaux graphiques État > Tableau de bord pour Websense Security Gateway (voir *Nouveaux rapports de Websense Web Security Gateway*, page 21)
- De nouveaux rapports de présentation pour Websense Security Gateway (voir *Nouveaux rapports de Websense Web Security Gateway*, page 21)

Alertes d'état étendues

Pour simplifier la surveillance de l'état de votre déploiement Websense, de nouveaux messages d'alerte s'affichent dans le tableau de bord Système et dans la page État > Alertes lorsque :

- L'espace disque disponible dans un ordinateur Filtering Service devient insuffisant (avertissement) ou très insuffisant (erreur).

  Il est alors possible que la base de données principale ne puisse plus effectuer les téléchargements et les mises à jour.
- L'espace disque disponible dans un ordinateur TRITON - Web Security (auparavant Websense Manager) devient insuffisant (avertissement) ou très insuffisant (erreur).

  Des problèmes de génération des rapports de présentation ou de performances peuvent alors survenir dans cet ordinateur.
- L'espace disque disponible dans un ordinateur Log Server devient insuffisant (avertissement) ou très insuffisant (erreur).

  La journalisation peut alors devenir intermittente ou cesser entièrement.
- La mémoire disponible dans un ordinateur Filtering Service devient insuffisante.

  Il est alors possible que le service de filtrage ne puisse plus appliquer les mises à jour de la base de données principale.

- L’utilisation du processeur est trop élevée dans l’ordinateur Filtering Service.

  La navigation peut alors être ralentie ou le filtrage des utilisateurs peut ne pas s’effectuer correctement. Cela peut également signifier que d’autres instances de Filtering Service sont nécessaires.
- La mémoire disponible dans un ordinateur Network Agent devient insuffisante.

  Cela peut empêcher le démarrage de Network Agent ou entraîner un filtrage incorrect.
- L’utilisation du processeur est trop élevée dans l’ordinateur Network Agent.

  Il est alors possible que le filtrage et la journalisation ne soient pas effectués correctement.
- Le service Websense TRITON - Web Security (auparavant ApacheTomcatWebsense) ne parvient pas à se connecter à Log Server.

  Lorsque ce problème survient, les travaux des rapports de présentation planifiés ne sont pas correctement enregistrés et sont alors perdus au redémarrage du service Websense TRITON - Web Security. Par ailleurs, les rapports de la page État > Tableau de bord ou de la page Rapports de présentation peuvent ne contenir aucune données, même lorsque ces informations ont été stockées correctement dans la base de données d’activité.
- Un ou plusieurs rapports de présentation planifiés échouent.

  Pour identifier les travaux en échec, utilisez la page Rapports de présentation > Planificateur.

Protection de la fonction Save and Deploy (Enregistrer et déployer)

Pour garantir la mise en cache appropriée des modifications (ou leur abandon délibéré), une nouvelle fonction désactive les boutons **Save and Deploy (Enregistrer et déployer)** et **Afficher les modifications en attente** de certaines pages de gestion des stratégies jusqu’à ce que vous cliquiez sur **OK** ou sur **Annuler**.

Les boutons Save and Deploy (Enregistrer et déployer) et Afficher les modifications en attente sont désactivés, même si vous avez déjà mis des modifications en cache dans d’autres pages (sans les enregistrer).

Cette modification n’affecte pas les pages Paramètres ni les pages des autres parties de TRITON - Web Security (auparavant Websense Manager) qui ne proposent pas de bouton **OK** (par exemple, Génération de rapports > Rapports d’investigation ou Gestion des stratégies > Stratégies).

Modification des rapports de présentation

L’utilisation des rapports de présentation est désormais simplifiée. Pour que la distinction entre les rapports modifiables et intangibles sont plus claire, une icône « W » est désormais accolée aux rapports prédéfinis. Il est toujours possible de générer un rapport prédéfini en cliquant sur **Exécuter** et en sélectionnant les dates à inclure.

Vous pouvez à présent créer un rapport personnalisé en une seule étape. Cliquez simplement sur **Enregistrer sous** pour créer une copie d'un rapport prédéfini et donnez un nom à cette copie. Vous pouvez ensuite modifier immédiatement le filtre du rapport, en sélectionnant des clients, des catégories, des protocoles ou des actions spécifiques à inclure. Vous pouvez également revenir au Catalogue des rapports et personnaliser le filtre du rapport ultérieurement.

Les rapports personnalisés sont désignés par une icône stylisée « utilisateur ». Pour modifier le filtre du rapport, sélectionnez un rapport personnalisé, puis cliquez sur **Modifier**.

Nouveaux rapports de Websense Web Security Gateway

Les nouveaux rapports donnent davantage d'informations sur l'analyse du contenu par Websense Web Security Gateway.

Par défaut, les graphiques du Tableau de bord présentent les activités d'analyse de Content Gateway.

Quatre nouveaux rapports de présentation ont également été ajoutés. Ces rapports s'affichent uniquement dans le Catalogue de rapports du groupe Activité d'analyse lorsqu'une analyse a détecté des sites dont le contenu a été modifié depuis leur classification dans la base de données principale.

Titre	Description
Detail of Full URLs for Scanned Requests (Détails des URL complètes des requêtes analysées)	Identifiez avec précision les différentes pages analysées dans chaque domaine dont le contenu ne correspondait pas à la catégorie standard, lorsque les URL complètes sont journalisées. Exploitez ces informations pour mieux comprendre l'évolution de la nature du contenu Internet.
Summary of Scanned Requests by User (Résumé des requêtes analysées par utilisateur)	Identifiez chaque jour les URL analysées dont la catégorie a été modifiée, résumées par utilisateur, date et catégorie. Identifiez les utilisateurs qui accèdent le plus souvent aux sites dont le contenu change dynamiquement et voyez s'il est nécessaire de modifier vos stratégies.
Top Categories by Scanned Requests (Principales catégories par requêtes analysées)	Découvrez les catégories pour lesquelles les requêtes sont le plus souvent soumises à l'analyse. Évaluez les risques de sécurité ou de productivité qui pèsent sur votre entreprise du fait de l'accès Internet.
User Activity Detail for Scanned Requests (Détails de l'activité des utilisateurs pour les requêtes analysées)	Consultez les informations détaillées sur les utilisateurs ayant demandé des sites dont le contenu analysé ne correspondait pas à la catégorisation standard. Découvrez l'action entreprise par Websense suite à la nouvelle catégorie et la quantité de bande passante consommée.

4 Nouveautés de la Version 7.5

La version 7.5 offre de nombreuses nouvelles fonctions, ainsi qu'une étroite intégration aux autres solutions de sécurité de Websense. Cette section présente les principaux ajouts et changements :

- *Websense Web Security Gateway Anywhere*
  - *Sécurité Web hybride*
  - *Prévention des pertes de données via Internet*
- *Présentation de TRITON - Web Security*
- *Priorités de la sécurité*
- *Amélioration de la génération des rapports de présentation*
- *Amélioration du résumé de l'historique*
- *Nouveaux paramètres de Websense Web Security Gateway*
- *Nouveaux rapports de Websense Web Security Gateway*

La description complète de toutes les nouvelles fonctionnalités est disponible dans les notes de publication de la version 7.5.

Websense Web Security Gateway Anywhere

Websense Web Security Gateway Anywhere est une solution de sécurité complète et flexible qui combine des capacités de filtrage Web et de prévention de perte de données (DLP).

Grâce à un abonnement Web Security Gateway Anywhere, votre organisation peut combiner diverses solutions de filtrage Web en fonction de ses besoins en matière de gestion et d'infrastructure :

- Utilisez une seule console, TRITON Unified Security Center, pour exécuter les tâches de gestion des stratégies et de génération de rapports pour tous les utilisateurs, quel que soit leur mode de filtrage.
- Exploitez la puissante solution de sécurité Web déjà installée et configurée dans votre réseau.
- Tirez parti du filtrage hybride de Websense pour réduire les ajouts nécessaires de matériel complémentaire ou les investissements en infrastructure, par exemple dans les bureaux satellites qui n'ont pas toujours de personnel informatique dédié.
- Utilisez le logiciel de filtrage à distance, le filtrage hybride ou les deux solutions pour gérer l'accès Internet de vos utilisateurs lorsqu'ils sont en déplacement.

Cette solution comprend également la totalité des capacités de Content Gateway, notamment la capacité d'analyse des sites et des fichiers permettant de détecter le contenu dangereux et des analyses antivirales héritées en temps réel, à mesure que les utilisateurs demandent des sites.

Web Security Gateway Anywhere comprend en outre des capacités de prévention des pertes de données qui vous permettent de réguler les différents types de contenu pouvant être publiés sur le Web depuis votre organisation.

Sécurité Web hybride

Web Security Gateway Anywhere est une alternative aux pures solutions de sécurité Web de type service, logiciel ou dispositif. Au lieu de choisir une solution cloud ou sur site pour votre entreprise, vous pouvez déployer une solution hybride qui tire parti des avantages de ces deux univers, et gérer cette solution à partir d'une seule interface utilisateur : TRITON - Web Security.

Une même organisation peut exploiter une solide solution de sécurité Web sur site pour son siège social ou son campus central, et le service hybride pour ses filiales ou ses campus régionaux (sans qu'une licence supplémentaire ne soit nécessaire). Il est ainsi possible de réduire les ajouts de matériel complémentaire et les investissements en infrastructure, par exemple dans les bureaux satellites qui n'ont pas toujours de personnel informatique dédié.

Bien que vous puissiez toujours installer le logiciel de filtrage à distance pour protéger les utilisateurs hors site, vous avez désormais la possibilité d'exploiter également le service hybride.

La sécurité hybride introduit deux nouveaux services, déployés en même temps que le logiciel Websense :

- **Websense Sync Service** transmet les données des stratégies et des utilisateurs au service hybride et récupère les données des rapports auprès de ce dernier.
- **Websense Directory Agent** récupère les données de vos utilisateurs et de vos groupes dans le service d'annuaire de votre organisation en vue de leur exploitation par le service hybride.

Servez-vous des pages **Paramètres > Hybrid Configuration (Configuration hybride)** pour configurer le filtrage hybride, puis des fonctionnalités de gestion des stratégies et de génération de rapports existantes pour imposer des stratégies à tous vos clients et examiner leur activité Internet, quel que soit leur mode de filtrage.

Deux nouveaux graphiques du Tableau de bord Web Security présentent l'activité Internet des membres de votre organisation, filtrés par le service hybride.

Nom du graphique	Description
Hybrid Requests Processed (Requêtes traitées par le service hybride)	Présente le nombre de requêtes effectuées par les utilisateurs de votre organisation que le service hybride a autorisées ou bloquées
Hybrid Bandwidth Usage (Utilisation de la bande passante - Service hybride)	Présente la bande passante consommée par les requêtes Internet des utilisateurs de votre organisation filtrés par le service hybride

Pour obtenir des informations détaillées sur les clients filtrés par le service hybride, vous pouvez générer des rapports d'investigation par Serveur source ou Adresse IP source. (Les rapports de présentation présentent les données combinées pour tous les clients, sans faire de distinction entre les clients filtrés par le service hybride et les parties sur site de votre logiciel Websense.)

Prévention des pertes de données via Internet

Websense Web Security Gateway Anywhere vous protège contre les pertes de données sur Internet et, combiné au filtrage Web, sécurise à la fois votre contenu entrant et sortant.

Après avoir installé Websense Content Gateway, servez-vous du programme d'installation de TRITON Unified pour installer Websense Web Security et Websense Data Security, puis de TRITON - Data Security pour définir les stratégies de sécurité des données et examiner les incidents et les rapports.

Les stratégies de sécurité des données contiennent des règles, des exceptions, des conditions et des ressources. Les règles et les exceptions définissent la logique de la stratégie. Les conditions définissent les circonstances à surveiller (par exemple, un numéro de 16 chiffres avec une date sur 4 chiffres pour les paiements par carte bancaire). Les ressources définissent les sources et les destinations des données de votre réseau, ainsi que l'action à exécuter lorsqu'une faille est détectée.

Vous pouvez utiliser des stratégies réglementaires prédéfinies ou créer des stratégies personnalisées pour votre organisation. Dans votre stratégie, vous devez indiquer si vous souhaitez surveiller ou bloquer les tentatives de transfert de données sensibles via les circuits Web (HTTP, HTTPS ou FTP sur HTTP).

Pour identifier vos données sensibles, vous pouvez exploiter la technologie PreciseID™ brevetée de Websense pour prendre leurs « empreintes ». (Vous pouvez également identifier des phrases clés, des modèles d'expression régulière, des dictionnaires et des propriétés de fichier.)

Vous pouvez relier vos logiciels Web et de sécurité des données pour permettre à Websense Data Security d'accéder aux informations de catégories de la Base de données principale et les informations relatives aux utilisateurs de Websense User Service.

Présentation de TRITON - Web Security

Les solutions Websense de sécurité Web, de données et de messagerie interagissant de plus en plus étroitement, TRITON Unified Security Center offre une approche centralisée de la gestion des logiciels Websense.

Lorsque vous vous connectez à un module TRITON, une barre de boutons indique le module actif (surligné en jaune) et les autres modules TRITON existants.

- Les noms des modules déjà configurés dans votre environnement et actuellement disponibles s'affichent en bleu.
- Les noms des modules qui n'ont pas encore été configurés ou qui ne sont pas disponibles s'affichent en gris.

Le menu Aide, qui propose désormais des liens vers la Base de connaissances Websense et les forums des clients, est placé dans la barre d'outils TRITON (juste au-dessous de la bannière Websense ; modification introduite avec la version 7.6). Les fonctions Select Policy Server (Sélectionner une instance de Policy Server) et Save and Deploy (Enregistrer et déployer) sont désormais situées dans la barre d'outils de Web Security (sous la barre d'outils TRITON). (Une présentation visuelle de la nouvelle disposition est disponible à la section *Console TRITON™ Unified Security Center*, page 7,.)

Les fonctionnalités TRITON - Web Security qui autorisent la réduction et le développement des panneaux de navigation gauche et droit permettent aux administrateurs d'agrandir le panneau de contenu en fonction de leurs besoins. Lorsque le panneau de navigation gauche est réduit, l'une des barres d'icônes suivantes s'affiche.

Chaque icône représente un regroupement fonctionnel : État, Génération de rapports et Gestion des stratégies dans l'onglet Principal ; Général, Alertes, Network Agent et Génération de rapports dans l'onglet Paramètres. (Des groupes de paramètres supplémentaires s'affichent dans un déploiement Websense Web Security Gateway Anywhere.) Pour accéder aux fonctionnalités d'un groupe sans développer le panneau de navigation, survolez une icône avec votre souris.

Priorités de la sécurité

Dans les versions précédentes, les définitions d'URL personnalisées et les filtres d'accès illimité (appelés auparavant listes d'acceptation) étaient prioritaires sur la catégorisation de la Base de données principale. Ainsi, lorsqu'un site était défini en tant qu'URL non filtrée ou reclassée dans une catégorie autorisée, ou lorsqu'un site apparaissait dans un filtre d'accès illimité, ce site était autorisé, y compris lorsqu'il avait également été affecté à une catégorie de la classe Risques de sécurité (telles que les catégories Sites Web dangereux, Logiciels espions et Phishing et autres escroqueries).

La version 7.5 a introduit la possibilité de configurer Websense de sorte que la catégorisation de sécurité soit prioritaire par rapport à la catégorisation personnalisée. Après modification de la configuration, lorsque la base de données principale ou une analyse Websense Web Security Gateway plaçait un site dans une catégorie de la classe Risques de sécurité et que cette catégorie était bloquée, ce site l'était également.

Dans la version 7.6, ce comportement a été modifié de sorte que Filtering Server et le service hybride donnent par défaut la priorité à la catégorisation de la classe Risques de sécurité. Voir *Filtrage basé sur l'état de la catégorie Risques de sécurité*, page 36.

Amélioration de la génération des rapports de présentation

Une nouvelle fonction des rapports de présentation améliore les performances des rapports générés à la volée, tout en simplifiant l'accès aux rapports très volumineux et leur planification.

Lorsque vous exécutez un rapport à la volée, vous disposez de deux options :

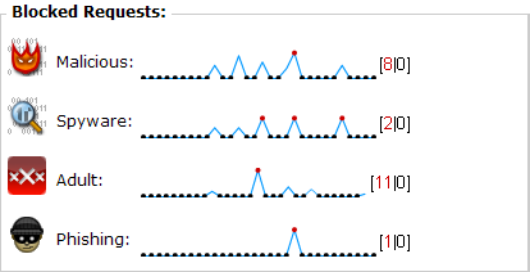
- Exécutez le rapport en arrière plan pour en planifier une seule exécution et l'exécuter immédiatement.
- Exécutez le rapport au premier plan pour le générer dans une nouvelle fenêtre sans le planifier.

Dans les deux cas, le rapport s'exécute immédiatement. Lorsque vous optez pour la planification du rapport, vous pouvez également choisir de recevoir une notification électronique dès que le rapport est prêt. Vous pouvez également consulter la file d'attente des travaux afin de vérifier l'état de votre rapport. Le rapport s'exécute en arrière-plan et apparaît dans la liste Review Reports (Examiner les rapports) lorsqu'il est terminé. Vous pouvez donc accéder à ce rapport et le gérer dans TRITON - Web Security.

Si vous préférez ne pas planifier votre rapport, il est généré dans une fenêtre distincte, ce qui vous permet de continuer à travailler dans TRITON - Web Security pendant que le rapport s'exécute. Lorsque le rapport est terminé, vous pouvez l'afficher et l'enregistrer. Le rapport n'est toutefois pas enregistré automatiquement et ne s'affiche pas dans la liste Review Reports (Examiner les rapports).

Amélioration du résumé de l'historique

La section **30-Day Risk Trends (Tendance des risques sur 30 jours)** du tableau de bord Risques a été modifiée de manière à détailler davantage les requêtes bloquées dans les catégories visées au cours des 30 derniers jours. Pour chaque catégorie, un graphique de tendances met en évidence le pic du nombre de requêtes bloquées, tout en présentant la tendance générale des requêtes de ces catégories.



Cliquez sur le numéro du pic accolé à une courbe pour ouvrir le tableau de bord Menaces ou un rapport d'investigation (selon la catégorie) présentant davantage d'informations sur les requêtes de la catégorie sélectionnée.

Notez que les 4 graphiques peuvent chacun utiliser une échelle distincte. Lorsqu'une catégorie présente un pic de 500 requêtes et un autre de 10 requêtes seulement, les graphiques peuvent sembler similaires alors que l'échelle est très différente. Pour mieux évaluer cette échelle, servez-vous des nombres situés à droite de chaque graphique.

Nouveaux paramètres de Websense Web Security Gateway

Les administrateurs de Web Security Gateway et de Web Security Gateway Anywhere ont désormais accès à la fonctionnalité améliorée suivante, configurée dans la page Paramètres > Analyse > Options d'analyse de TRITON - Web Security.

- La fonction **Embedded URL link analysis (Analyse des liens intégrés aux URL)** peut éventuellement être exécutée pendant la catégorisation du contenu de sorte que celle-ci soit plus précise pour certains types de pages. Par exemple, une page qui ne contient que peu, voire aucun contenu indésirable, mais qui comprend des liens vers des sites connus pour être indésirables peut elle-même être catégorisée de façon plus précise. L'analyse des liens des URL peut détecter les liens malveillants intégrés dans les parties masquées d'une page, de même que les pages renvoyées par les serveurs d'images qui relient des miniatures à des sites indésirables.
- Le **contrôle de la sensibilité de la catégorisation du contenu** vous permet d'ajuster la sensibilité des méthodes (classificateurs) utilisées pour classer le contenu et identifier une catégorie. Il est important de comprendre que cette catégorisation est le résultat d'une analyse de contenu impliquant plusieurs méthodes (classificateurs). Par rapport à la catégorie résultante, l'impact de la modification du niveau de sensibilité n'est pas prévisible. Le niveau de sensibilité est optimisé (réglé) par les laboratoires Websense Security Labs à l'aide d'un vaste lot de tests d'URL afin de garantir des résultats précis pour ce lot de tests.
- La fonction **Tunneled protocol detection (Détection des protocoles en tunnel)** analyse le trafic lorsqu'il transite par Content Gateway afin de détecter les protocoles mis en tunnel sur HTTP et HTTPS. Ce type de trafic est signalé à Filtering Service de sorte que le filtrage des protocoles soit imposé. L'analyse porte à la fois sur le trafic entrant et sortant. Cette fonction permet de bloquer les protocoles utilisés pour la messagerie instantanée, les applications peer-to-peer et le contournement du proxy.
- Les options de sécurité permettent à présent d'analyser, de détecter et de bloquer les **applications Internet multimédia**, par exemple les applications Flash, qui contiennent du code dangereux.
- Une nouvelle option d'analyse du contenu comportant un risque pour la sécurité prend en charge l' **analyse du contenu Web sortant associé au trafic « zombie » ou « d'appel automatique »**. Lorsqu'un tel trafic est détecté, il est transmis à la base de données des journaux d'analyse et catégorisé, de sorte que vous pouvez ensuite exécuter un rapport pour obtenir la liste des ordinateurs de votre système infectés par des robots et des logiciels espion.

Contournement du décryptage SSL (Content Gateway)

Pour aider les organisations qui utilisent SSL Manager dans Content Gateway à gérer le trafic crypté, et qui ne souhaitent pas décrypter les sessions HTTPS que les utilisateurs ouvrent sur des sites sensibles (par exemple les sites des banques ou des prestataires de soins médicaux), les administrateurs peuvent désormais définir les catégories de sites devant ignorer le décryptage SSL dans la page Paramètres > Analyse > SSL Decryption Bypass (Contournement du décryptage SSL) de TRITON - Web Security.

Pour plus de commodité, un groupe Privacy Category (Catégories confidentielles) prédéfini regroupe les catégories auxquelles des conditions réglementaires peuvent s'appliquer, par exemple l'enseignement, les services financiers, les organismes médicaux, etc. Les administrateurs peuvent également spécifier la liste des noms d'hôtes ou des adresses IP pour lesquels le décryptage SSL ne doit pas être effectué.

Nouveaux rapports de Websense Web Security Gateway

Les nouveaux graphiques et rapports de présentation de la page État > Tableau de bord donnent des informations sur les sites Web 2.0 demandés par les utilisateurs de votre organisation et analysés par Websense Web Security Gateway.

Le tableau de bord Usage comprend 2 nouveaux graphiques :

Nom du graphique	Description
Catégories Web 2.0	Affiche les catégories Web 2.0 les plus demandées. Servez-vous de ces informations pour connaître les modèles d'utilisation d'Internet et détecter les éventuels problèmes de productivité.
Web 2.0 Bandwidth (Bande passante Web 2.0)	Présente les sites Web 2.0 qui consomment le plus de bande passante. Servez-vous de ces informations pour identifier les changements de stratégie éventuellement nécessaires en matière de gestion de la bande passante.

Dans la page Rapports de présentation, les six nouveaux modèles de rapport ajoutés dans le Catalogue des rapports mettent en évidence les activités d'analyse au sein de votre réseau.

Nom du rapport	Description
Top Web 2.0 Categories Visited by Requests (Principales catégories Web 2.0 consultées)	Présente les catégories les plus souvent affectées aux sites Web 2.0 analysés
Top Web 2.0 Sites by Bandwidth (Principaux sites Web 2.0 par bande passante)	Présente les sites Web 2.0 qui consomment le plus de bande passante
Top Web 2.0 Users by Browse Time (Principaux utilisateurs Web 2.0 par temps de navigation)	Présente les utilisateurs qui passent le plus de temps à consulter des sites Web 2.0
Web 2.0 User Activity Summary (Résumé de l'activité des utilisateurs Web 2.0)	Indique qui a consulté tel ou tel site Web 2.0 et quand
Top Sites Blocked by Link Analysis (Principaux sites bloqués par l'analyse des liens)	Présente les sites bloqués par l'analyse des liens
Link Analysis: Detail of Full URLs (Analyse des liens : Détails des URL complètes)	Présente l'URL complète des pages bloquées par l'analyse des liens, lorsque les URL complètes sont enregistrées dans le journal

5 Nouveautés de la Version 7.6

La version 7.6 introduit les fonctionnalités suivantes, nouvelles ou étendues :

- *Amélioration de TRITON Unified Security Center*
- *Présentation de Real-Time Monitor*
- *Nouvelles plateformes pour la base de données d'activité*
- *Administration déléguée et génération de rapports*
- *Nouvelles alertes de fonctionnement de DC Agent*
- *Pages de blocage*
- *Filtrage basé sur l'état de la catégorie Risques de sécurité*
- *Surveillance de l'état de Web Security*
- *Prise en charge du Client Remote Filtering 64 bits*
- *Gestion des clés de Policy Server*
- *Mise en cache de User Service*
- *Filtrage IPv6*
- *Modification des alertes d'utilisation*
- *Prise en charge des noms de domaine internationaux (IDN)*
- *Accès à Content Gateway et alertes*

Amélioration de TRITON Unified Security Center

Jusqu'à présent, les consoles de gestion de Websense Web Security et Data Security étaient étroitement intégrées pour former une interface utilisateur initiale partagée : TRITON Unified Security Center.

Cette version introduit la prochaine génération de TRITON Unified Security Center, qui permet de générer des rapports et d'administrer de manière centralisée la sécurité Web, la sécurité des données et la sécurité de la messagerie, mais permet également :

- D'accéder à tous les dispositifs V-Series de votre réseau via un même point d'accès. Dans la barre d'outils TRITON (juste sous la bannière), cliquez sur Appliances (Dispositifs) pour afficher des informations sur tous les dispositifs enregistrés.
- De créer de manière centralisée des comptes d'administrateur pour tous les modules. Créez des administrateurs dans la page Paramètres > Administrateurs de TRITON, puis accordez-leur l'accès à un ou plusieurs modules TRITON.

- De gérer la récupération des mots de passe des administrateurs dans tous les modules. Pour activer cette fonctionnalité, configurez les paramètres SNMP dans la page Paramètres > Notifications de TRITON.

Tous les composants de gestion peuvent désormais être installés dans un seul ordinateur Windows Server 2008 R2, une même interface utilisateur permettant d'y accéder. L'intégration des différents modules ayant lieu pendant l'installation, il n'est plus nécessaire de relier manuellement les consoles de gestion.

Lorsque Websense Web Security est installé de façon autonome, sans les autres modules Websense TRITON Enterprise, TRITON - Web Security peut s'exécuter dans un dispositif Websense. Cette configuration est uniquement recommandée à des fins d'évaluation.

Pour prendre en charge les modifications apportées à TRITON, les services Web Security suivants ont été renommés comme suit :

- Apache2Websense devient désormais **Websense Web Reporting Tools**.
- ApacheTomcatWebsense devient désormais **Websense TRITON - Web Security**.

Présentation de Real-Time Monitor

Le nouvel outil de génération de rapports, Real-Time Monitor, fournit des informations détaillées sur le filtrage de l'activité Internet en cours dans votre réseau. Vous pouvez filtrer les résultats pour cibler un sous-ensemble spécifique du trafic ou interrompre la surveillance pour examiner les données existantes en profondeur.

Les informations affichées sont les suivantes :

- L'origine de chaque requête (nom d'utilisateur ou adresse IP)
- Tout ou partie de l'URL demandée (configurable)
- Si l'URL a été recatégorisée ou non par une analyse Content Gateway (Websense Web Security Gateway et Gateway Anywhere)

  Cette information est indiquée par la présence d'une icône. Survolez cette icône avec votre souris pour identifier la catégorie d'origine du site.
- La catégorie de sites utilisée pour le filtrage
- L'action (autorisée ou bloquée) appliquée à la requête
- L'heure à laquelle Real-Time Monitor a reçu l'enregistrement

  Du fait des différences de mode de réception des données du filtrage par Real-Time Monitor et la Base de données d'activité, l'heure indiquée peut différer légèrement de celle qui s'affiche dans les autres outils de génération de rapports, par exemple dans les rapports d'investigation.

Real-Time Monitor récupère les données en temps réel auprès de Usage Monitor, composant généralement installé avec Policy Server, et non pas auprès de Log Server. Par conséquent, Real-Time Monitor :

- Doit être connecté à une instance de Policy Server exécutant le service Usage Monitor
- Peut être utilisé dans les environnements qui n'exploitent pas d'autres outils de génération de rapports

Une instance de Real-Time Monitor affiche les données d'un seul serveur Policy Server à la fois. Pour surveiller le trafic lié à plusieurs instances de Policy Server, vous pouvez ouvrir plusieurs fenêtres Real-Time Monitor simultanément. (Dans ce cas, chaque instance de Policy Server doit disposer de sa propre instance d'Usage Monitor.)

Real-Time Monitor est généralement installé avec TRITON Unified Security Center et comprend 3 services : le Client Websense RTM (Real-Time Monitor), le Serveur Websense RTM et la Base de données Websense RTM.

Des informations détaillées sur la configuration et l'utilisation de Real-Time Monitor sont disponibles dans l'Aide de TRITON - Web Security.

Nouvelles plateformes pour la base de données d'activité

La version 7.6 prend désormais en charge Microsoft SQL Server Express 2008 R2.

La prise en charge de MSDE (Microsoft SQL Server 2000 Desktop Engine) a été abandonnée.

Suite à cette modification, la page Paramètres > Génération de rapports > Base de données d'activité a été modifiée de manière à refléter les différences des méthodes de remplacement et des tailles de partition prises en charge.

Administration déléguée et génération de rapports

L'intégration complète de TRITON Unified Security Center a entraîné quelques modifications en matière de création et de gestion des comptes d'administrateur. Par ailleurs, TRITON - Web Security inclut désormais un nouveau type de rôle et plusieurs nouvelles autorisations réservées aux administrateurs.

Important

Le compte Administrateur Websense n'est plus le compte d'administrateur par défaut.

Le compte par défaut (disposant d'autorisations complètes sur tous les modules de TRITON Unified Security Center) est désormais le compte **admin**.

Gestion des administrateurs

La gestion des comptes d'administrateur (locaux et réseau) s'effectue désormais via la page Paramètres > Administrateurs dans TRITON. Les administrateurs de la sécurité globale qui disposent d'un accès complet aux paramètres TRITON et à tous les modules de TRITON Unified Security Center (Web Security, Data Security et Email Security) peuvent créer des comptes d'administrateur et leur accorder des autorisations d'accès à un ou plusieurs modules TRITON.

Les rôles d'administration déléguée et les autorisations propres aux différents rôles sont toujours attribués aux administrateurs dans TRITON - Web Security.

Réinitialisation du mot de passe

La version 7.6 introduit un nouveau mécanisme de réinitialisation du mot de passe des comptes d'administrateur local (appelés auparavant « comptes d'utilisateur Websense »). Cela implique que tous les comptes d'administrateur locaux soient associés à une adresse de messagerie.

Lorsqu'un administrateur demande un nouveau mot de passe, un mot de passe temporaire à usage unique est envoyé par e-mail à l'adresse associée à son compte. Ce mot de passe est valable pendant une période limitée. Lorsque l'administrateur saisit ce mot de passe temporaire, il est invité à en créer un nouveau.

La configuration de SNMP permettant d'activer le système de récupération des mots de passe basé sur la messagerie s'effectue dans les Paramètres de TRITON.

Nouveau type de rôle et nouvelles autorisations

Les options d'administration déléguée disponibles dans TRITON - Web Security ont été améliorées :

- Il existe désormais 2 types de rôles d'administration déléguée : gestion des stratégies et génération de rapports, et génération de rapports d'investigation.
  - Les administrateurs associés aux rôles **gestion des stratégies et génération de rapports** peuvent toujours être autorisés à créer des stratégies pour les clients gérés, à générer des rapports sur tous les clients ou sur les clients gérés uniquement ou à créer des stratégies et à exécuter des rapports. Les stratégies de clients gérés attribuées à ce type de rôle sont gérées par les administrateurs de ce rôle.
  - Les administrateurs associés aux rôles **génération de rapports d'investigation** peuvent générer des rapports sur les clients gérés par le rôle, mais les stratégies de ces clients sont gérées par d'autres rôles.

    Un même client peut être ajouté à plusieurs rôles de génération de rapports d'investigation, mais uniquement à un seul rôle de gestion des stratégies et génération de rapports.
- Quel que soit le rôle (y compris Super administrateur), des autorisations **Auditor (Vérificateur)** peuvent désormais être attribuées aux administrateurs. Ces autorisations leur permettent d'accéder en lecture seule aux fonctionnalités et fonctions à la disposition des autres administrateurs du rôle. Ces vérificateurs peuvent donc examiner TRITON - Web Security et les capacités de gestion à la disposition des autres administrateurs, mais pas enregistrer de modifications.
- Les administrateurs du rôle Super administrateur et des rôles de gestion des stratégies et de génération de rapports disposent d'une nouvelle autorisation de génération de rapports : **Real-Time Monitor**. Cette autorisation permet aux administrateurs de surveiller toute l'activité de filtrage liée à une instance de Policy Server. Notez que les autorisations Real-Time Monitor ne peuvent pas être limitées à l'affichage des informations des clients gérés uniquement.

Options de distribution des stratégies lors de la création du rôle

Lors de la création d'un nouveau rôle d'administration déléguée (gestion des stratégies et génération de rapports), deux options permettent désormais aux Super administrateurs de définir les stratégies initialement associées au nouveau rôle :

- Attribuer au nouveau rôle une unique stratégie Par défaut, composée de la catégorie Par défaut du Super administrateur et des filtres de protocole (comportement de la version 7.x précédente)
- Attribuer au nouveau rôle un instantané de tous les filtres et toutes les stratégies (à l'exception de Autoriser tout) déjà présents dans le rôle Super administrateur

Les filtres copiés dans un rôle d'administration déléguée sont toujours soumis au Verrouillage du filtre.

Nouvelles alertes de fonctionnement de DC Agent

Deux nouvelles alertes de fonctionnement signalent aux administrateurs les problèmes de configuration courants de DC Agent :

- Une instance de DC Agent ne dispose pas des autorisations suffisantes.

  Cette alerte s'affiche lorsque DC Agent s'exécute sans les autorisations **administrateur de domaine** ou **administrateur d'entreprise** dont il a besoin pour communiquer avec les contrôleurs de domaine et les serveurs d'annuaire.
- Une instance de DC Agent ne parvient pas à accéder à un fichier requis.

  Cette alerte s'affiche lorsque DC Agent ne peut pas ouvrir, créer ou écrire dans le fichier **dc_config.txt** qui stocke les informations relatives aux contrôleurs de domaine.

Pages de blocage

Deux nouvelles fonctionnalités viennent renforcer l'intérêt des pages de blocage :

- Du texte de pointage a été ajouté dans l'icône et le message de blocage afin de mieux informer les utilisateurs lorsqu'une page de blocage partiel s'affiche dans une section de page autrement autorisée.
- Une fonction de remplacement de compte permet aux utilisateurs, lorsqu'elle est activée, de saisir de nouveaux identifiants de connexion dans la page de blocage afin de modifier la stratégie de filtrage appliquée à une requête.

Affichage des pages de blocage dans des petites sections d'écran

Lorsqu'une partie du contenu d'une page autrement autorisée est bloquée, les utilisateurs peuvent ne voir qu'un petit bout de la page de blocage. Dans ce cas, le problème ou la raison pour laquelle cette section de contenu est bloquée peut ne pas être très clair.

Désormais, lorsque l'utilisateur survole la partie visible de la page de blocage avec sa souris, un message lui explique que le contenu est bloqué et qu'il peut cliquer sur le message pour afficher la page de blocage complète et obtenir davantage d'informations sur la raison du blocage.

Lorsque l'utilisateur clique sur le message, la page de blocage complète s'affiche dans une nouvelle fenêtre.

Remplacement de compte

Lorsque des autorisations de remplacement de compte sont attribuées à un client et qu'un site demandé par ce client est bloqué, la page de blocage propose un bouton **Switch Credentials (Changer d'identifiants de connexion)**. L'utilisateur peut alors saisir d'autres identifiants de connexion réseau (nom d'utilisateur et mot de passe) de sorte que la requête soit filtrée par une autre stratégie.

- Si la nouvelle stratégie autorise cette requête, le site s'affiche.
- Si la nouvelle stratégie bloque cette requête, l'utilisateur n'a pas accès au site. Selon les autorisations affectées au compte filtré, l'utilisateur peut ou non avoir la possibilité de saisir d'autres identifiants de connexion.

Les nouveaux identifiants de connexion continuent de s'appliquer aux requêtes pendant la période configurée dans la page Paramètres > Général > Filtrage (5 minutes, par défaut).

Des autorisations de remplacement de compte peuvent par exemple être accordées à un ordinateur (adresse IP) lorsque celui-ci correspond à une borne destinée aux utilisateurs internes et aux invités qui ne sont pas invités à s'authentifier. Par défaut, la stratégie basée sur l'adresse IP s'applique généralement à l'ensemble des requêtes, mais les utilisateurs qui disposent d'identifiants de connexion réseau valides peuvent saisir ces informations lorsqu'une requête est bloquée afin de voir si leur stratégie de filtrage habituelle leur permet d'y accéder.

Filtrage basé sur l'état de la catégorie Risques de sécurité

Lorsque Filtering Service ou le service hybride détermine qu'un site appartient à une catégorie de risques pour la sécurité, le site est à présent filtré en fonction de l'état de la catégorie Risques de sécurité, y compris lorsqu'il s'agit :

- D'une URL recatégorisée
- D'une URL non filtrée
- D'un site inclus dans un filtre d'accès limité

La possibilité de déterminer si le filtrage d'un site de la classe Risques de sécurité dépend de l'état de la catégorie en question ou d'une catégorisation personnalisée a été introduite dans la version 7.5. À ce moment-là, le comportement par défaut donnait la priorité à la catégorisation personnalisée.

Si vous souhaitez que le filtrage dépende systématiquement de la catégorisation personnalisée, que le site apparaisse ou non dans la catégorie Risques de sécurité (par exemple Sites Web dangereux ou Logiciels espions), vous pouvez modifier le paramètre **SecurityCategoryOverride** des fichiers **eimserver.ini** et **syncservice.ini** pour désactiver le comportement par défaut. Pour plus d'informations, consultez la rubrique « Définition de la priorité de la catégorisation Risques de sécurité » dans l'Aide de TRITON - Web Security.

Surveillance de l’état de Web Security

Comme dans les versions précédentes, vous avez la possibilité de consulter les pages Tableau de bord et Alertes de TRITON - Web Security sans délai d’attente. Désormais, l’invocation de cette option permet également d’accéder à Real-Time Monitor.

Le mécanisme qui permet d’activer cette option a été modifié. Au lieu de cocher une case de la page Tableau de bord, cliquez sur le bouton **Status Monitor (Moniteur d’état)** de la barre d’outils située en haut du Tableau de bord, ou sélectionnez **Status Monitor Mode (Mode Moniteur d’état)** dans le champ déroulant Rôle de la barre d’outils Web Security.

Lorsque vous passez en mode Status Monitor (Moniteur d’état) dans TRITON - Web Security, vous êtes déconnecté de tous les autres modules TRITON auxquels vous avez pu accéder.

Prise en charge du Client Remote Filtering 64 bits

Le Client Remote Filtering est désormais pris en charge dans les systèmes d’exploitation 64 bits suivants :

- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2003 SP2 et versions ultérieures et R2 SP2 et versions ultérieures
- Windows Server 2008 SP1 et versions ultérieures et Windows Server 2008 R2

De plus, les modifications apportées à l’utilitaire de configuration du client Remote Filtering (qui fait partie du Générateur de package TRITON Unified Endpoint) simplifient désormais la création et la modification des profils de déploiement du client Remote Filtering. Définissez les instances de Serveur Remote Filtering utilisées par chaque ensemble de clients, puis le mode d’installation et le niveau de protection adéquat de ces clients.

Gestion des clés de Policy Server

La page Paramètres > Général > Policy Servers (Serveurs Policy Server) a été modifiée de manière à présenter des informations sur les clés de tous les serveurs Policy Server associés à une instance de TRITON - Web Security.

Comme avant, cette page vous permet d’ajouter ou de supprimer des connexions Policy Server. À présent, vous pouvez également établir des relations entre les différentes instances de Policy Server qui partagent une même clé. Lorsque vous désignez une instance en tant qu’instance principale de Policy Server, puis que vous associez d’autres instances en tant qu’instances secondaires, la hiérarchie définie se reflète dans cette page. Lorsque la clé de l’instance principale change, toutes les instances secondaires sont automatiquement mises à jour.

Vous pouvez également utiliser plusieurs instances principales de Policy Server disposant chacune de leur propre clé.

Lorsque vous ajoutez une nouvelle instance principale de Policy Server, servez-vous du bouton **Verify Connection (Vérifier la connexion)** pour vérifier que TRITON - Web Security peut communiquer avec la nouvelle instance. Si la connexion est établie, le message de confirmation indique si l'instance de Policy Server sélectionnée est déjà associée à une clé ou non. Dans l'affirmative, la clé en question s'affiche.

L'instance de Policy Server de base (instance de Policy Server à laquelle TRITON - Web Security se connecte pendant l'installation) doit toujours être une instance principale. Il est toujours possible d'afficher et de modifier la clé de cette instance dans la page Paramètres > Général > Compte.

Mise en cache de User Service

Comme dans les versions précédentes, User Service met les correspondances d'utilisateurs et de groupes en cache pendant une période de 3 heures (par défaut). Auparavant toutefois, le cache User Service était systématiquement effacé dès qu'un administrateur cliquait sur Enregistrer tout (à présent Save and Deploy (Enregistrer et déployer)) pour implémenter des modifications dans TRITON - Web Security et ce, quelles qu'étaient les modifications apportées à User Service.

Pour de meilleures performances, le cache User Service n'est désormais plus effacé à chaque action d'enregistrement, mais uniquement lorsqu'une modification a été apportée dans la page Paramètres > Général > Services d'annuaire.

Par ailleurs, la page Services d'annuaire comprend désormais un bouton **Clear Cache (Effacer le cache)** qui permet aux administrateurs de demander au besoin à User Service d'effacer le contenu de ses caches locaux et de récupérer les informations mises à jour dans le service d'annuaire.

Filtrage IPv6

Depuis la version 7.6, il était possible de laisser Network Agent autoriser ou bloquer l'ensemble du trafic IPv6.

Dans la version 7.7, cette fonctionnalité s'étend au filtrage complet des URL et des clients IPv6. Voir *Filtrage des URL et des clients IPv6*, page 53.

Modification des alertes d'utilisation

Les pages Paramètres > Alertes > Category Usage (Utilisation des catégories) et Protocol Usage (Utilisation des protocoles) ont été mises à jour de manière à simplifier la configuration simultanée de plusieurs alertes d'utilisation.

Ce fonctionnement simplifie désormais le processus de création et de mise à jour des paramètres d'alerte d'utilisation des catégories ou protocoles associés aux mêmes seuils d'alerte et méthodes de notification d'alerte, et fait gagner du temps aux administrateurs.

Prise en charge des noms de domaine internationaux (IDN)

TRITON - Web Security prend désormais en charge les noms de domaine internationaux (Unicode) dans les contextes suivants :

- Rapports d'investigation et de présentation
- Graphiques des tableaux de bord
- Alertes de catégorie dans Usage Monitor
- URL personnalisées
- Filtres d'accès limité

Dans les parties de la console qui ne prennent pas en charge les caractères Unicode, des messages d'erreur s'affichent pour indiquer que l'utilisation de Punycode est requise.

Important

La Base de données principale (URL) utilisant Punycode, les expressions régulières et les mots-clés qui incluent des caractères Unicode ne trouvent jamais de correspondance.

Accès à Content Gateway et alertes

Dans les déploiements Websense Web Security Gateway et Gateway Anywhere, Content Gateway récupère à présent automatiquement les informations de ses clés auprès de Policy Server. La saisie de ces informations dans Content Gateway Manager n'est donc plus nécessaire.

Par ailleurs :

- Une nouvelle page **Paramètres > Général > Content Gateway Access (Accès à Content Gateway)** de TRITON - Web Security permet aux administrateurs de démarrer Content Gateway Manager depuis TRITON.

  La page présente l'état (en exécution ou arrêté), l'adresse IP et le nom d'hôte, le nom du cluster et la description de chaque instance de Content Gateway enregistrée auprès de l'instance de Policy Server sélectionnée.
- Les alertes importantes à propos du fonctionnement de Content Gateway s'affichent dans TRITON - Web Security.

  Comme pour les autres alertes de fonctionnement, une brève alerte apparaît dans le Tableau de bord et un message plus détaillé dans la page Alertes.
- Pour configurer les alertes système Web Security et Content Gateway, servez-vous de la page Paramètres > Alertes > Système.

  Comme pour les alertes Web Security existantes, vous pouvez configurer quelles conditions de Content Gateway doivent entraîner l'envoi de messages d'alerte et quelles méthodes (e-mail, message contextuel ou SNMP) doivent être utilisées pour envoyer l'alerte.

6 Nouveautés de la Version 7.7

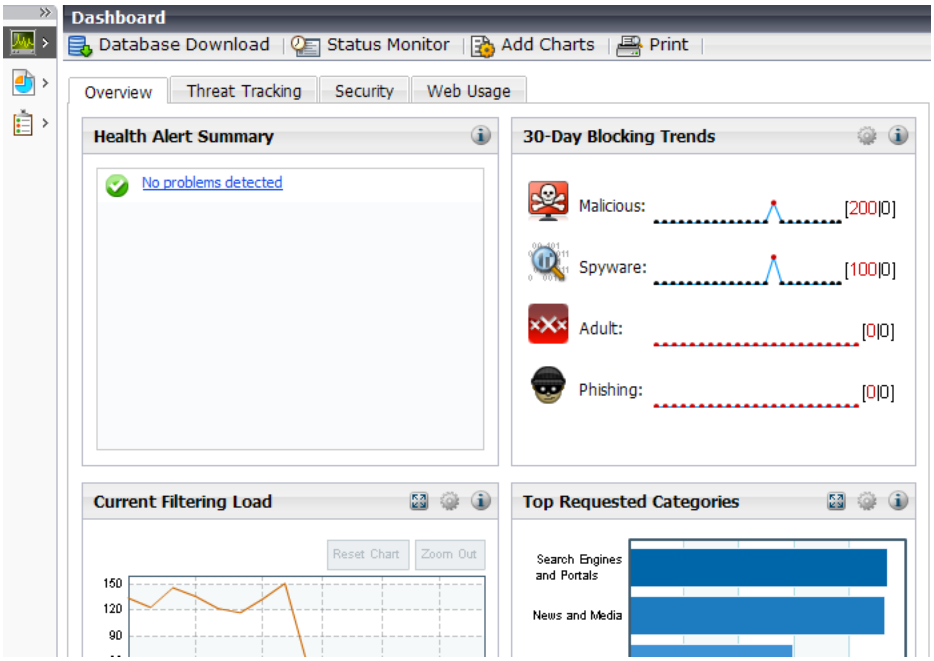
La version 7.7 introduit les fonctionnalités suivantes, nouvelles ou étendues :

- *Amélioration du Tableau de bord de Web Security*, page 42
- *Outils de protection contre le contenu malveillant avancé*, page 43
- *Exceptions : Listes blanche et noire d'URL*, page 44
- *Amélioration des rapports de présentation*, page 45
- *Temps de navigation disponible dans les rapports d'investigation détaillés*, page 46
- *Amélioration du blocage des types de fichiers*, page 47
- *Informations supplémentaires dans les pages de blocage*, page 48
- *Configuration centralisée de Log Server*, page 48
- *Amélioration de la configuration de la Base de données d'activité*, page 49
- *Prise en charge étendue des ports SQL Server non standard*, page 49
- *Prise en charge du cryptage SSL avec SQL Server*, page 50
- *Amélioration de la configuration de DC Agent*, page 50
- *Nouvelle identification transparente et journalisation des alertes de fonctionnement*, page 51
- *Actions dépendant du temps dans les déploiements Filtering Service multiples*, page 52
- *Intégration aux solutions SIEM tierces*, page 52
- *Filtrage des URL et des clients IPv6*, page 53
- (*Web Security Gateway* et *Gateway Anywhere*) *Accès direct du Super administrateur à Content Gateway Manager*, page 53
- (*Web Security Gateway Anywhere*) *Amélioration de la configuration de Directory Agent*, page 53
- (*Web Security Gateway Anywhere*) *Génération de rapports d'agent utilisateur hybride et authentification personnalisée*, page 54
- (*Web Security Gateway Anywhere*) *Basculement vers le service hybride*, page 55
- (*Web Security Gateway Anywhere*) *Autres améliorations du service hybride*, page 55

Amélioration du Tableau de bord de Web Security

Les pages État > Aujourd'hui et Historique ont été fusionnées au sein d'une page État > Tableau de bord présentant plusieurs onglets.

Lorsque vous vous connectez à TRITON - Web Security, le Tableau de bord Menaces s'affiche et vous donne des informations sur l'activité suspecte de votre réseau. Le type d'informations et le niveau de détails dépendent de votre niveau d'abonnement. Web Security Gateway ou Web Security Gateway Anywhere est exigé pour afficher des informations sur les menaces sortantes et pour fournir des données d'analyse détaillées à propos des menaces. Voir *Outils de protection contre le contenu malveillant avancé*, page 43.



Le tableau de bord comprend 3 onglets supplémentaires :

- L'onglet **Risques** donne des informations sur les requêtes d'URL autorisées et bloquées appartenant à la classe Risques de sécurité. Le volume d'informations donné dépend de votre niveau d'abonnement. Pour pouvoir afficher les informations relatives aux requêtes de certaines catégories de sécurité, Web Security, Web Security Gateway ou Web Security Gateway Anywhere est nécessaire.
- L'onglet **Usage** donne des informations sur les modèles de trafic de votre réseau.
- L'onglet **Système** présente les messages d'alerte, les informations d'état et les graphiques illustrant l'état actuel de votre logiciel Web Security, en se concentrant sur l'activité Internet de votre réseau.

Les éléments des tableaux de bord Risques, Usage et Système peuvent être configurés de manière à afficher les données de diverses périodes (par défaut, de 1 à 30 jours). La plupart des graphiques peuvent être modifiés pour s'afficher sous forme de graphiques à barres, de courbes ou de graphiques en secteurs.

Par ailleurs, vous avez désormais la possibilité d'afficher plusieurs versions du même élément de tableau de bord dans le même onglet ou dans des onglets distincts. Vous pouvez afficher un graphique des principaux sites non catégorisés et leurs valeurs du jour à côté d'un graphique des sites non catégorisés au cours des deux dernières semaines.

Vous pouvez afficher jusqu'à 12 éléments de tableau de bord dans chaque onglet.

Les modifications apportées aux graphiques des tableaux de bord et à la mise en page du tableau de bord général sont enregistrées séparément pour chaque compte d'administrateur.

Outils de protection contre le contenu malveillant avancé

Le tableau de bord **Menaces** vous permet de surveiller et d'examiner l'activité dangereuse de votre réseau susceptible de révéler des attaques potentiellement malveillantes.

- Web Security Gateway ou Web Security Gateway Anywhere est exigé pour afficher des informations sur les menaces sortantes et pour fournir des données d'analyse détaillées à propos des menaces.
- Dans le tableau de bord Menaces, vous ne pouvez ni ajouter ni retirer des éléments.

Le tableau de bord Menaces initial présente trois éléments principaux :

- L'élément **Top Security Destinations (Principales destinations de sécurité)** présente les 10 principaux pays (destinations) visés par le trafic réseau suspect.
- L'élément **Security Events by Type (Événements de sécurité par type)** présente le nombre de requêtes de sites (destinations) bloquées dans les catégories de sécurité associées aux menaces dangereuses.
- L'élément **Suspicious Event Summary (Synthèse des événements suspects)** donne des informations sur la gravité, l'adresse IP source, l'utilisateur, le nom d'hôte (si disponible ; requiert Websense Content Gateway), la catégorie, l'heure, la direction et la destination des requêtes bloquées et autorisées liées à des menaces dangereuses.

Les commandes situées en haut de l'onglet vous permettent de limiter l'affichage des informations à des types de gravité (Critique, Élevée, Moyenne ou Faible), de directions (trafic entrant ou sortant) et de périodes spécifiques (depuis minuit, dernières 24 heures, dernières 48 heures, semaine précédente, etc.).

Vous pouvez également cliquer sur une zone géographique ou sur une catégorie des graphiques situés en haut de la page pour affiner encore davantage les informations affichées dans le tableau de synthèse.

Cliquez sur un nom d'utilisateur, une adresse IP ou un nom de périphérique dans le tableau de synthèse pour afficher une page détaillant les informations relatives à l'ensemble des incidents liés au client sélectionné, y compris les données d'analyse (éventuellement) collectées.

Notez que les Super administrateurs inconditionnels peuvent accorder un accès au tableau de bord Menaces tout en bloquant l'accès aux données d'analyse liées aux incidents. Comme les attaques dangereuses avancées tentent d'accéder aux données sensibles des individus et des organisations, les données d'analyse peuvent inclure des fichiers renfermant des informations confidentielles.

Déclenchement d'alertes en fonction de la gravité de l'activité Internet suspecte

Websense peut vous avertir par courrier électronique ou SNMP lorsqu'une activité suspecte de niveau de gravité défini (critique, élevée, moyenne ou faible) atteint le seuil défini. Cette activité suspecte peut être le signe d'une attaque dangereuse avancée potentielle dans votre réseau.

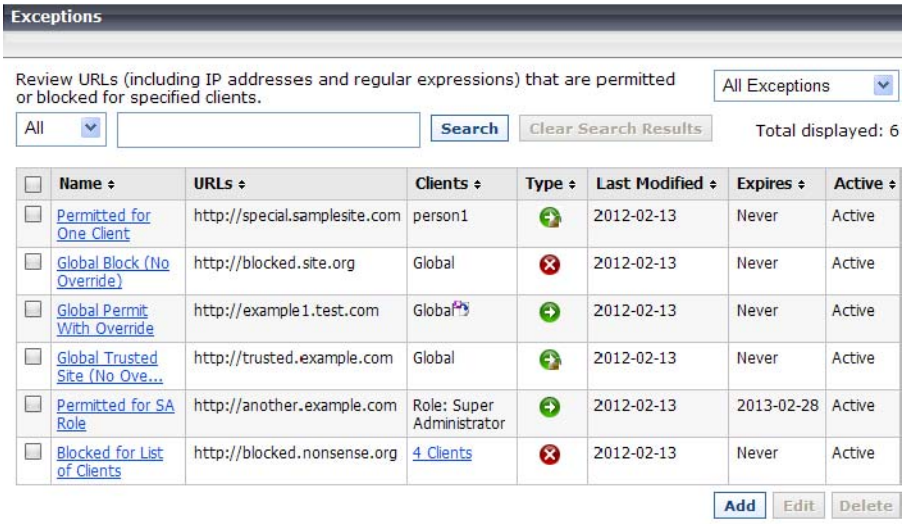
- Définissez des alertes pour les requêtes autorisées et bloquées à chaque niveau de gravité.
- Chaque message d'alerte inclut un lien conduisant à la page Menaces > Event Details (Détails de l'événement) qui vous permet d'examiner les incidents associés.

Pour activer, désactiver ou modifier la configuration des alertes liées aux événements suspects détectés dans votre réseau, servez-vous de la page **Paramètres > Alertes > Suspicious Activity (Activité suspecte)**.

Les paramètres de contrôle des flux configurés pour les alertes d'utilisation de catégories et de protocoles s'appliquent également aux alertes d'activité suspecte.

Exceptions : Listes blanche et noire d'URL

Les exceptions permettent aux administrateurs d'autoriser rapidement des URL et des adresses IP appartenant à des catégories bloquées ou de bloquer des URL et des adresses IP appartenant à des catégories autorisées.



La création d'une exception n'implique pas la modification de la catégorie de l'URL et ne change pas la stratégie appliquée aux clients concernés. Les exceptions permettent simplement de répondre rapidement et avec une grande souplesse aux requêtes des utilisateurs, aux changements de politique de l'entreprise, à des pics d'activité Internet ou à d'autres changements contextuels.

Les exceptions autorisées remplacent les URL non filtrées et permettent d'autoriser un ou plusieurs clients à accéder aux URL ou aux adresses IP classées dans des catégories bloquées.

Pour gérer les exceptions, utilisez la page **Gestion des stratégies > Exceptions** de TRITON - Web Security.

Les Super administrateurs peuvent voir toutes les exceptions, quel que soit le rôle dans lequel ils ont été créés. Les administrateurs délégués peuvent voir toutes les exceptions qui affectent leur rôle actuel.

Des exceptions peuvent être créées pour :

- Un unique client (utilisateur, groupe, unité d'organisation (UO), adresse IP ou plage réseau)
- Une liste de clients spécifiques (identifiés par utilisateur, groupe, unité d'organisation (UO), adresse IP ou plage d'adresses IP)
- Tous les clients dans tous les rôles (exception globale)

  Seuls les Super administrateurs peuvent créer des exceptions globales. Lors de la création d'une exception globale, le Super administrateur peut indiquer si cette exception est prioritaire sur toutes celles définies par les administrateurs délégués (par défaut), ou si les exceptions définies par les administrateurs délégués remplacent cette exception globale.
- Tous les clients d'un rôle d'administration déléguée

Amélioration des rapports de présentation

Les améliorations apportées aux rapports de présentation vous permettent de :

- Créer entièrement vos propres rapports. En plus d'exploiter les rapports existants (personnalisés ou prédéfinis), vous pouvez sélectionner l'un des deux **modèles de base** pour créer un rapport de **tendances** ou de **N premiers**.

Nom du modèle	Description
Modèles de base > Nouveau rapport de tendances	Permet de définir un nouveau rapport de tendances Saisissez le nom et le titre du rapport, affectez-le à une catégorie de rapports, puis définissez ses éléments de base, notamment : • L'unité de temps (jour, semaine, mois ou année) • L'option de tri (catégorie, protocole, classe de risques, action, utilisateur ou groupe) • L'unité de mesure principale (requêtes, temps de navigation, bande passante) • D'autres unités de mesure (lorsque les requêtes sont définies comme mesure principale, il est possible d'ajouter le temps de navigation et la bande passante comme mesures secondaires) Cliquez sur **Enregistrer et modifier** pour affiner encore le rapport en utilisant les mêmes filtres que pour les rapports prédéfinis ou personnalisés.

Nom du modèle	Description
Modèle de base > Nouveau rapport N premiers	Permet de définir un nouveau rapport N premiers Saisissez le nom et le titre du rapport, affectez-le à une catégorie de rapports, puis définissez ses éléments de base, notamment : • L'option de tri (catégorie, protocole, classe de risques, action, utilisateur ou groupe) • L'unité de mesure principale (requêtes, temps de navigation, bande passante) • D'autres unités de mesure (lorsque les requêtes sont définies comme mesure principale, il est possible d'ajouter le temps de navigation et la bande passante comme mesures secondaires) Cliquez sur **Enregistrer et modifier** pour affiner encore le rapport en utilisant les mêmes filtres que pour les rapports prédéfinis ou personnalisés.

- Nouveaux rapports de tendances prédéfinis pour surveiller les tendances des catégories Social Networking (Réseaux sociaux) et Risques de sécurité

Nom du rapport	Description
Tendances > Social Networking Trends by Requests (Tendances Réseaux sociaux par requêtes)	Présente les demandes d'URL classées dans les catégories Social Networking (Réseaux sociaux) sur la période sélectionnée. Des informations résumées présentant le nombre total de requêtes pour chaque point de données de la période sont fournies au-dessous du graphique.
Tendances > Security Risk Trends by Requests (Tendances Risques de sécurité par requêtes)	Présente les demandes d'URL classées dans les catégories Risques de sécurité sur la période sélectionnée. Des informations résumées présentant le nombre total de requêtes pour chaque point de données de la période sont fournies au-dessous du graphique.

- Nouvelle catégorie **User-Defined (Défini par l'utilisateur)** au sein du Catalogue de rapports pour stocker les rapports personnalisés
- Combinez les informations de requêtes, de temps de navigation et de bande passante (si disponible) dans les rapports existants. Jusqu'à présent, il n'était pas possible d'afficher ces trois mesures simultanément.

Temps de navigation disponible dans les rapports d'investigation détaillés

Dans les versions précédentes, les rapports d'investigation ne pouvaient inclure d'informations relatives au temps de navigation Internet que dans les rapports résumés. La version 7.7 vous permet d'activer le calcul du temps de navigation dans les rapports d'investigation détaillés via la page **Paramètres > Génération de rapports > Base de données d'activité** de TRITON - Web Security.

Lorsque cette option est activée, la colonne **Temps de navigation** s'affiche lorsque vous créez ou modifiez des rapports d'investigation détaillés.

- L'enregistrement des détails du temps de navigation augmente la taille de la Base de données d'activité. Après avoir activé cette fonctionnalité, surveillez les données **Growth Rates and Sizing (Taux de croissance et tailles)** de la page Base de données d'activité dans le cas où la différence de taille implique une modification de vos paramètres de remplacement.
- Les informations de temps de navigation indiquées dans les rapports détaillés ne sont disponibles que pour les dates ultérieures à la date d'activation de cette fonctionnalité.

Amélioration du blocage des types de fichiers

Dans les versions précédentes, lorsque le blocage de types de fichiers s'appliquait à une catégorie, ce blocage était exclusivement basé sur l'extension des fichiers.

Désormais, lorsque les clients Websense Web Security Gateway et Gateway Anywhere activent le blocage des types de fichiers et qu'un utilisateur demande un site, Websense :

1. Détermine la catégorie de l'URL
2. Vérifie l'extension du fichier
3. Lorsque l'extension de ce fichier n'est pas bloquée, Content Gateway ou le service hybride analyse son contenu pour identifier son type réel.

Les différents types de fichiers prédéfinis utilisés pour l'association des extensions ont en outre été modifiés comme suit :

Type de fichier	Extensions associées
Fichiers compressés	.ace, .arc, .arj, .b64, .bhx, .cab, .gz, .gzip, .hqx, .iso, .jar, .lzh, .mim, .rar, tar, taz, .tgz, .tz, .uu, .uue, .xxe, .z, .zip
Documents	.ade, .adp, .asd, .cwk, .doc, .docx, .dot, .dotm, .dotx, .grv, .iaf, .lit, .lwp, .maf, .mam, .maq, .mar, .mat, .mda, .mdb, .mde, .mdt, .mdw, .mpd, .mpp, .mpt, .msg, .oab, .obi, .oft, .olm, .one, .ops, .ost, .pa, .pdf, .pip, .pot, .potm, .potx, .ppa, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .pst, .pub, .puz, .sldm, .sldx, .snp, .svd, .thmx, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .wbk, .wks, .wll, .wri, .xar, .xl, .xla, .xlb, .xlc, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xsf, .xsn
Exécutables	.bat, .exe
Images	.bmp, .cmu, .djvu, .emf, .fbm, .fits, .gif, .icb, .ico, .jpeg, .jpg, .mgr, .miff, .pbf, .pbm, .pcx, .pdd, .pds, .pix, .png, .psb, .psd, .psp, .rle, .sgi, .sir, .targa, .tga, .tif, .tiff, .tpic, .vda, .vst, .zif
Multimédia	.aif, .aifc, .aiff, .asf, .asx, .avi, .ivf, .m1v, .m3u, .mid, .midi, .mov, .mp2, .mp2v, .mp3, .mpa, .mpe, .mpg, .mpv2, .ogg, .qt, .ra, .ram, .rmi, .snd, .wav, .wax, .wm, .wma, .wmp, .wmv, .wmx, .wxv
Applications Internet multimédia	.swf
Texte	.htm, .html, .txt, .xht, .xhtml, .xml
Menaces	.vbs, .wmf

Informations supplémentaires dans les pages de blocage

Lorsqu'un utilisateur clique sur **Plus d'informations** dans une page de blocage, une page de blocage secondaire indique :

- La **Catégorie en temps réel** éventuellement affectée à l'URL. Il s'agit là de la catégorie renvoyée par Content Gateway après analyse du site.
- La **Catégorie statique** affectée à l'URL dans la Base de données principale Websense
- Le composant Web Security à l'origine de la catégorie ayant entraîné le blocage du site (**Catégorie définie par**).

Comme dans les versions précédentes, les administrateurs peuvent cliquer du bouton droit sur le cadre principal de la page Plus d'informations pour obtenir plus de détails sur le mode de filtrage de la requête.

Les déploiements Websense Web Security Gateway et Gateway Anywhere permettent désormais d'ajouter un lien vers ACEInsight dans la page de blocage de sécurité. Ce service gratuit fourni par les laboratoires Websense Security Labs permet de consulter des informations détaillées sur une URL.

Pour activer le lien ACEInsight dans la page de blocage de sécurité, sélectionnez **Paramètres > Général > Filtrage** de TRITON - Web Security.

Lorsqu'un site HTTPS est envoyé à ACEInsight pour analyse, la page de blocage transmet uniquement la portion du domaine de l'URL. Les informations sensibles éventuellement incluses dans la chaîne de requête ne sont donc pas transmises par Internet. Par conséquent, ACEInsight ne peut pas analyser la page avec la même profondeur que Content Gateway et peut éventuellement renvoyer une catégorisation autre que celle utilisée pour bloquer la requête.

Configuration centralisée de Log Server

Les fonctionnalités et fonctions de l'utilitaire de configuration de Web Security Log Server sont désormais intégrées à la console TRITON. Au lieu de démarrer un outil distinct pour gérer les détails des connexions Log Server, ouvrez la page **Paramètres > Génération de rapports > Log Server** dans TRITON - Web Security.

Cette page vous permet de :

- Actualiser les informations sur les ports de Log Server
- Gérer la connexion à la Base de données d'activité ODBC
- Activer ou désactiver la communication SSL cryptée avec la Base de données d'activité (voir *Prise en charge du cryptage SSL avec SQL Server*, page 50)
- Gérer le compte utilisé par Log Server pour se connecter à la Base de données d'activité
- Tester la communication entre Log Server et la Base de données d'activité
- Configurer la méthode utilisée pour ajouter des enregistrements dans la base de données (ODBC ou BCP), ainsi que l'emplacement de stockage des fichiers BCP
- Configurer le regroupement des enregistrements de journaux et choisir de stocker les visites ou les accès

- Définir la fréquence à laquelle Log Server doit récupérer les informations d'utilisateur et de groupe auprès de User Service

La configuration de WebCatcher s'effectue à présent dans la page **Paramètres > Général > Comptes**.

Grâce à ces modifications, les mises à jour apportées à la configuration de Log Server n'exigent plus le redémarrage du service Websense Log Server. Les modifications de la connexion à la base de données requièrent toutefois le redémarrage du service Websense TRITON - Web Security afin que les graphiques et rapports de présentation du tableau de bord puissent continuer à récupérer les données des rapports.

Amélioration de la configuration de la Base de données d'activité

La page **Paramètres > Génération de rapports > Base de données d'activité** de TRITON - Web Security simplifie désormais la configuration de la Base de données d'activité et offre de nouvelles fonctionnalités.

- Un nouveau graphique **Growth Rates and Sizing (Taux de croissance et tailles)** présente la taille moyenne quotidienne de chaque partition de journalisation de la Base de données d'activité.

  Exploitez ces informations pour prévoir la croissance future et optimiser la planification des remplacements.
- Les options **Internet Browse Time (Temps de navigation Internet)** permettent désormais de calculer en détail le temps de navigation pour alimenter les rapports d'investigation détaillés. Voir *Temps de navigation disponible dans les rapports d'investigation détaillés*, page 46.

  L'activation des calculs détaillés du temps de navigation augmente la taille de la Base de données d'activité.
- Pour prendre en charge les rapports de tendances dans le Tableau de bord Web Security et les rapports de présentation, les options **Trend Data Retention (Conservation des données de tendances)** vous permettent de choisir de calculer ou de stocker les données de tendances. Vous pouvez également définir la durée de conservation des données des tendances hebdomadaires, mensuelles et annuelles. Les données des tendances quotidiennes sont stockées pendant 90 jours.

  L'activation du stockage des données de tendances accroît la taille de la Base de données d'activité.

Prise en charge étendue des ports SQL Server non standard

Lors de l'installation de TRITON Unified Security Center, vous pouvez à présent sélectionner un port Microsoft SQL Server non standard. Lorsque vous saisissez un port non standard dans le programme d'installation de l'infrastructure TRITON, des informations relatives à ce port sont transmises au programme d'installation de Web Security.

Les versions précédentes imposaient l'utilisation du port par défaut 1433 pendant l'installation et permettaient de le modifier une fois l'installation terminée.

Au besoin, vous pouvez toujours modifier le port de connexion de SQL Server après l'installation via la page Paramètres > Génération de rapports > Log Server de TRITON - Web Security. (L'utilitaire de configuration de Log Server n'est plus nécessaire.)

Prise en charge du cryptage SSL avec SQL Server

Si votre installation Microsoft SQL Server est configurée pour utiliser le cryptage SSL, une nouvelle option **Utiliser SSL** est à présent disponible dans le programme d'installation de TRITON Unified et dans la page Paramètres > Génération de rapports > Log Server de TRITON - Web Security.

Important

Selon votre configuration Microsoft SQL Server (si l'option « Faire confiance au certificat du serveur » est définie sur « Non » dans SQL Server), il vous faudra éventuellement déployer des certificats signés par une autorité de certification dans SQL Server, dans le serveur de gestion TRITON et dans les ordinateurs Log Server avant de pouvoir activer cette fonction dans le programme d'installation ou dans la console TRITON.

Avec ce fonctionnement, les organisations qui exigent des conditions de sécurité particulières peuvent crypter les données que Log Server envoie à la base de données d'activité.

Pour plus d'informations sur la configuration du cryptage SSL, reportez-vous à votre documentation Microsoft SQL Server.

Amélioration de la configuration de DC Agent

Pour enregistrer les domaines et les contrôleurs de domaine qu'il détecte, DC Agent utilise un fichier nommé **dc_config.txt**. Lorsqu'une ou plusieurs instances de DC Agent sont installées dans votre réseau, vous pouvez désormais consulter la liste complète des domaines et des contrôleurs de domaine interrogés par toutes les instances de DC Agent de votre réseau depuis TRITON - Web Security. Pour cela, ouvrez la page **Paramètres > Général > Identification des utilisateurs**, puis cliquez sur **View Domain List (Afficher la liste des domaines)**.

Par ailleurs, vous pouvez désormais configurer les paramètres de détection des domaines de DC Agent dans la page **Identification des utilisateurs > DC Agent**.

- Activez ou désactivez la détection automatique des domaines (processus par lequel DC Agent identifie les domaines et les contrôleurs de domaine qu'il peut interroger).

- Indiquez la fréquence d'exécution du processus de détection par DC Agent.
- Indiquez si la détection des domaines doit être effectuée par DC Agent ou User Service.

Comme dans les versions précédentes, vous pouvez configurer manuellement ces paramètres dans le fichier **transid.ini** pour chaque instance de DC Agent. (Le fichier transid.ini n'est plus créé au moment de l'installation, mais est conservé lors des mises à niveau, et peut également être créé manuellement.)

Nouvelle identification transparente et journalisation des alertes de fonctionnement

Une série de nouvelles alertes de fonctionnement préviennent les administrateurs lorsque Filtering Service ne peut plus communiquer avec un agent d'identification Websense transparent :

- Filtering Service ne peut pas communiquer avec DC Agent.
- Filtering Service ne peut pas communiquer avec Logon Agent.
- Filtering Service ne peut pas communiquer avec eDirectory Agent.
- Filtering Service ne peut pas communiquer avec RADIUS Agent.

Lorsque problème de réseau ou de communication empêche Filtering Service de communiquer avec un agent d'identification transparent, les correspondances des utilisateurs de Filtering Service peuvent ne pas être mises à jour en temps voulu et les stratégies basées sur l'utilisateur risquent de ne pas s'appliquer correctement.

Les autres nouvelles alertent de fonctionnement préviennent par avance les administrateurs des problèmes de la Base de données d'activité et de Log Server :

- Le répertoire du cache d'une instance de Log Server contient plus de 100 fichiers en cache.

  Habituellement, les fichiers mis en cache par Log Server sont régulièrement déplacés dans la Base de données d'activité. Cette accumulation de fichiers dans le cache peut révéler un problème réseau, une modification du compte utilisé par Log Server pour se connecter à la Base de données d'activité, des problèmes d'espace disque dans l'ordinateur de la Base de données d'activité ou d'autres problèmes encore.
- Log Server n'a pas reçu les fichiers journaux de Filtering Service depuis plus d'une heure.

  Filtering Service est chargé de transmettre les données des journaux à Log Server. Si Filtering Service ne peut pas communiquer avec Log Server, ces données sont perdues.
- La tâche ETL de la base de données d'activité n'a pas pu être effectuée depuis 4 heures.

  La tâche d'extraction, de transformation et de chargement (ETL, Extract, Transform, and Load) est chargée de traiter les données de la base de données des partitions. Pour bien fonctionner, cette tâche doit disposer de suffisamment d'espace disque, de vitesse de disque et d'autres ressources système.

Actions dépendant du temps dans les déploiements Filtering Service multiples

Si, dans votre déploiement, plusieurs instances de Filtering Service sont susceptibles de gérer une requête provenant d'un même utilisateur, il est possible d'installer un composant facultatif, **Websense State Server**, pour activer l'application appropriée des actions de filtrage temporel (Quota, Confirmer, Accès par mot de passe et Account Override (Remplacement de compte)).

Une fois installé, ce composant State Server permet aux instances de Filtering Service associées de partager les informations temporelles, de sorte que les utilisateurs puissent recevoir les affectations appropriées de quota, de confirmation ou de changement de session.

State Server est généralement installé dans un serveur Policy Server et une seule instance de State Server est requise par **déploiement logique**. Un déploiement logique est un groupe quelconque d'instances de Policy Server et de Filtering Service susceptibles de gérer les requêtes provenant du même ensemble d'utilisateurs.

- Toutes les instances de Filtering Service qui communiquent avec la même instance de State Server doivent partager le même fuseau horaire et l'heure de ces ordinateurs doit être synchronisée.
- Chaque instance de Filtering Service peut uniquement communiquer avec une seule instance de State Server.
- Toutes les instances de Filtering Service associées à la même instance de Policy Server doivent communiquer avec la même instance de State Server.
- Plusieurs instances de Policy Server peuvent partager une même instance de State Server.

Intégration aux solutions SIEM tierces

Si votre organisation utilise une solution SIEM (Security Information and Event Management), vous pouvez configurer Websense pour qu'il transmette les données des journaux de Filtering Service au produit SIEM.

Avant d'activer l'intégration SIEM, vous devez installer un nouveau composant, **Websense Multiplexer**, pour chaque instance de Policy Server présente dans votre déploiement.

Activez l'intégration SIEM dans la page **Paramètres > Général > SIEM Integration (Intégration SIEM)** de TRITON - Web Security, puis sélectionnez la syntaxe à utiliser pour mettre les données en forme (syslog/CEF [Arcsight], syslog/LEEF [QRadar], syslog/key-value pairs [Splunk et autres] ou personnalisée). Si vous choisissez de personnaliser la syntaxe, vous êtes invité à saisir une chaîne de format.

Une fois l'intégration SIEM activée, Websense Multiplexer commence à transmettre les données de Filtering Service à Log Server et au produit SIEM.

Filtrage des URL et des clients IPv6

La possibilité de bloquer ou d'autoriser le trafic IPv6 via Network Agent, introduite dans la version 7.6, a été élargie de manière à autoriser le filtrage complet des adresses IPv6.

- Pour recatégoriser, bloquer ou autoriser les sites Web identifiés par des adresses IPv6, créez des exceptions ou des URL personnalisées.
- Ajoutez et attribuez des stratégies aux clients identifiés par une adresse ou une plage d'adresses IPv6.

Aucune configuration particulière n'est nécessaire pour activer cette fonctionnalité.

Lorsqu'un champ de TRITON - Web Security requiert un format d'adresse IP spécifique, le format est indiqué (par exemple, « adresse IPv4 »). Dans le cas contraire, vous pouvez utiliser n'importe quel format.

Les ordinateurs qui hébergent des composants Websense Web Security doivent avoir une adresse IPv4.

Accès direct du Super administrateur à Content Gateway Manager

Les administrateurs de la sécurité globale et les Super administrateurs inconditionnels de Websense Web Security Gateway et Gateway Anywhere peuvent désormais activer l'authentification unique pour les Super administrateurs qui se connectent à Content Gateway Manager à partir de TRITON - Web Security.

Lorsque l'accès par authentification unique est activé, les Super administrateurs qui disposent d'autorisations **Content Gateway single sign-on (Authentification unique Content Gateway)** peuvent accéder à la page **Paramètres > Général > Content Gateway Access (Accès à Content Gateway)** de TRITON - Web Security et cliquer sur l'option **Se connecter** accolée à l'adresse IP ou au nom d'hôte d'une instance de Content Gateway.

Les autorisations d'authentification unique pour Content Gateway sont attribuées lors de l'ajout de l'administrateur au rôle Super administrateurs et peuvent être supprimées par les Super administrateurs inconditionnels.

L'administrateur accède alors directement à Content Gateway Manager sans passer par la page de connexion et sans saisir ses identifiants de connexion.

Amélioration de la configuration de Directory Agent

La page **Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées)** de TRITON - Web Security a été modifiée de manière à simplifier la configuration de Directory Agent par les administrateurs Websense Web Security Gateway Anywhere et à inclure et exclure certains contextes de services d'annuaire.

Au lieu de demander la saisie des informations de contexte de l'annuaire, l'arborescence des annuaires s'affiche. Accédez au contexte que vous souhaitez inclure ou exclure des recherches de Directory Agent ou servez-vous de l'option de recherche pour afficher les contextes correspondants dans l'arborescence.

Les administrateurs peuvent alors plus facilement :

- Identifier les contextes qui contiennent des utilisateurs filtrés par le service hybride
- Limiter les contextes d'annuaire synchronisés avec le service hybride pour gagner du temps et améliorer les performances
- Exclure les contextes susceptibles d'induire des problèmes de synchronisation (par exemple, les contextes qui contiennent des groupes incluant des entrées d'adresse électronique en double)

Génération de rapports d'agent utilisateur hybride et authentification personnalisée

La page **État > Hybrid Service (Service hybride)** contient à présent un lien qui permet d'accéder au rapport **User Agent Volume (Volume User Agent)**. Le résultat du rapport est un tableau qui indique :

- Les agents utilisateur qui ont demandé l'authentification

  Un agent utilisateur est une chaîne envoyée par le navigateur ou l'application pour s'identifier et qui précise son numéro de version et des détails système tel que le système d'exploitation.
- Le nombre de requêtes d'authentification et de requêtes totales effectuées par chaque agent utilisateur
- La date de la dernière mise à jour du nombre de requêtes
- Si une règle d'authentification personnalisée a ou non été créée pour l'agent utilisateur

Si l'un des agents utilisateur du rapport est associé à un grand nombre de demandes d'authentification, il est possible qu'il rencontre des problèmes pour s'authentifier. Vous pouvez créer une nouvelle règle d'authentification personnalisée pour autoriser l'agent à ignorer l'authentification ou à utiliser un autre type d'authentification. Sélectionnez un ou plusieurs agents utilisateur dans le rapport, puis cliquez sur **Create Rule (Créer une règle)**.

Vous devez configurer les règles d'authentification personnalisées dans la nouvelle page **Paramètres > Hybrid Configuration (Configuration hybride) > Custom Authentication (Authentification personnalisée)**. Cette page vous permet d'identifier les applications qui ne gèrent pas correctement les demandes d'authentification en définissant des agents utilisateur, des domaines ou des URL, ou encore une combinaison de ces options.

Après avoir défini l'application, définissez le type d'authentification éventuellement nécessaire.

Basculement vers le service hybride

Les administrateurs de Websense Web Security Gateway Anywhere ont à présent la possibilité de configurer le basculement vers le service hybride des emplacements filtrés qui utilisent des proxy explicites. Ce fonctionnement garantit l'accès à Internet et le filtrage systématique des utilisateurs lorsque vos autres proxy ne sont pas disponibles.

Le basculement vers le service hybride d'un emplacement filtré doit être approuvé afin que les services Websense puissent provisionner le nombre d'utilisateurs approprié au sein du centre de données le plus proche de votre site local. Une fois que le basculement d'un emplacement filtré a été approuvé, sa réapprobation n'est plus nécessaire si vous en modifiez les détails ou lorsque vous le désactivez avant de le réactiver.

Autres améliorations du service hybride

- La page **Paramètres > Hybrid Configuration (Configuration hybride) > Filtered Locations (Emplacements filtrés)** a été modifiée de manière à mieux faire la différence entre les emplacements filtrés par des composants sur site et les emplacements filtrés par le service hybride.
- La page **Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs)** comprend à présent une option qui permet de créer ou de modifier le mot de passe d'anti-altération de Websense Web Endpoint.
- La page **Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs)** inclut désormais également une autre méthode d'identification et d'authentification des utilisateurs. Outre l'authentification NTLM et de base, il est possible d'utiliser une forme sécurisée d'authentification.
- Pour les sites qui souhaitent utiliser le fichier PAC par défaut, mais pour lesquels le port 8082 ou 8081 est verrouillé, la section Fichier d'auto-configuration du proxy de la page **Paramètres > Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)** propose à présent 2 options :
  - L'URL du fichier PAC par défaut, récupérée via le port 8082 (requiert également le port 8081)
  - Une autre URL de fichier PAC, récupérée via le port 80

7 Où puis-je trouver...?

Le processus de mise à niveau préserve les informations existantes (configuration, clients et stratégies). Toutefois, les modifications apportées à TRITON - Web Security (auparavant Websense Manager) signifient que certaines fonctions communes ont été déplacées ou renommées.

Cette section vous permettra de localiser les fonctions et outils habituels tout au long de votre découverte de TRITON - Web Security.

Pour démarrer, sélectionnez l'outil ou la fonction que vous recherchez :

- *Ma stratégie Global*, page 57
- *Mes jeux de catégories et de protocoles Default Settings*, page 58
- *Pages Aujourd'hui et Historique*, page 58
- *Mes listes d'acceptation*, page 59
- *Mes URL personnalisées*, page 59
- *Mes URL non filtrées*, page 59
- *Mes objets d'annuaire*, page 59
- *Websense Explorer*, page 60
- *Websense Reporter*, page 60
- *Utilitaire de configuration de Log Server*, page 60
- *Mes rapports*, page 60
- *Real-Time Analyzer*, page 63
- *Mes paramètres de serveurs*, page 63
- *Mes paramètres Network Agent locaux*, page 63
- *Gestion des comptes d'administrateur*, page 63
- *Détecteur de trafic réseau (Outil de visibilité du trafic)*, page 64
- *Gestion des clés d'abonnement*, page 64

Ma stratégie Global

Votre stratégie ***Global** a été renommée **Par défaut**.

- Elle impose toujours les mêmes paramètres de filtrage, avec le même planning.
- Elle continue de filtrer tous les clients tant qu'aucune autre stratégie n'est appliquée.

Pour vérifier que vos paramètres de filtrage n'ont pas changé, sélectionnez **Gestion des stratégies > Stratégies**, puis cliquez sur **Par défaut**. Cliquez sur une période du planning pour voir quels filtres (auparavant jeux de catégories, jeux de protocoles et listes d'acceptation) sont imposés par cette stratégie.

Important

La stratégie **Par défaut** doit couvrir toutes les périodes, 24 heures sur 24 et 7 jours sur 7. Lorsque certaines périodes n'étaient pas couvertes par votre stratégie Global, vous n'étiez pas invité à définir une couverture complète. Lorsque vous modifiez la stratégie Par défaut, toutefois, vous ne pouvez pas enregistrer vos modifications tant que certaines périodes ne sont pas couvertes.

Mes jeux de catégories et de protocoles Default Settings

Vos jeux de catégories et de protocoles **Default Settings** ont été renommés. Ils correspondent à présent aux filtres de catégories et de protocoles **Par défaut**.

Il ne s'agit là que d'un changement de nom qui n'affecte pas vos paramètres de filtrage.

Pour vérifier les paramètres appliqués par les filtres de catégories et de protocoles Par défaut, sélectionnez **Gestion des stratégies > Filtres**, puis cliquez sur le nom du filtre dans la liste appropriée.

Pages Aujourd'hui et Historique

Les pages Aujourd'hui et Historique ont été fusionnées dans le **Tableau de bord Web Security**. Le tableau de bord comprend 4 onglets : Menaces, Risques, Usage et Système.

Les modifications apportées aux onglets et graphiques du tableau de bord sont enregistrées séparément pour chaque compte d'administrateur.

Les graphiques et compteurs disponibles dans les versions 7.0 et ultérieures se répartissent dans les tableaux de bord Risques, Usage et Système.

Lorsqu'une version « aujourd'hui » et « historique » du même graphique était présente dans les versions précédentes, il est désormais possible de configurer un seul graphique présentant les données d'« aujourd'hui » ou d'une période (configurable) plus longue. Vous pouvez également afficher 2 copies du graphique, l'une présentant les données du jour, l'autre les données d'une période plus longue.

Vous pouvez modifier les graphiques et les compteurs affichés dans chaque onglet.

Les nouveaux outils du tableau de bord Menaces vous permettent désormais de surveiller l'activité suspecte généralement associée à des attaques malveillantes avancées. Les graphiques et tableaux qui alimentent cet onglet n'existaient pas avant la version 7.7.

Mes listes d'acceptation

Les listes d'acceptation s'appellent désormais **Filtres d'accès limité**. Les filtres de catégories, d'accès limité et de protocoles sont tous gérés dans la page **Gestion des stratégies > Filtres**.

Pour afficher ou modifier le contenu d'un filtre d'accès limité, cliquez sur son nom dans la liste **Filtres d'accès limité**.

Mes URL personnalisées

Les URL personnalisées sont maintenant regroupées sous le titre **Composants de filtre**.

Pour afficher et modifier des **URL recatégorisées** (appelées auparavant URL personnalisées/recatégorisées), accédez à la page **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Modifier les catégories**. Sélectionnez une catégorie pour afficher ses URL recatégorisées.

Les **URL non filtrées** (auparavant URL personnalisées/non filtrées) ont été remplacées par des **exceptions** autorisées. Voir *Mes URL non filtrées*, page 59.

Mes URL non filtrées

La fonctionnalité auparavant assurée par les URL non filtrées est à présent assurée par les **exceptions autorisées**. Une exception vous permet d'autoriser ou de bloquer une ou plusieurs URL pour un ou plusieurs clients.

Lors de la mise à niveau, les URL non filtrées sont converties en exceptions autorisées à rôle unique. L'exception autorisée s'applique à tous les clients du rôle dans lequel l'URL non filtrée a été définie.

Pour créer et gérer les exceptions autorisées et bloquées, utilisez la page **Gestion des stratégies > Exceptions**.

Mes objets d'annuaire

Dans TRITON - Web Security, le titre général **Annuaire** remplace désormais Objets d'annuaire. Ce terme général regroupe les utilisateurs, les groupes, les domaines et les unités d'organisation définis dans un service d'annuaire pris en charge.

Pour afficher, ajouter ou modifier ces clients, ouvrez la page **Gestion des stratégies > Clients** et développez l'arborescence **Annuaire**.

Websense Explorer

Websense Explorer a été remplacé par les rapports d'investigation, directement accessibles dans TRITON - Web Security. Notez que, pour cela, Log Server doit être installé dans un ordinateur Windows. Cliquez sur **Génération de rapports > Rapports d'investigation** dans le panneau de navigation situé à gauche pour créer, planifier et exécuter des rapports comme vous le faisiez dans Websense Explorer.

Websense Reporter

Websense Reporter a été remplacé par les rapports de présentation, directement accessibles dans TRITON - Web Security. Notez que, pour cela, Log Server doit être installé dans un ordinateur Windows. Cliquez sur **Génération de rapports > Rapports de présentation** dans le panneau de navigation situé à gauche pour définir des filtres de rapports personnalisés, planifier des rapports et exécuter des rapports avec cet outil.

Utilitaire de configuration de Log Server

Les fonctionnalités et fonctions de l'utilitaire de configuration de Log Server sont désormais intégrées dans TRITON - Web Security.

Ouvrez la page **Paramètres > Génération de rapports > Log Server** pour gérer les informations de connexion à la base de données d'activité, les paramètres ODBC et BCP, la consolidation, les paramètres d'accès et de visite et les paramètres de connexion à User Service.

La configuration des paramètres WebCatcher s'effectue à présent dans la page **Paramètres > Général > Compte**.

Mes rapports

Un grand nombre de modèles de rapports prédéfinis étaient fournis avec Websense Reporter. La plupart des modèles fournissaient des informations très similaires, avec de légères variations de format ou de contenu prédéfini (utilisateurs, catégories, etc.).

Dans le cas des rapports de présentation, les modèles ont été rationalisés de sorte qu'un format et un contenu particuliers soient présentés sous la forme d'un seul rapport prédéfini. Vous pouvez copier un rapport prédéfini et modifier son filtre pour sélectionner une combinaison différente de clients, de catégories, de protocoles et d'actions (appelés auparavant dispositions).

Le tableau suivant présente la liste des rapports de l'application Reporter v6.3.x et le nom du rapport de présentation équivalent dans la version 7.

Rapport v6.3.x	Rapport v7
Détails des destinations par utilisateur	Détails de l'activité utilisateur (remplace également le rapport précédent Détails de l'activité utilisateur)
Catégories principales par accès Internet bloqué	Principales catégories bloquées par demandes (sans pourcentage)
Actions par occurrences	Principales actions de filtrage par requêtes
Catégories principales par temps de navigation sur Internet	Catégories principales par temps de navigation
Catégories principales par octets transférés	Catégories par bande passante
Catégories principales par accès	Principales catégories visitées
Groupes principaux par temps de navigation sur Internet	Groupes principaux par temps de navigation
Groupes principaux par octets transférés	Groupes principaux par bande passante
Groupes principaux par accès	Groupes principaux par demandes
Destinations principales par temps de navigation sur Internet	Sites principaux par temps de navigation (sans catégorie)
Destinations principales par octets transférés	Sites principaux par bande passante (sans catégorie)
Destinations principales par accès	Principaux sites visités (sans catégorie)
Utilisateurs principaux par temps de navigation sur Internet	Utilisateurs principaux par temps de navigation
Utilisateurs principaux par octets transférés	Utilisateurs principaux par bande passante
Utilisateurs principaux par accès	Activité principales des utilisateurs par demandes
Résumé des risques pour l'entreprise	(à ajouter)
Destinations principales par accès Internet bloqué	Principaux sites bloqués par demandes (sans pourcentage ni catégorie)
Détails de l'activité utilisateur	Détails de l'activité utilisateur (remplace également le rapport précédent Détails des destinations par utilisateur)
Groupes principaux par accès Internet bloqué	Principaux groupes bloqués par demandes (sans pourcentage)
Principaux protocoles par accès Internet bloqué	Principaux protocoles bloqués par demandes (sans pourcentage)
Protocoles par octets transférés	Principaux protocoles par bande passante
Résumé des destinations des utilisateurs	Résumé de l'activité des utilisateurs (remplace également le rapport précédent Résumé des destinations par date et utilisateur)

Rapport v6.3.x	Rapport v7
Utilisateurs principaux par accès Internet bloqué	Principaux utilisateurs bloqués par demandes
Résumé des destinations par date et utilisateur	Résumé de l'activité des utilisateurs (remplace également le rapport Résumé des destinations des utilisateurs)

Les rapports suivants, qui étaient disponibles dans Websense Reporter v6.3.x, peuvent être recréés en substance dans la vue résumée ou détaillée des rapports d'investigation. Les valeurs de coûts et de pourcentage ne sont cependant pas prises en charge dans la version 7.

- Détails des octets transférés par catégorie
- Détails des octets transférés par utilisateur
- Détails des octets transférés par groupe
- Détails des utilisateurs par catégorie
- Détails des groupes par catégorie
- Détails des destinations d'URL complètes par catégorie et date
- Détails des octets transférés par protocole
- Détails des octets transférés par date et protocole
- Détails des destinations par groupe
- Catégories par octets transférés
- Détails de l'activité des groupes (multiple)
- Détails des groupes par protocole
- Résumé des groupes par protocole
- Analyse des protocoles – Bande passante
- Analyse des protocoles – Accès
- Résumé des catégories par accès
- Résumé du temps de navigation sur Internet par catégorie
- Résumé du temps de navigation sur Internet par destination
- Résumé de la bande passante des groupes
- Résumé du temps de navigation sur Internet des groupes
- Résumé des destinations des groupes
- Résumé de la bande passante des utilisateurs
- Résumé du temps de navigation sur Internet des utilisateurs
- Résumé des destinations principales par accès
- Détails des utilisateurs par protocole
- Résumé des utilisateurs par protocole
- Résumé des octets transférés par catégorie
- Résumé des octets transférés par date et catégorie
- Résumé des octets transférés par utilisateur
- Résumé des octets transférés par date et utilisateur
- Résumé des octets transférés par groupe
- Résumé des octets transférés par date et groupe
- Résumé des catégories par date et utilisateur
- Résumé des catégories par date et groupe
- Résumé des destinations par groupe
- Résumé des destinations par date et groupe
- Résumé des destinations par heure du jour et groupe (niveau non résumé)
- Résumé des octets transférés par protocole
- Résumé des octets transférés par date et protocole
- Résumé des destinations principales par utilisateur
- Résumé des destinations principales par octets transférés et catégorie
- Résumé des destinations principales par octets transférés
- Résumé des destinations par utilisateur
- Résumé des destinations par heure du jour et utilisateur (niveau non résumé)
- Temps total de navigation sur Internet

Real-Time Analyzer

Websense Real-Time Analyzer a été remplacé par une combinaison d'autres outils :

- **Real-Time Monitor** présente les URL actuellement demandées dans votre réseau. Vous pouvez filtrer les résultats pour cibler un sous-ensemble de trafic spécifique ou interrompre la surveillance pour examiner les données existantes en profondeur. Voir *Présentation de Real-Time Monitor*, page 32.
- Les graphiques de la page **État > Tableau de bord** donnent un aperçu du volume filtré, résument l'activité du filtrage et présentent des statistiques sur les requêtes filtrées. Vous y trouverez également :
  - Les alertes de fonctionnement du filtrage liées aux problèmes de ressources système des principaux composants, aux problèmes de téléchargement de la base de données principale, aux défaillances des services, etc.
  - Des informations portant sur chaque instance de Filtering Service associée au serveur Policy Server actif, notamment sur l'état de la connexion de chaque service à Network Agent et Content Gateway

Mes paramètres de serveurs

Les options de configuration de Websense précédemment accessibles via le menu Serveur > Paramètres de Websense Manager sont à présent accessibles par un clic sur l'onglet **Paramètres** du panneau de navigation situé à gauche dans TRITON - Web Security.

Mes paramètres Network Agent locaux

Pour accéder aux paramètres Network Agent locaux, ouvrez l'onglet **Paramètres** dans le panneau de navigation de gauche, développez au besoin la section **Network Agent**, survolez **Global** avec votre souris, puis cliquez sur l'adresse IP de l'instance de Network Agent que vous souhaitez configurer. La page des paramètres locaux de l'instance de Network Agent sélectionnée s'affiche.

Gestion des comptes d'administrateur

Les comptes d'administrateur local (auparavant comptes d'utilisateur Websense) et les comptes d'administrateur réseau sont désormais gérés dans TRITON et non plus dans le module Web Security. Cliquez sur **Paramètres TRITON** dans la barre d'outils TRITON, puis sur **Administrateurs** dans le panneau de navigation gauche. Vous pouvez ensuite :

- Ajouter et supprimer des comptes d'administrateur
- Définir des mots de passe d'administrateur
- Définir les modules TRITON auxquels chaque administrateur peut accéder

Seuls les administrateurs disposant d'autorisations d'administrateur de sécurité globale peuvent créer et supprimer des comptes d'administrateur.

L'administrateur de sécurité globale détermine si un compte dispose ou non d'autorisations Super administrateur inconditionnel dans le module Web Security. Un Super administrateur du module Web Security doit ajouter des administrateurs délégués à un ou plusieurs rôles et définir leur niveau d'autorisations.

Un administrateur délégué autorisé à accéder à Web Security par l'administrateur de sécurité globale mais qui n'a encore été ajouté à aucun rôle peut voir certaines parties de la page État > Tableau de bord, mais ne peut pas accéder aux autres fonctionnalités de Web Security.

L'ancienne page Gérer les comptes d'administrateur de TRITON - Web Security s'appelle désormais **View Administrator Accounts (Afficher les comptes d'administrateur)** et répertorie les administrateurs autorisés à accéder à Web Security en indiquant les rôles auxquels ils ont éventuellement été affectés. Seuls les administrateurs répertoriés dans cette page (et le compte d'administrateur de sécurité globale par défaut, **admin**) peuvent être ajoutés à des rôles TRITON - Web Security.

Détecteur de trafic réseau (Outil de visibilité du trafic)

Le Détecteur de trafic réseau (auparavant Outils de visibilité du trafic) n'est plus inclus dans Network Agent. À la place, Websense, Inc., recommande d'utiliser un analyseur de paquets tiers, par exemple Wireshark, pour vérifier que chaque instance de Network Agent peut détecter le trafic provenant des adresses IP qu'elle doit surveiller.

Gestion des clés d'abonnement

La gestion des clés d'abonnement Policy Server a été étendue.

- Lorsqu'aucune clé d'abonnement n'a été saisie (par exemple, tout de suite après l'installation), un message contextuel vous invite à le faire.
- Si vous ne passez pas par ce message contextuel, vous pouvez saisir la clé du serveur Policy Server actif dans la page Paramètres > Général > Compte.
- Dans les environnements à plusieurs serveurs Policy Server, utilisez la page **Paramètres > Général > Policy Servers (Serveurs Policy Server)** pour gérer les clés de toutes vos instances de Policy Server.
  - Lorsque plusieurs instances de Policy Server partagent une même clé, désignez-en une en tant qu'instance principale et saisissez sa clé. Désignez les autres instances de Policy Server en tant qu'instances secondaires.

    Ces instances pourront alors hériter des paramètres de clé d'abonnement du serveur principal (ce qui simplifie la gestion des clés), sans que leur fonctionnement n'en soit affecté.

Si vous saisissez une nouvelle clé pour l'instance principale de Policy Server, les informations des clés de toutes les instances secondaires sont automatiquement mises à jour.

- Si chaque instance de Policy Server dispose de sa propre clé, désignez-les chacune en tant qu'instance principale. Les informations relatives à la clé et au niveau d'abonnement s'affichent séparément pour chaque instance principale de Policy Server.

8 Procédures

Bien que d'importantes modifications aient été apportées à l'interface de gestion, les procédures de base qui permettent d'effectuer la plupart des tâches de filtrage, de génération de rapports et de configuration ne diffèrent pas beaucoup de celles des versions précédentes.

Cette section vous permet de retrouver rapidement vos tâches habituelles dans la nouvelle interface de TRITON - Web Security.

- *Téléchargement de la base de données principale*, page 67
- *Ajout de clients*, page 68
- *Création d'une stratégie*, page 69
- *Attribution d'une stratégie aux clients*, page 69
- *Vérification de l'application de la stratégie appropriée*, page 70
- *Création d'un rapport de présentation*, page 70
- *Création d'un rapport d'investigation*, page 71
- *Création ou modification d'une catégorie personnalisée*, page 71
- *Recatégorisation d'une URL*, page 72
- *Autorisation d'une URL pour tous les clients*, page 72
- *Définition de mots-clés*, page 73
- *Utilisation des types de fichiers*, page 73
- *Création de comptes Websense pour les administrateurs*, page 73
- *Connexion des administrateurs à l'aide des comptes réseau*, page 74
- *Déplacement de clients d'un rôle à un autre*, page 75
- *Gestion des paramètres du journal d'audit*, page 76
- *Configuration du filtrage Web hybride*, page 76
- *Prévention des pertes de données sur Internet*, page 77

Téléchargement de la base de données principale

Le compte **admin** et les membres du rôle Super administrateur peuvent à tout moment déclencher manuellement le téléchargement de la base de données principale Websense via la page **État > Tableau de bord** dans TRITON - Web Security.

1. Dans la barre d'outils située en haut du panneau de contenu, cliquez sur **Téléchargement de la base de données**.

   La liste des instances de Filtering Service associées au serveur Policy Server actif s'affiche.
2. Cliquez sur le bouton **Mettre à jour** situé à droite d'une adresse IP de Filtering Service, ou cliquez sur **Tout mettre à jour** pour télécharger une mise à jour de la base de données principale dans tous les ordinateurs exécutant Filtering Service.
3. Cliquez sur l'adresse IP d'une instance de Filtering Service dans la liste de gauche pour afficher la progression du téléchargement ou sur **Fermer** pour revenir au tableau de bord.

Si vous êtes connecté à TRITON - Web Security avec des autorisations de stratégie lorsque la mise à jour de la base de données principale ajoute ou supprime des catégories ou des protocoles, vous devez vous déconnecter puis vous reconnecter pour que les modifications apportées aux catégories ou aux protocoles apparaissent dans TRITON - Web Security.

Configurez les téléchargements automatiques dans la page **Paramètres > Général > Téléchargement de la base de données**.

Ajout de clients

La page **Gestion des stratégies > Clients** permet d'ajouter des clients dans TRITON - Web Security.

1. Cliquez sur **Ajouter** (sous la liste Clients).
2. Identifiez les clients que vous souhaitez ajouter :
   - Si vous avez configuré Websense pour qu'il communique avec le service d'annuaire de votre réseau, parcourez l'arborescence **Annuaire** pour localiser les utilisateurs, les groupes ou les domaines (unités d'organisation) à ajouter en tant que clients.

     Si vous utilisez un service d'annuaire LDAP, vous pouvez également utiliser l'option **Rechercher** pour identifier des utilisateurs, des groupes ou des domaines (unités d'organisation).
   - Pour ajouter un seul ordinateur de votre réseau en tant que client, entrez son adresse IP ou son nom d'hôte sous **Ordinateur**.
   - Pour ajouter un groupe d'ordinateurs aux adresses IP contiguës en tant que clients, entrez l'adresse IP de départ et celle de fin sous **Réseau**.
3. Cliquez sur la flèche droite (>) appropriée pour ajouter les clients à la liste **Clients sélectionnés**.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Clients. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Création d'une stratégie

La page **Gestion des stratégies > Stratégies** permet d'ajouter des stratégies dans TRITON - Web Security.

1. Cliquez sur **Ajouter** sous la liste des stratégies.
2. Entrez un **Nom de stratégie** unique (50 caractères maximum) pour la nouvelle stratégie.
3. Entrez une **Description** (255 caractères maximum) de la stratégie. Cette description doit clairement désigner l'objectif de la stratégie pour simplifier la maintenance ultérieure.
4. 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.
5. Cliquez sur **OK** pour mettre vos modifications en cache et accéder à la page Modifier la stratégie.
6. Servez-vous de la page Modifier la stratégie pour modifier le planning et les filtres imposés par la stratégie.

   Pour obtenir des instructions détaillées, ouvrez la page **Aide > Expliquer cette page** depuis la page Modifier la stratégie.
7. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Stratégies. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Attribution d'une stratégie aux clients

Deux méthodes permettent d'attribuer des stratégies aux clients :

- Dans la page **Gestion des stratégies > Stratégies > Modifier la stratégie** de la stratégie à attribuer aux clients, cliquez sur **Appliquer aux clients** dans la barre d'outils située en haut de la page. Sélectionnez un ou plusieurs clients dans l'arborescence, puis cliquez sur **OK**.
- Dans la page **Gestion des stratégies > Clients**, sélectionnez un ou plusieurs clients dans l'arborescence, puis cliquez sur **Éditer**. Sous Stratégie, cliquez sur **Modifier**, puis sélectionnez une nouvelle stratégie dans la liste déroulante. Lorsque vous avez terminé, cliquez sur **OK**.

Lorsque l'attribution de stratégies aux clients est terminée, cliquez sur **Save and Deploy (Enregistrer et déployer)** dans le panneau de raccourcis à droite pour enregistrer et implémenter vos modifications.

Vérification de l'application de la stratégie appropriée

1. Cliquez sur **Vérifier la stratégie** dans le panneau de raccourcis à droite.
2. Identifiez le client pour lequel vous souhaitez vérifier la stratégie de filtrage :
   - Pour les utilisateurs, les groupes, les domaines et les unités d'organisation, entrez le nom unique complet (FQDN) de l'utilisateur, ou cliquez sur **Rechercher un utilisateur**.

     Si vous utilisez un service d'annuaire de type LDAP, un clic sur 'Rechercher un utilisateur' vous permet d'effectuer une recherche dans cet annuaire ou de le parcourir.
   - Dans le cas d'ordinateurs client, entrez une adresse IP.
3. Cliquez sur **Ok**.

Une fenêtre contextuelle s'affiche et présente la stratégie actuellement appliquée à ce client.

Création d'un rapport de présentation

Servez-vous de la page **Génération de rapports > Rapports de présentation** pour générer un rapport de présentation.

1. Développez les entrées du Catalogue de rapports et mettez le rapport à générer en surbrillance.
2. Cliquez sur **Exécuter**, puis sélectionnez les dates à inclure et le format de sortie.
3. Sous la section Génération des rapports, servez-vous de la case à cocher **Schedule the report to run in the background (Planifier l'exécution du rapport en arrière-plan)** pour définir le mode d'exécution du rapport :
   - Si cette case est cochée, le rapport est planifié pour une exécution immédiate et commence automatiquement en arrière-plan dès que vous cliquez sur **Exécuter**. Si vous fournissez une adresse électronique, le rapport est envoyé à un ou plusieurs destinataires lorsqu'il est terminé. Le rapport est également accessible via la page Génération des rapports > Rapports de présentation > Review Reports (Examiner les rapports).
   - Si cette case à cocher est désactivée, une nouvelle fenêtre de navigateur s'ouvre pour présenter la progression de la génération du rapport lorsque vous cliquez sur **Exécuter**. Dès que le rapport est prêt, soit il s'affiche dans la fenêtre du navigateur, soit le système vous invite à ouvrir ou enregistrer le fichier. Le rapport n'est pas stocké automatiquement et ne s'affiche pas dans la page Review Reports (Examiner les rapports).
4. Après avoir sélectionné le mode d'exécution du rapport, cliquez sur **Exécuter**.

Pour sélectionner une autre combinaison de données pour le même rapport :

1. Mettez un rapport prédéfini ou un rapport personnalisé existant en surbrillance, puis cliquez sur **Enregistrer sous**.

2. Entrez le nom d'affichage du rapport. Ce nom apparaîtra dans le Catalogue de rapports.
3. Cliquez sur **Enregistrer et modifier**.
4. Renseignez les onglets de la page **Modifier le filtre du rapport** pour sélectionner avec précision les utilisateurs, les catégories, les protocoles et les actions à inclure.
5. Choisissez d'enregistrer simplement la nouvelle définition de ce rapport en vue d'une utilisation future, d'enregistrer et d'exécuter le rapport immédiatement, ou d'enregistrer le rapport et d'en planifier l'exécution ultérieure ou périodique.

Pour planifier des rapports de présentation, cliquez sur **Planificateur** en haut de la page Rapports de présentation. Renseignez ensuite les onglets de la page **Planificateur** pour définir le travail.

Création d'un rapport d'investigation

La page **Génération de rapports > Rapports d'investigation** présente un graphique à barres illustrant les accès par classe de risques. Cette page étant pratiquement identique à la page principale de Websense Explorer des versions précédentes, servez-vous des techniques auxquelles vous êtes habitué pour générer un rapport.

- Cliquez sur le nom d'une classe de risques dans la colonne gauche, puis choisissez **Catégories**, par exemple, pour afficher des informations sur toutes les catégories associées à la classe de risques sélectionnée.
- Sélectionnez des éléments dans la barre grise située au-dessus du graphique pour créer un rapport multi-niveaux présentant par exemple les cinq principaux utilisateurs de chacune des 10 principales catégories.
- Cliquez sur une barre ou sur un numéro pour générer un rapport détaillé sur les données associées.
- Cliquez sur **Rapports favoris** pour enregistrer ce rapport en tant que Favori et accéder aux options de planification.
- Cliquez sur **Cas particuliers** pour identifier les utilisateurs dont l'utilisation d'Internet est statistiquement différente de celle des autres dans l'organisation.

Création ou modification d'une catégorie personnalisée

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories** permet de créer et de modifier des catégories personnalisées.

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 personnalisés (URL, 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 ajouter une nouvelle catégorie, cliquez sur **Ajouter**.

  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, cliquez sur **Renommer**.
- Pour modifier l'action de filtrage (Autoriser, Bloquer) associée à une catégorie dans tous les filtres de catégories, cliquez sur **Remplacer l'action**.

Recatégorisation d'une URL

1. Procédez de l'une des manières suivantes :
   - Cliquez sur **Recatégoriser une URL** dans le panneau de raccourcis à droite.
   - Sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Modifier les catégories**.
2. Sélectionnez une catégorie dans la liste. Les informations relatives à cette catégorie, y compris la liste des URL recatégorisées et les mots clés qui lui sont associés, s'affichent dans la partie droite de l'arborescence des catégories.
3. Cliquez sur **Ajouter des URL** dans la section URL recatégorisées.
4. Entrez les URL ou les adresses IP que vous souhaitez associer à la catégorie sélectionnée, une par ligne.
5. Cliquez sur **OK** pour revenir à la page Modifier les catégories, puis de nouveau sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Autorisation d'une URL pour tous les clients

Pour autoriser une URL pour tous les clients, les Super administrateurs peuvent procéder comme suit :

1. Cliquez sur **Create Exception (Créer une exception)** dans le panneau de raccourcis de droite.
2. Entrez le **Nom** unique de l'exception.
3. Entrez l'**URL** à autoriser.
4. Par défaut, l'exception est définie pour s'appliquer à tous les clients (l'option **Global** est activée).
5. Par défaut, l'exception est définie sur **Bloquer l'URL**. Pour modifier ce paramètre, définissez le **Type** sur **Autoriser**.
6. Définissez au besoin une date d'expiration.
7. Cliquez sur **OK**, puis sur **Save and Deploy (Enregistrer et déployer)**.

Définition de mots-clés

1. Sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Modifier les catégories**.
2. Sélectionnez une catégorie dans l'arborescence. La partie droite de l'écran présente alors les URL recatégorisées et les mots-clés actuellement associés à cette catégorie.
3. Sous Mots-clés, cliquez sur **Ajouter des mots-clés**.
4. Entrez un mot-clé par ligne. Cliquez sur **Tester** pour vérifier que le mot-clé correspond aux chaînes prévues.
5. Lorsque l'ajout des mots-clés est terminé, cliquez sur **OK** pour revenir à la page Modifier les catégories.
6. Cliquez de nouveau sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Pour bloquer des sites en fonction des mots-clés, vous devez également :

- Vérifier que le blocage par mot-clé est activé globalement. Ouvrez la page **Paramètres > Filtrage**, puis activez l'option **Options de recherche de mots-clés** sous Filtrage général.
- Activer le blocage par mots-clés pour cette catégorie dans un filtre de catégories actif.

Utilisation des types de fichiers

1. Sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Types de fichiers**.
2. Sélectionnez un type de fichiers dans la liste pour afficher les extensions associées à ce type, ou cliquez sur **Ajouter un type de fichiers** pour définir un nouveau type de fichiers.

   Pour ajouter des extensions à un type de fichiers existant, cliquez sur **Ajouter des extensions**.

Pour bloquer des sites en fonction de leur type de fichiers, activez le blocage de types de fichiers pour des catégories individuelles d'un filtre de catégories actif.

Création de comptes Websense pour les administrateurs

Vous pouvez définir des comptes locaux utilisés uniquement pour la connexion à TRITON Unified Security Center. Les administrateurs peuvent utiliser ces comptes pour accéder à TRITON - Web Security, plutôt que leur compte d'annuaire réseau.

Les comptes locaux se révèlent particulièrement utiles dans les environnements distribués, dans lesquels les administrateurs délégués peuvent s'authentifier dans différents services d'annuaire. Pour plus d'informations, consultez la section *Connexion des administrateurs à l'aide des comptes réseau*, page 74.

Pour créer des comptes locaux :

1. Sélectionnez **Paramètres TRITON > Administrateurs**.
2. Cliquez sur **Add Local Account (Ajouter un compte local)**.
3. Saisissez le **Nom d'utilisateur**, une **Adresse électronique** de contact et le **Mot de passe** du nouveau compte.

   L'adresse électronique est utilisée par le processus automatique de récupération du mot de passe.
4. Les cases à cocher situées sous le champ de confirmation du mot de passe vous permettent d'activer ou non les options **Notify administrator of the new account via email (Signaler le nouveau compte à l'administrateur par e-mail)**, via l'adresse fournie à l'étape précédente, et **Force administrator to create a new password at logon (Obliger l'administrateur à créer un nouveau mot de passe lors de la connexion)**.
5. Pour que le comte puisse accéder à un ou plusieurs modules TRITON, affectez-lui des autorisations.
   - L'option **Global Security Administrators (Administrateurs de la sécurité globale)** permet aux administrateurs d'accéder de façon non limitée à l'ensemble des modules TRITON, y compris aux Paramètres TRITON.
   - L'option **Personnaliser** vous permet d'attribuer des privilèges d'**accès** ou d'**accès et de modification**.
     - Le privilège **Accès** permet à l'administrateur de se connecter et d'afficher un sous-ensemble de la page État > Tableau de bord jusqu'à ce que le compte soit affecté à un rôle d'administrateur délégué ou de Super administrateur conditionnel.
     - Le privilège **Accès et modification** accorde des autorisations de Super administrateur inconditionnel au compte dans le module Web Security.
6. Cliquez sur **OK** pour enregistrer vos modifications.

Les nouveaux comptes créés avec des autorisations Web Security sont ajoutés dans la page **Gestion des stratégies > Administration déléguée > View Administrator Accounts (Afficher les comptes d'administrateur** de TRITON - Web Security.

Après avoir ajouté un compte associé uniquement à des privilèges d'accès, ajoutez cet utilisateur à un ou plusieurs rôles d'administration déléguée via la page **Gestion des stratégies > Administration déléguée**.

Connexion des administrateurs à l'aide des comptes réseau

Si les administrateurs accèdent à TRITON - Web Security avec leurs identifiants de connexion réseau, vous devez configurer le service d'annuaire à utiliser pour l'authentification.

Ce service d'annuaire doit correspondre à celui que tous les administrateurs utilisent pour s'authentifier ou il doit disposer d'une relation approuvée avec leurs services d'annuaire.

Configurez le service d'annuaire dans les Paramètres TRITON :

1. Sélectionnez **Paramètres TRITON > User Directory (Annuaire des utilisateurs)**.
2. Configurez la connexion au service d'annuaire pris en charge qui doit servir pour authentifier les administrateurs.
3. Cliquez sur **OK** pour enregistrer vos modifications.

Déplacement de clients d'un rôle à un autre

Le déplacement d'un client d'un rôle d'administration déléguée vers un autre rôle requiert des autorisations de Super administrateur inconditionnel. Commencez par supprimer le client du rôle actuel. Ajoutez-le ensuite au nouveau rôle.

Certains clients ne peuvent pas être supprimés directement de la liste des clients gérés (Administration déléguée > Modifier le rôle). Cela se produit lorsque l'administrateur a appliqué une stratégie au client dans la page Clients. Cela arrive également lorsque l'administrateur a appliqué une stratégie à un ou plusieurs membres du réseau, groupe, domaine ou unité d'organisation à déplacer.

Dans ce cas, le Super administrateur inconditionnel doit procéder comme suit :

1. Ouvrez la liste **Rôle** dans la barre d'outils et sélectionnez le rôle duquel les clients gérés doivent être supprimés.
2. Ouvrez la page **Gestion des stratégies > Clients** pour voir la liste de tous les clients auxquels l'administrateur délégué a attribué une stratégie de façon spécifique.

   Cela peut comprendre les clients spécifiquement identifiés dans la liste des clients gérés de ce rôle et les clients membres de réseaux, de groupes, de domaines ou d'unités d'organisation présents dans la liste des clients gérés.
3. Dans la page Clients, supprimez tous les clients devant être retirés de ce rôle, et les membres individuels des réseaux, groupes, domaines ou unités d'organisation à retirer du rôle.
4. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.
5. Ouvrez la liste **Rôle** dans la barre d'outils et sélectionnez le rôle **Super administrateur**.
6. Ouvrez la liste **Gestion des stratégies > Administration déléguée**, puis cliquez sur le nom du rôle dont les clients gérés doivent être supprimés. La page **Modifier le rôle** apparaît.
7. Supprimez les clients appropriés dans la liste des clients gérés.
8. Cliquez sur **OK** pour mettre vos modifications en cache.
9. Dans la page Administration déléguée, modifiez le nouveau rôle de ces clients et ajoutez-les en tant que clients gérés.
10. Cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Les administrateurs délégués peuvent à présent déplacer les nouveaux clients gérés vers leur page Clients et leur affecter des stratégies.

Les clients sont gérés par la stratégie par défaut du rôle jusqu'à ce qu'une autre stratégie leur soit affectée.

Gestion des paramètres du journal d'audit

En cliquant sur **État > Journal d'audit**, les Super administrateurs peuvent consulter un journal d'audit qui identifie les administrateurs ayant accédé à TRITON - Web Security et les modifications qu'ils y ont apportées.

Lorsque la page 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 autres enregistrements.

Les enregistrements d'audit sont conservés pendant 60 jours, puis supprimés du journal. Contrairement aux versions précédentes, vous ne pouvez pas configurer de limites de taille ou de temps pour les enregistrements d'audit.

Pour conserver les enregistrements plus longtemps, servez-vous de l'option d'exportation. (Le processus d'exportation ne retire pas les enregistrements du journal d'audit.)

Configuration du filtrage Web hybride

Dans les déploiements Websense Web Security Gateway Anywhere, vous devez d'abord activer le filtrage hybride pour que le service hybride puisse assurer le filtrage des membres de votre organisation. Dès que votre compte est actif, vous pouvez configurer les personnes filtrées par le service hybride, spécifier les sites à ne pas filtrer et définir la fréquence d'envoi des données utilisateur au service hybride.

La procédure générale est la suivante :

1. Ouvrez la page **Paramètres > Compte** et saisissez une **Adresse électronique de contact** pour activer votre compte de filtrage hybride.
2. Servez-vous de la page **Paramètres > Hybrid Configuration (Configuration hybride) > Filtered Locations (Emplacements filtrés)** pour définir les domaines, les adresses IP et les sous-réseaux que le service hybride doit filtrer. Il s'agit là des adresses IP des succursales que vous souhaitez protéger.
3. Servez-vous de la page **Unfiltered Destinations (Destinations non filtrées)** pour définir les domaines, les adresses IP et les sous-réseaux que le service hybride ne doit éventuellement **pas** filtrer. Cela peut inclure les sites intranet que le service hybride ne voit pas et les sites externes (par exemple le site de messagerie Web de votre organisation) auxquels vos utilisateurs doivent pouvoir accéder, y compris lorsque le filtrage hybride n'est pas disponible.
4. Servez-vous de la page **User Access (Accès des utilisateurs)** pour définir le mode d'identification et d'authentification des utilisateurs et le fuseau horaire à employer pour l'application des stratégies, et pour indiquer si les requêtes sont autorisées ou bloquées lorsque le service hybride ne peut pas imposer les stratégies définies.

5. Servez-vous de la page **Shared User Data (Données utilisateur partagées)** afin de configurer Websense Directory Agent pour qu'il collecte les données des utilisateurs et des groupes pour le service hybride.
6. Servez-vous de la page **Planification** pour définir la fréquence d'envoi des données de l'annuaire au service hybride et la fréquence à laquelle les données des rapports du service hybride doivent être récupérées.

La procédure de configuration complète est disponible dans la rubrique d'aide « Configuration du filtrage hybride » de TRITON - Web Security.

Prévention des pertes de données sur Internet

L'ensemble des instructions relatives à l'installation et à la configuration de la prévention des pertes de données sur Internet est disponible dans le Centre Installation et déploiement.

La procédure générale comprend les étapes suivantes :

1. Installez les modules Content Gateway, Websense Web Security et Websense Data Security de votre produit Websense Web Security Gateway Anywhere.
2. Enregistrez le moteur de stratégies de Content Gateway Manager auprès du serveur de gestion Data Security Management Server.
3. Configurez l'agent Content Gateway dans le serveur Data Security Management Server.
4. Connectez-vous à TRITON - Data Security et exécutez l'Assistant de stratégie initial.
5. Toujours dans TRITON - Data Security, activez la liaison pour que Websense Data Security puisse accéder aux noms d'utilisateur et aux catégories de la base de données principale fournis par Websense Web Security.

Pour obtenir des instructions sur la liaison des logiciels Websense Data et Web Security et sur la création de stratégies personnalisées, reportez-vous à l'Aide de TRITON - Data Security.