Aide de TRITON - Web Security

Solutions Websense® Web Security

v7.7

10240 Sorrento Valley Rd., San Diego, CA 92121, États-Unis

Publié en 2012
Imprimé aux États-Unis et en Irlande

Marques déposées

Contenu

Rubrique 1 **Mise en route 17**

Présentation 17
Utilisation de TRITON - Web Security 18
Vérification, enregistrement et annulation des modifications. 23
Votre abonnement 24
Gestion de votre compte via le portail MyWebsense 24
Configuration des informations de votre compte 24
Base de données principale Websense 27
Configuration des téléchargements de la base de données 28
Qu'est-ce que WebCatcher ? 30
Support technique de Websense 31

Rubrique 2 **Tableau de bord de Web Security 33**

Tableau de bord Threats (Menaces) 35
Examen des détails des événements suspects 37
Affectation d'un niveau de gravité à une activité suspecte 39
Examen des détails des incidents suspects 39
Examen des données d'analyse liées aux menaces 41
Tableau de bord Risques 41
Tableau de bord Usage 42
Tableau de bord Système 43
Ajout d'éléments dans un onglet du tableau de bord 44
Économies de temps et de bande passante 45
Mode Status Monitor (Moniteur d'état) de Web Security 46

Rubrique 3 **Filtres de l'utilisation Internet 49**

Filtrage des catégories et des protocoles 50
Nouvelles catégories et nouveaux protocoles de la Base de données principale 52
Catégories spéciales 52
Classes de risque 54
Groupes de protocoles de sécurité. 57
Actions de filtrage 57
Utilisation de temps contingenté pour limiter l'accès à Internet. 58
Filtrage de la recherche 59
Fonctionnement des filtres 59

Création d'un filtre de catégories 60
Modification d'un filtre de catégories 61
Création d'un filtre de protocoles 63
Modification d'un filtre de protocoles 64
Filtres de catégories et de protocoles définis par Websense 65
Modèles de filtres de catégories et de protocoles 66
Configuration des paramètres de filtrage de Websense 67

Rubrique 4 **Clients 71**

Fonctionnement des clients 72
Fonctionnement avec des ordinateurs et des réseaux 73
Fonctionnement avec des utilisateurs et des groupes 74
Services d'annuaire 75
Windows Active Directory (en mode mixte) 76
Windows Active Directory (en mode natif) 76
Novell eDirectory et Oracle (Sun Java) Directory Server 78
Paramètres avancés de l'annuaire 78
Fonctionnement des groupes LDAP personnalisés 80
Ajout ou modification d'un groupe LDAP personnalisé 81
Ajout d'un client 81
Recherche dans le service d'annuaire 82
Modifications des paramètres des clients 83
Accès par mot de passe 84
Remplacement de compte 84
Déplacements de clients vers des rôles 86
Fonctionnement des clients du filtrage hybride 86

Rubrique 5 **Stratégies de filtrage Internet 89**

La stratégie Par défaut 90
Fonctionnement des stratégies 91
Création d'une stratégie 92
Modification d'une stratégie 93
Attribution d'une stratégie aux clients 95
Ordre du filtrage 95
Priorités des stratégies de groupe et de domaine 97
Filtrage d'un site 98

Rubrique 6 **Exceptions aux stratégies de filtrage 103**

Gestion des exceptions de filtrage 103
Organisation des exceptions 105
Ajout ou modification d'une exception de filtrage 106
Contournement d'une exception de filtrage 108
Lorsque plusieurs exceptions s'appliquent, laquelle est prioritaire ? 109
Modification simultanée de plusieurs exceptions de filtrage 109

Raccourcis des exceptions 110
Comment bloquer ou autoriser une URL pour tous ? 111
Comment bloquer ou autoriser une URL pour une seule personne ? 111
Comment bloquer ou autoriser une URL pour l'ensemble de mon rôle d'administration déléguée ? 112
Comment bloquer ou autoriser une URL pour l'un de mes clients gérés ? . 112
Comment créer une URL non filtrée ? 113

Rubrique 7 **Pages de blocage 115**

Blocage des publicités graphiques 117
Blocage des pages intégrées 117
Messages de blocage de protocoles 118
Fonctionnement des pages de blocage 119
Personnalisation du message de blocage 121
Modification de la taille du cadre du message 122
Modification du logo affiché sur la plage de blocage 123
Utilisation des variables du contenu de la page de blocage 123
Réinitialisation des pages de blocage par défaut 125
Création de messages de blocage alternatifs 125
Utilisation d'une page de blocage alternative dans un autre ordinateur 126
Identification de la cause du blocage d'une requête 127
Requête bloquée par Filtering Service 127
Requête bloquée par le filtrage hybride 128

Rubrique 8 **Exploitation des rapports pour évaluer l'efficacité du filtrage 129**

Qu'est-ce que le temps de navigation sur Internet ? 130
Rapports de présentation 131
Création d'un nouveau rapport de présentation 133
Définition du filtre du rapport 135
Sélection des clients pour un rapport 136
Sélection des catégories pour un rapport 137
Sélection des protocoles pour un rapport 138
Sélection des actions pour un rapport 138
Définition des options du rapport 139
Personnalisation du logo des rapports 140
Confirmation de la définition du filtre de rapport 140
Fonctionnement des favoris 141
Exécution d'un rapport de présentation 142
Planification des rapports de présentation 143
Définition du planning 145
Sélection des rapports à planifier 147
Définition de la plage de dates 147
Sélection des options de sortie 148
Affichage de la liste des tâches planifiées 149
Affichage de l'historique d'une tâche 150
Examen des rapports de présentation planifiés 151

Rapports d'investigation 152
Rapports récapitulatifs 154
Anonymat des rapports d'investigation 157
Option Anonyme 158
Rapports récapitulatifs multi-niveaux 158
Rapports détaillés flexibles 159
Colonnes des rapports détaillés flexibles 161
Rapports Détails de l'activité utilisateur 163
Détail de l'activité utilisateur par jour 164
Activité utilisateur par mois 165
Correspondance des catégories 166
Rapports standard 168
Rapports d'investigation favoris 169
Enregistrement d'un rapport en tant que Favori 170
Création ou suppression d'un rapport Favori 170
Modification d'un rapport favori 171
Planification des rapports d'investigation 172
Gestion des tâches planifiées de rapports d'investigation 174
Rapports Cas particuliers 175
Sortie dans un fichier 176
Impression des rapports d'investigation 176
Rapports sur activité propre 177
Real-Time Monitor 178
Real-Time Monitor dans les déploiements à plusieurs serveurs Policy Server . 180

Rubrique 9 **Options d'analyse et contournement du décryptage SSL 181**

Options d'analyse 183
Catégorisation du contenu 184
Détection des protocoles mis en tunnel 186
Risques de sécurité : Sécurité du contenu 187
Risques de sécurité : Analyse des fichiers 188
Sécurité sortante 190
Options avancées 191
Exceptions d'analyse 193
Fichiers de données utilisés avec l'analyse 195
Génération de rapports sur l'activité d'analyse 196
Journalisation de l'analyse 197
Contournement du décryptage SSL 198

Rubrique 10 **Configuration du filtrage hybride 203**

Activation de votre compte de filtrage hybride 204
Définition des emplacements filtrés 205
Ajout d'emplacements filtrés 206
Modification des emplacements filtrés 208

Gestion des proxy explicites 209
Ajout d'un proxy explicite 210
Modification d'un proxy explicite 210
Configuration du basculement vers le service hybride 211
Définition des sites non filtrés par le service hybride 211
Ajout de destinations non filtrées 212
Modification des destinations non filtrées 213
Configuration de l'accès des utilisateurs au filtrage hybride 214
Ajout de domaines. 216
Modification des domaines 216
Personnalisation des pages de blocage du service hybride 217
Activation des pages de notification HTTPS 218
Qu'est-ce qu'un fichier PAC ? 219
Envoi de données d'utilisateur et de groupe au service hybride 220
Configuration des paramètres de Directory Agent pour le filtrage hybride . 221
Configuration du mode de collecte des données pour le filtrage hybride 222
Oracle (Sun Java) Directory Server et filtrage hybride. 223
Novell eDirectory et filtrage hybride 224
Ajout et modification de contextes d'annuaire 224
Optimisation des résultats des recherches. 226
Planification de la communication avec le filtrage hybride 227
Définition de paramètres d'authentification personnalisés 229
Ajout de règles d'authentification personnalisées. 230
Modification des règles d'authentification personnalisées 231
Surveillance de la communication avec le service hybride 233
Affichage des rapports d'authentification du service hybride 234
Affichage du rapport Volume par agent utilisateur. 235

Rubrique 11 **Filtrage des utilisateurs hors site. 237**

Fonctionnement du logiciel Remote Filtering 238
Lorsque la communication du serveur échoue 239
Configuration des paramètres de Remote Filtering. 240
Configuration du filtrage à distance pour ignorer le trafic FTP ou HTTPS . 241
Configuration de l'intervalle des pulsations du client Remote Filtering . 242
Filtrage hybride des utilisateurs hors site 242
Configuration du filtrage hybride pour les utilisateurs hors site. 243
Auto-enregistrement des utilisateurs hors site 243

Rubrique 12 **Protection des informations vitales. 245**

Rubrique 13 **Réglage des stratégies de filtrage 247**

Limitation des utilisateurs à une liste définie d'URL. 247
Filtres d'accès limité et priorités du filtrage 248

Création d'un filtre d'accès limité 249
Modification d'un filtre d'accès limité 250
Ajout de sites depuis la page Modifier la stratégie 251
Copie de filtres et de stratégies vers des rôles 252
Construction de composants de filtres 253
Fonctionnement des catégories. 254
Modification des catégories et de leurs attributs. 254
Vérification de tous les attributs des catégories personnalisées 255
Modification du filtrage global des catégories. 256
Modification du nom d'une catégorie personnalisée 256
Création d'une catégorie personnalisée. 257
Filtrage par mots-clés 258
Définition des mots-clés 259
Redéfinition du filtrage pour des sites spécifiques 260
Définition de la priorité de la catégorisation Risques de sécurité 262
Blocage des publications destinées à des sites de certaines catégories 263
Fonctionnement des protocoles 264
Filtrage des protocoles 265
Modification des protocoles personnalisés 266
Ajout ou modification d'identificateurs de protocole 266
Modification du nom d'un protocole personnalisé 267
Modification du filtrage global des protocoles 267
Création d'un protocole personnalisé 268
Ajout à un protocole défini par Websense 270
Exploitation de Bandwidth Optimizer pour gérer la bande passante 270
Configuration des limites par défaut de Bandwidth Optimizer. 272
Gestion du trafic en fonction du type de fichiers 273
Filtrage basé sur l'extension des fichiers 274
Filtrage basé sur l'analyse des fichiers 277
Activation du blocage des types de fichier dans un filtre de catégorie 278
Fonctionnement des définitions des types de fichiers. 279
Ajout de types de fichiers personnalisés 280
Ajout d'extensions à un type de fichiers 280
Utilisation d'expressions régulières 281
Utilisation de la boîte à outils pour vérifier le comportement du filtrage 282
Catégorie d'URL 282
Vérifier la stratégie 282
Tester le filtrage 283
Accès à l'URL. 283
Analyser l'utilisateur 283
Identification d'un utilisateur pour vérifier la stratégie ou tester le filtrage . 284

Rubrique 14 **Identification des utilisateurs 285**

Identification transparente 285
Identification transparente des utilisateurs distants. 286
Authentification manuelle 287
Configuration des méthodes d'identification des utilisateurs 287
Définition de règles d'authentification pour des ordinateurs spécifiques . . . 289
Définition d'exceptions dans les paramètres d'identification des utilisateurs 290
Vérification des exceptions aux paramètres d'identification des utilisateurs 291
Authentification manuelle sécurisée 292
Création de clés et de certificats 293
Activation de l'authentification manuelle sécurisée 294
Acceptation du certificat dans le navigateur client 294
DC Agent 295
Configuration de DC Agent 296
Vérification des domaines et contrôleurs de domaine interrogés par DC Agent 299
Fichier dc_config.txt 299
Logon Agent. 300
Configuration de Logon Agent 301
RADIUS Agent 303
Configuration de RADIUS Agent. 303
eDirectory Agent 304
Configuration d'eDirectory Agent 305
Ajout d'une réplique de serveur eDirectory. 306
Configuration d'eDirectory Agent pour l'utilisation de LDAP. 307
Activation des requêtes complètes du serveur eDirectory. 308
Configuration d'un agent pour ignorer certains noms d'utilisateur 309
Identification des utilisateurs du filtrage hybride. 311
Priorité et dérogation d'authentification 313
Présentation du déploiement de Web Endpoint 314
Déploiement manuel de Web Endpoint pour Windows 316
Déploiement de Websense Authentication Service 317
Websense Directory Agent 319
Directory Agent et User Service 319
Lorsque les utilisateurs ne sont pas identifiés. 321

Rubrique 15 **Administration déléguée et génération de rapports 323**

Principes fondamentaux de l'administration déléguée. 323
Rôles d'administration déléguée. 324
Administrateurs délégués 325
Autorisations d'administration déléguée et de génération de rapports. 326

Administrateurs attribués à plusieurs rôles 329
Accès de plusieurs administrateurs à TRITON - Web Security 329
Préparation de l'administration déléguée 330
Création d'un verrouillage du filtre 332
Verrouillage de catégories 332
Verrouillage de protocoles 333
Préparation des administrateurs délégués 334
Gestion des rôles d'administration déléguée 335
Ajout de rôles 336
Modification des rôles 337
Ajout d'administrateurs 340
Ajout de clients gérés 342
Gestion des conflits entre rôles 343
Mise à jour des rôles d'administration déléguée 344
Suppression de rôles 345
Suppression de clients gérés 345
Gestion des clients des Super administrateurs 346
Exécution des tâches d'administration déléguée 346
Affichage de votre compte d'utilisateur 347
Affichage de la définition de votre rôle 348
Ajout de clients dans la page Clients 348
Création de stratégies et de filtres 349
Application de stratégies à des clients 350
Génération de rapports 351
Vérification des comptes d'administrateur 351
Activation des comptes réseau 351

Rubrique 16 **Administration du serveur Web Security 353**

Composants du produit Websense Web Security 354
Composants du filtrage et de la gestion 354
Composants de la génération de rapports 357
Composants de l'identification des utilisateurs 358
Composants d'interopérabilité 359
Fonctionnement de la Base de données des stratégies 360
Fonctionnement de Policy Server 360
Vérification des connexions à Policy Server 361
Ajout ou modification des instances de Policy Server 362
Fonctionnement d'un environnement à plusieurs serveurs Policy Server . . 363
Modification de l'adresse IP de Policy Server 363
Fonctionnement de Filtering Service 365
Vérification des détails du service Filtering Service 366
Vérification de l'état du téléchargement de la base de données principale . 366
Reprise des téléchargements de la base de données principale 367
Prise en charge de YouTube for Schools par Filtering Service 367

Policy Server, Filtering Service et State Server 368
Intégration à une solution SIEM tierce. 371
Fonctionnement de Content Gateway 372
Gestion des connexions à Content Gateway 372
Affichage et exportation du journal d'audit 373
Arrêt et démarrage des services Websense 375
Répertoires d'installation de Websense Web Security. 377
Alertes. 377
Contrôle des flux 378
Configuration des options d'alerte générales 378
Configuration des alertes système. 380
Configuration des alertes d'utilisation de catégories 381
Ajout d'alertes d'utilisation de catégories 382
Configuration des alertes d'utilisation de protocole 382
Ajout d'alertes d'utilisation de protocole 383
Configuration des alertes d'activité suspecte 384
Vérification de l'état actuel du système 385
Sauvegarde et restauration de vos données Websense 386
Planification des sauvegardes 388
Exécution de sauvegardes immédiates 390
Maintenance des fichiers de sauvegarde 391
Restauration de vos données Websense 391
Interruption des sauvegardes planifiées 393
Références des commandes. 393

Rubrique 17 **Administration de la génération de rapports. 395**

Attribution de catégories aux classes de risque 396
Configuration des préférences de génération de rapports 397
Configuration du mode de journalisation des requêtes filtrées 398
Configuration de Log Server 400
Test de la connexion à la base de données d'activité 405
Présentation de la base de données d'activité. 406
Tâches de la base de données 407
Paramètres d'administration de la base de données d'activité 408
Configuration des options de partition de la base de données 409
Configuration des options de maintenance de la base de données d'activité 412
Configuration de la journalisation des URL 413
Configuration des options du temps de navigation sur Internet 414
Configuration de la conservation des données de tendance 416
Conseils sur le dimensionnement de la base de données d'activité 417
Configuration des rapports du tableau de bord. 418
Configuration des rapports d'investigation 421

Connexion à la base de données et paramètres par défaut des rapports 421
Options d'affichage et de sortie 423
Rapports sur activité propre 425

Rubrique 18 **Configuration du réseau 427**

Configuration de Network Agent 428
Configuration des paramètres globaux 428
Configuration des paramètres locaux 430
Configuration des paramètres des cartes réseau 431
Configuration des paramètres de surveillance d'une carte réseau 433
Ajout ou modification des adresses IP 434
Vérification de la configuration de Network Agent 435

Rubrique 19 **Dépannage 437**

Problèmes d'installation et d'abonnement 437
Il existe un problème d'abonnement. 438
Impossible de vérifier la clé d'abonnement 438
Après la mise à niveau, absence de certains utilisateurs dans TRITON - Web Security 439
Problèmes de la base de données principale. 439
Utilisation de la base de données pour le filtrage initial 439
Base de données principale âgée de plus d'une semaine 440
Échec du téléchargement de la base de données principale 440
Clé d'abonnement 441
Accès Internet 441
Vérification des paramètres du pare-feu ou du serveur proxy 442
Espace disque insuffisant dans l'ordinateur Filtering Service 443
Mémoire insuffisante dans l'ordinateur Filtering Service 444
Applications restrictives. 444
Échec du téléchargement de la base de données principale à l'heure définie . . . 445
Contact du support technique pour les problèmes de téléchargement de la base de données 445
Problèmes de filtrage 445
Dysfonctionnement de Filtering Service. 446
User Service non disponible 446
Utilisation intensive du processeur dans l'ordinateur Filtering Service 447
Classement incorrect des sites dans la catégorie Technologies de l'information 448
Mots-clés non bloqués. 448
Problème de filtrage des URL de filtre d'accès limité ou personnalisé 449
Requêtes FTP non bloquées comme prévu 449
Non application des stratégies de groupe ou d'utilisateur. 449
Utilisateurs distants non filtrés par la stratégie appropriée 449
Problèmes liés à Network Agent 450

Network Agent non installé. 450
Non exécution de Network Agent. 450
Network Agent ne surveille aucune carte réseau 451
Network Agent ne peut pas communiquer avec Filtering Service 451
Mise à jour des informations d'ID unique ou de l'adresse IP de Filtering Service 451
Mémoire insuffisante dans l'ordinateur Network Agent. 452
Utilisation intensive du processeur dans l'ordinateur Network Agent 452
Problèmes de configuration et d'identification des utilisateurs 453
Non application des stratégies basées sur les utilisateurs et les groupes . . . 453
Défaut de communication de Filtering Service avec un agent d'identification transparente 454
Autorisations insuffisantes de DC Agent 455
Défaut d'accès de DC Agent au fichier requis 456
Page des domaines et des contrôleurs de DC Agent vide 457
Impossible d'ajouter des utilisateurs et des groupes dans TRITON - Web Security 457
Connectivité et configuration du service d'annuaire 458
Configuration du service d'annuaire dans TRITON - Web Security . . . 458
Identification des utilisateurs et Windows Server 2008 459
Activation du service Explorateur d'ordinateur. 459
Modification des autorisations de DC Agent, Logon Agent et User Service . . 460
User Service sous Linux 461
Utilisateurs distants non invités à s'authentifier manuellement 462
Filtrage incorrect des utilisateurs distants 462
Problèmes de messages de blocage 463
Aucune page de blocage affichée pour un type de fichier bloqué 463
Erreur du navigateur à la place de la page de blocage 463
Affichage d'une page blanche à la place de la page de blocage 464
Défaut d'affichage des messages de blocage de protocoles 464
Affichage d'un message de blocage de protocole à la place de la page de blocage 465
Problèmes liés aux journaux, aux messages d'état et aux alertes. 465
Où puis-je trouver les messages d'erreur liés aux composants de Websense ? . 466
Alertes d'état de Websense 466
Génération de deux enregistrements de journal pour une seule requête 468
Usage Monitor indisponible 469
Non exécution d'Usage Monitor. 469
Problèmes liés à Policy Server et à la base de données des stratégies 469
Oubli du mot de passe 470
Non démarrage du service Websense Policy Database. 470
Arrêt inopiné de Policy Server 471

Problèmes d'administration déléguée. 471
Les clients gérés ne peuvent pas être supprimés de leur rôle. 471
Erreur de connexion indiquant que quelqu'un d'autre est connecté à mon ordinateur 472
Sites recatégorisés non filtrés par la catégorie appropriée 472
Impossible de créer un protocole personnalisé 472
Problème de Log Server et de la base de données d'activité 472
Non exécution de Log Server 473
Non réception par Log Server des fichiers journaux de Filtering Service . . 474
Espace disque faible dans l'ordinateur Log Server. 476
Aucun Log Server installé pour un serveur Policy Server 477
Plusieurs instances de Log Server installées pour une seule instance de Policy Server 477
Non création de la base de données d'activité 479
Base de données d'activité non disponible 479
Taille de la base de données d'activité retardant la génération des rapports 481
Plus de 100 fichiers dans le répertoire du cache de Log Server 481
Dernière exécution réussie de la tâche ETL depuis plus de 4 heures 483
Configuration de Log Server pour l'utilisation d'un compte de base de données 483
Aucun enregistrement de Log Server dans la base de données d'activité . . 484
Mise à jour du compte ou du mot de passe de connexion à Log Server 484
Configuration des autorisations d'utilisateur pour Microsoft SQL Server . . 485
Problèmes de connexion de Log Server au service d'annuaire. 486
Affichage d'une page de rapport incorrecte 486
Problèmes des rapports d'investigation et de présentation. 487
Planificateur de rapports de présentation non connecté à la base de données d'activité 487
Espace disque inadéquat pour générer des rapports de présentation 488
Échec des tâches planifiées dans les rapports de présentation 488
Données erronées dans les rapports du temps de navigation sur Internet. . . 489
Bande passante plus importante que prévu 489
Absence des données de tendance dans la base de données d'activité 489
Rapports de tendance vides. 490
Absence de journalisation de certaines requêtes de protocoles. 490
Rapports vides. 491
Partitions de base de données 491
Tâche SQL Server Agent. 491
Configuration de Log Server 492
Données de rapport manquantes dans le document Microsoft Excel 492
Enregistrement du résultat des rapports de présentation au format HTML . 493
Erreur de génération ou d'affichage des rapports de présentation 493
Problèmes de recherche dans les rapports d'investigation 494

Problèmes généraux liés aux rapports d'investigation 494
Autres problèmes de génération de rapports 494
Mémoire faible dans l'ordinateur Real-Time Monitor 495
Non exécution de Real-Time Monitor 495
Plus de réponse de Real-Time Monitor. 496
Impossible d'accéder à certaines fonctions de génération de rapports 496
Aucun graphique affiché dans la page État > Tableau de bord. 496
Problème de configuration des données d'analyse 497
Emplacement du référentiel d'analyse inaccessible 497
Données d'analyse sur le point de dépasser la limite de taille ou d'âge 498
Non exécution ou indisponibilité de Websense Multiplexer 498
Problèmes d'interopérabilité 499
Non exécution de Content Gateway 499
Indisponibilité de Content Gateway 500
Alertes non critiques de Content Gateway 500
Accès impossible de l'administrateur aux autres modules TRITON 503
Indisponibilité de Sync Service. 503
Problème de téléchargement des fichiers journaux par Sync Service. 504
Problème d'envoi des données de Sync Service à Log Server 505
Données du filtrage hybride manquantes dans les rapports 505
Espace disque faible dans l'ordinateur Sync Service 506
Fichier de configuration de Sync Service 506
Non exécution de Directory Agent 507
Impossibilité pour Directory Agent de se connecter au contrôleur de domaine . 508
Problèmes de communication de Directory Agent 509
Service d'annuaire non pris en charge par Directory Agent 509
Fichier de configuration de Directory Agent 510
Paramètres de ligne de commande de Directory Agent 511
Envoi d'alertes par le service hybride 512
Impossible de se connecter au service hybride 513
Problème d'authentification des connexions du service hybride 513
Absence d'informations essentielles dans la configuration hybride 514
Suppression du proxy de basculement hybride dans les listes de proxy explicites 514
Conseils et outils de dépannage 515
Emplacement du répertoire « bin » de Websense 515
Boîte de dialogue Services de Windows. 515
Observateur d'événements de Windows. 516
Fichier journal Websense 516

1 Mise en route

Pour apprendre à exploiter les solutions Websense Web Security et trouver les réponses à vos questions, parcourez ce guide ou sélectionnez directement l'une des rubriques suivantes.

Procédure de base	Solutions initiales
• *Utilisation de TRITON - Web Security* • *Votre abonnement* • *Tableau de bord de Web Security*	• *Problèmes d'installation et d'abonnement* • *Problèmes de la base de données principale* • *Conseils et outils de dépannage*
Démarrage du filtrage	**Solutions de filtrage**
• *Filtrage des catégories et des protocoles* • *Ajout d'un client* • *Fonctionnement des stratégies* • *Attribution d'une stratégie aux clients*	• *Problèmes de filtrage* • *Problèmes de configuration et d'identification des utilisateurs* • *Problèmes de messages de blocage*
Utilisation des rapports	**Solutions de génération de rapports**
• *Rapports de présentation* • *Rapports d'investigation* • *Real-Time Monitor* • *Utilisation de la boîte à outils pour vérifier le comportement du filtrage*	• *Problèmes liés aux journaux, aux messages d'état et aux alertes* • *Problème de Log Server et de la base de données d'activité* • *Problèmes des rapports d'investigation et de présentation*
Outils avancés	**Autres solutions**
• *Exceptions aux stratégies de filtrage* • *Redéfinition du filtrage pour des sites spécifiques* • *Administration déléguée et génération de rapports*	• *Problèmes d'administration déléguée* • *Problèmes d'interopérabilité* • *Conseils et outils de dépannage*

Présentation

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

La suite de composants Websense (décrits à la section *Composants du produit Websense Web Security*, page 354) offre des capacités de filtrage Internet, d'identification des utilisateurs, de création d'alertes, de génération de rapports et de dépannage.

Une présentation des nouvelles fonctionnalités incluses dans cette version de Websense est disponible dans les Notes de publication, accessibles via la Bibliothèque technique de Websense.

Après son installation, Websense applique la stratégie **Par défaut** pour surveiller l'utilisation d'Internet sans bloquer les requêtes. Cette stratégie gère l'accès Internet de tous les clients du réseau jusqu'à ce que vous définissiez vos propres stratégies et les attribuiez aux clients. Après la création de vos propres paramètres de filtrage personnalisés, la stratégie Par défaut continue à s'appliquer chaque fois qu'un client n'est pas géré par une autre stratégie. Pour plus d'informations, consultez *La stratégie Par défaut*, page 90.

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

- *Filtres de l'utilisation Internet*, page 49
- *Clients*, page 71
- *Stratégies de filtrage Internet*, page 89

Un même outil de type navigateur (la console TRITON™ Unified Security Center) fournit une interface graphique centrale aux fonctions générales de configuration, de gestion des stratégies et de génération de rapports de vos solutions Websense Web Security, Data Security et Email Security. Pour plus d'informations, consultez *Utilisation de TRITON - Web Security*, page 18.

Pour autoriser certains administrateurs à gérer un ou plusieurs modules TRITON, vous pouvez définir différents niveaux d'accès à la console TRITON Unified Security Center. Le module Web Security vous permet d'affiner encore davantage les autorisations d'accès afin d'autoriser les administrateurs à configurer le comportement du filtrage Internet, à gérer les stratégies de filtrage et à exécuter des tâches de génération de rapports, entre autres. Pour plus d'informations, consultez *Administration déléguée et génération de rapports*, page 323.

Utilisation de TRITON - Web Security

La console TRITON Unified Security Center est l'interface de configuration

Rubriques connexes :

- *Navigation dans TRITON - Web Security*, page 20
- *Tableau de bord de Web Security*, page 33

centralisée qui permet de gérer les logiciels Websense Web Security, Email Security et Data Security. Cette interface comprend un module Web Security (appelé TRITON - Web Security) qui permet de personnaliser le comportement du filtrage, de surveiller l'utilisation d'Internet, de générer des rapports sur l'utilisation d'Internet et de gérer la configuration et les paramètres de Websense Web Security.

Important

L'Affichage de compatibilité Internet Explorer 8 n'est **pas** pris en charge avec la console TRITON. En cas de comportement étrange ou de problème de mise en page dans Internet Explorer 8, vérifiez que le bouton Affichage de compatibilité (situé entre l'URL et le bouton Actualiser de la barre d'adresse du navigateur) n'est pas activé.

Lors de l'installation, la console TRITON Unified Security Center est configurée pour que l'accès complet à la totalité des modules et paramètres TRITON ne soit accordé qu'à un seul compte d'administrateur : **admin**. Le mot de passe de ce compte est défini pendant l'installation.

Lorsque vous vous connectez à l'aide du compte admin ou avec un autre compte d'administrateur disposant d'autorisations Web Security, la page État > Tableau de bord du module Web Security s'affiche.

- S'il s'agit de votre première connexion à TRITON - Web Security, vous avez la possibilité de visionner le didacticiel Démarrage rapide. Si vous découvrez Websense, ou cette version de Websense, ce didacticiel est vivement conseillé.
- Lors de la première connexion, lorsqu'un administrateur quitte le Tableau de bord, le bouton **Save and Deploy (Enregistrer et déployer)** s'active. Ce bouton permet d'enregistrer les paramètres initiaux par défaut du tableau de bord pour ce compte d'administrateur. (Une fois ces paramètres initiaux enregistrés, le bouton Save and Deploy (Enregistrer et déployer) ne s'active à la sortie du tableau de bord que si des graphiques ont été ajoutés, supprimés ou modifiés.)
- Si vous utilisez un compte autorisé à accéder à plusieurs modules TRITON, servez-vous de la barre d'outils TRITON pour passer d'un module à l'autre. Voir *Navigation dans TRITON - Web Security*, page 20.
- Si vous utilisez l'administration déléguée et que vous avez créé des rôles administratifs, vous pouvez être invité(e) à sélectionner un rôle à gérer. Voir *Administration déléguée et génération de rapports*, page 323.

Lors de la connexion, TRITON - Web Security se connecte à l'instance de Policy Server par défaut (de base) définie pendant l'installation. Pour gérer une autre instance de Policy Server, sélectionnez son adresse IP dans la liste déroulante Policy Server de la barre d'outils de Web Security.

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

- Si la page comprend des modifications non mises en cache ou des modifications en attente de mise en cache, ces modifications sont perdues lorsque la session se termine. N'oubliez pas de cliquer sur **OK** pour mettre vos modifications en cache et sur **Save and Deploy (Enregistrer et déployer)** pour les enregistrer et les implémenter.
- Si TRITON - Web Security est ouvert dans plusieurs onglets de la même fenêtre du navigateur, toutes ses instances partagent la même session. Si la session arrive à expiration dans un onglet, il en est de même pour tous les autres onglets.

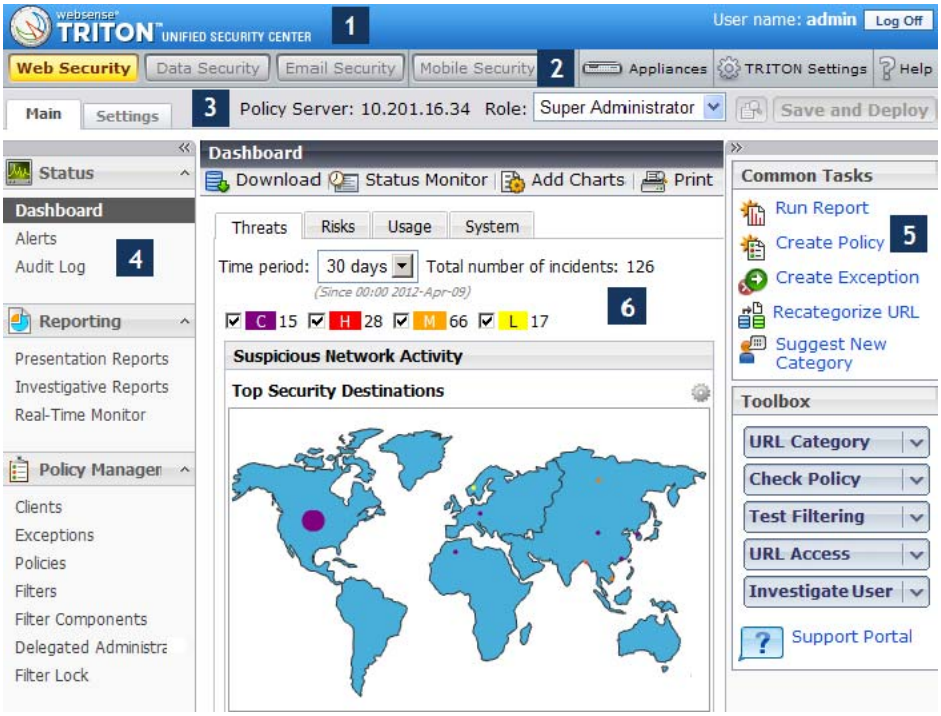
- Si TRITON - Web Security est ouvert dans plusieurs fenêtres de navigateur sur le même ordinateur, ses instances partagent la même session **si** :
  - Vous utilisez Microsoft Internet Explorer et le raccourci clavier Ctrl-N pour ouvrir une nouvelle instance de TRITON - Web Security.
  - Vous utilisez Mozilla Firefox.

  Si la session arrive à expiration dans une fenêtre, il en est de même pour toutes les autres fenêtres.
- Dans les instances suivantes, vous pouvez ouvrir plusieurs instances de TRITON - Web Security qui ne partagent pas de session. Dans ce cas, lorsqu'une fenêtre arrive à expiration, les autres ne sont pas affectées.
  - Ouvrez plusieurs fenêtres Internet Explorer indépendamment les unes des autres.
  - Utilisez la commande Fichier > Nouvelle session pour ouvrir une nouvelle fenêtre Internet Explorer 8.
  - Utilisez Internet Explorer pour ouvrir une connexion à TRITON - Web Security, puis Firefox pour en ouvrir une autre.

Si vous fermez le navigateur sans vous déconnecter de la console TRITON Unified Security Center, ou si l'ordinateur distant à partir duquel vous accédez à un module TRITON s'éteint inopinément, il est possible que votre compte soit temporairement verrouillé. Websense détecte généralement ce problème en 2 minutes environ et met fin à la session interrompue, ce qui vous permet de vous reconnecter.

Navigation dans TRITON - Web Security

L'interface TRITON - Web Security est divisée en 6 zones principales :



1. Bannière
2. Barre d'outils TRITON

3. Barre d'outils Web Security
4. Panneau de navigation gauche
5. Panneau de raccourcis droit
6. Panneau de contenu

Ce guide présente les options disponibles avec le compte **admin**. Les administrateurs délégués peuvent voir un sous-ensemble des fonctionnalités décrites ici. Pour plus d'informations, consultez *Administration déléguée et génération de rapports*, page 323.

Bannière

La bannière, située en haut de la page du navigateur, présente :

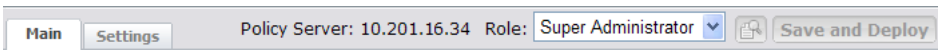
- Le **nom d'utilisateur** associé à votre compte de connexion en tant qu'administrateur
- Un bouton **Déconnecter**, que vous pouvez utiliser pour mettre fin à votre session administrative

Barre d'outils TRITON

La barre d'outils TRITON, située sous la bannière, vous permet d'effectuer les opérations suivantes :

- Passer d'un module TRITON Unified Security Center à l'autre
- Vous connecter à Appliance Manager pour l'un des **dispositifs** V-Series déployés dans votre réseau
- Configurer les **Paramètres TRITON** globaux affectant tous les modules installés
- Consulter l'**Aide**, les didacticiels, les informations relatives au produit et les ressources du Support technique de Websense

Barre d'outils Web Security



La barre d'outils de Web Security, située sous la barre d'outils TRITON, permet de :

- Passer de l'onglet **Principal** à l'onglet **Paramètres** et vice-versa dans le panneau de navigation gauche
- Identifier l'instance de Policy Server à laquelle vous êtes connecté et passer éventuellement d'une instance de Policy Server à l'autre (voir *Fonctionnement de Policy Server*, page 360)
- Afficher votre **Rôle** administratif, passer d'un rôle à l'autre ou attribuer des autorisations de stratégie au rôle en cours

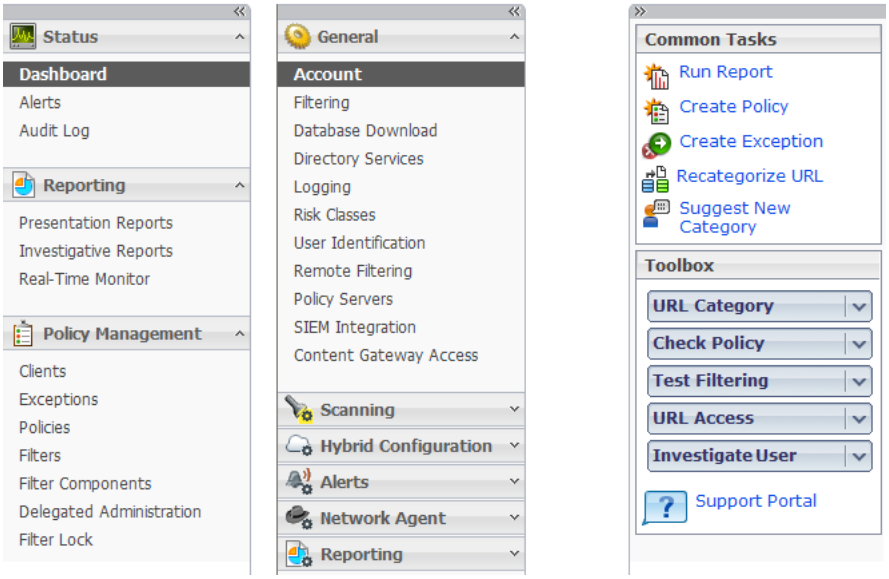
Conseil

Si vous disposez d'autorisations de gestion des stratégies et de génération de rapports, mais que seules les fonctions de génération de rapports s'affichent, il est possible qu'un autre administrateur soit connecté à ce rôle. Un seul administrateur à la fois peut accéder aux fonctions de gestion des stratégies pour chaque rôle.

- **Afficher les modifications en attente** (via la petite icône en forme de loupe), puis **enregistrer et déployer** ces modifications. Lorsque le cache ne contient pas de modifications en attente d'enregistrement, ces boutons sont désactivés.

  Pour plus d'informations, consultez *Vérification, enregistrement et annulation des modifications*, page 23.

Panneaux de navigation droit et gauche



Le panneau de navigation gauche comprend deux onglets : **Principal** et **Paramètres**. L'onglet **Principal** permet d'accéder aux fonctions d'état, de génération de rapports et de gestion des stratégies. L'onglet **Paramètres** vous permet de gérer votre compte Websense et d'exécuter des tâches d'administration globale du système. (Notez que, selon votre niveau d'inscription, les options de l'onglet Paramètres diffèrent.)

Le panneau de raccourcis droit contient des liens permettant d'accéder aux outils et aux tâches administratives courantes.

- La section **Tâches courantes** fournit des raccourcis vers les tâches administratives les plus utilisées. Cliquez sur un élément de la liste pour ouvrir directement la page dans laquelle s'exécute cette tâche.
- La section **Boîte à outils** contient des outils de recherche rapide qui vous permettent de vérifier votre configuration du filtrage. Pour plus d'informations, consultez *Utilisation de la boîte à outils pour vérifier le comportement du filtrage*, page 282.

Les panneaux de navigation droit et gauche peuvent tous deux être réduits par un clic sur l'icône en forme de double flèche (<< ou >>) située en haut de chaque panneau. Pour afficher le panneau, cliquez sur l'icône inverse (>> ou <<).

Pour afficher le menu des fonctionnalités associées sans développer le panneau gauche, survolez une icône de raccourci de ce panneau.

Vérification, enregistrement et annulation des modifications

Lorsque vous apportez une modification dans TRITON - Web Security, un clic sur le bouton **OK** situé au bas de la page est généralement nécessaire pour mettre cette modification en cache. Cliquez ensuite sur **Save and Deploy (Enregistrer et déployer)** pour enregistrer la modification dans la base de données de stratégies et l'implémenter.

- Certains champs et sections de TRITON - Web Security disposent de leur propre bouton **Enregistrer** ou **Enregistrer maintenant**. Les modifications apportées à ces fonctionnalités sont enregistrées et implémentées immédiatement, sans être mises en cache, puis enregistrées.
- Certains types de modifications impliquent que vous cliquiez sur OK dans une page secondaire et une page principale pour les mettre en cache.

Important

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

Pour revoir les modifications mises en cache, utilisez la page **Afficher les modifications en attente**. Les modifications apportées à une seule zone de fonctionnalités sont généralement regroupées sous une seule entrée dans la liste du cache. Par exemple, si vous ajoutez 6 clients et que vous en supprimez 2, la liste du cache indique uniquement que des modifications ont été apportées aux Clients. À l'inverse, les modifications apportées à une seule page Paramètres peuvent se traduire par plusieurs entrées dans la liste du cache. Cela se produit lorsqu'une seule page Paramètres est utilisée pour configurer plusieurs fonctions de Websense.

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

Lorsque vous choisissez Enregistrer toutes les modifications ou Annuler toutes les modifications, vous revenez dans la dernière page sélectionnée. Les fonctions Enregistrer tout ou Annuler tout ne peuvent pas être annulées.

Pour revoir les détails des modifications apportées dans TRITON - Web Security, servez-vous du Journal d'audit. Pour plus d'informations, consultez *Affichage et exportation du journal d'audit*, page 373.

Votre abonnement

Les abonnements à Websense sont générés par client (utilisateur ou adresse IP).

Pour pouvoir commencer à filtrer vos connexions, vous devez fournir une clé d'abonnement valide (voir *Configuration des informations de votre compte*, page 24). Cela vous autorise à télécharger la Base de données principale (voir *Base de données principale Websense*, page 27), qui permet au logiciel Websense de filtrer les clients.

Dès le premier téléchargement réussi de la base de données, TRITON - Web Security affiche le nombre de clients inclus dans l'abonnement et le type d'abonnement (Web Filter, Web Security, Web Security Gateway ou Web Security Gateway Anywhere). Avant ce premier téléchargement, des espaces réservés s'affichent.

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

Lorsque le nombre de clients présents dans la table atteint le niveau maximal, tous les client non listés précédemment qui demandent un accès Internet sortent du cadre de l'abonnement. Dans ce cas, soit ils sont totalement privés d'accès Internet, soit ils reçoivent un accès non filtré, selon le paramètre choisi. De même, lorsqu'un abonnement arrive à expiration, tous les clients sont soit entièrement bloqués, soit non filtrés, selon ce paramètre.

Pour configurer le comportement du filtrage en cas d'abonnement périmé, consultez *Configuration des informations de votre compte*, page 24.

Pour configurer Websense de sorte qu'il envoie des alertes par courrier électronique lorsque votre abonnement touche à sa fin ou est périmé, consultez *Configuration des alertes système*, page 380.

Gestion de votre compte via le portail MyWebsense

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

Lorsque vous créez un compte, ce dernier est associé à votre clé d'abonnement Websense (ou à vos clés). Cela facilite votre accès aux informations, aux alertes et aux correctifs appropriés à votre produit et à votre version de Websense.

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

Configuration des informations de votre compte

Rubriques connexes :

- *Votre abonnement*, page 24
- *Configuration des téléchargements de la base de données*, page 28
- *Fonctionnement des protocoles*, page 264

La page **Paramètres > Général > Compte** vous permet de saisir ou de vérifier vos informations d'abonnement et d'identifier le comportement de Websense lorsque cet abonnement arrive à expiration ou en cas de dépassement du niveau d'abonnement.

Cette page vous permet également d'indiquer à Websense d'envoyer anonymement les données d'utilisation des catégories et des protocoles à Websense, Inc. Ces informations permettent éventuellement d'optimiser la Base de données principale de Websense et l'efficacité du filtrage (voir *Base de données principale Websense*, page 27) et de contribuer à améliorer le réseau Websense Security Labs ThreatSeeker® (voir websense.com/content/Threatseeker.aspx).

Après l'installation de Websense, ou dès que vous recevez une nouvelle clé d'abonnement, utilisez le champ **Clé d'abonnement** pour saisir votre clé, puis cliquez sur **Appliquer**. Après vérification de la syntaxe de la clé, Filtering Service tente alors de télécharger la Base de données principale.

- Si une clé s'affiche alors que le champ de la clé d'abonnement est désactivé, vous êtes connecté à une instance secondaire de Policy Server. Cela signifie que cette instance récupère ses informations de clé auprès de l'instance principale de Policy Server dont l'adresse IP s'affiche sous le nombre d'utilisateurs abonnés.
- La page **Paramètres > Général > Policy Servers (Serveurs Policy Server)** permet de gérer les clés d'abonnement dans les environnements à plusieurs serveurs Policy Server (voir *Fonctionnement d'un environnement à plusieurs serveurs Policy Server*, page 363).
- Lorsque la syntaxe de la clé est correcte mais que le téléchargement de la Base de données principale échoue parce que cette clé n'est pas valide ou est périmée, un message d'alerte de fonctionnement s'affiche dans la page État > Alertes. Par défaut, le message s'affiche également dans l'onglet Système de la page État > Tableau de bord.

Dès le premier téléchargement réussi de la base de données principale, la page Compte présente les informations suivantes :

Date d'expiration de la clé	Date d'expiration de votre abonnement actuel. Après cette date, vous devez renouveler l'abonnement pour continuer à télécharger la base de données principale et filtrer votre réseau.
Utilisateurs abonnés	*Web Security Gateway Anywhere* : Total des utilisateurs filtrés par les composants sur site, le filtrage hybride et le filtrage distant
Utilisateurs abonnés du réseau	Nombre d'utilisateurs du réseau pouvant être filtrés
Utilisateurs abonnés distants	Nombre d'utilisateurs pouvant être filtrés à l'extérieur du réseau (requiert des composants de filtrage à distance en option)
Instance principale de Policy Server	Adresse IP de l'instance de Policy Server auprès de laquelle cette instance de Policy Server récupère les informations de la clé d'abonnement Apparaît uniquement lorsque les informations d'une instance secondaire de Policy Server s'affichent.

1. Sélectionnez **Bloquer les utilisateurs lorsque l'abonnement expire ou est dépassé** pour :
   - Bloquer tous les accès Internet de tous les utilisateurs lorsque l'abonnement arrive à expiration

- Bloquer tous les accès Internet des utilisateurs qui ont dépassé le nombre d'utilisateurs abonnés

Si cette option n'est pas activée, ces utilisateurs ont accès à Internet sans être filtrés.

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

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

3. Sous WebCatcher, cochez **Send URL information to Websense (Envoyer les informations sur les URL à Websense)** pour aider Websense, Inc., à améliorer la catégorisation des URL et à renforcer l'efficacité et la sécurité. Pour plus d'informations sur cet outil, consultez la section *Qu'est-ce que WebCatcher ?*, page 30.

   - Pour envoyer les URL non catégorisées afin qu'elles soient évaluées, puis classées, cochez l'option **Send uncategorized URLs to improve URL categorization (Envoyer les URL non catégorisées pour améliorer la catégorisation des URL)**.
   - Pour envoyer les URL liées à la sécurité et participer au suivi de l'activité des sites Web malveillants, cochez l'option **Send security URLs to improve security effectiveness (Envoyer les URL de sécurité pour améliorer l'efficacité de la sécurité)**.
   - Pour conserver une copie locale des informations envoyées à Websense, Inc. et pouvoir ensuite les examiner, cochez l'option **Enregistrer une copie des données envoyées à Websense**.

     Lorsque cette option est activée, WebCatcher enregistre les données sous forme de fichiers XML non cryptés dans le répertoire **Websense\Web Security\bin** de l'ordinateur Log Server. Ces fichiers comportent une date et une heure.
   - Sélectionnez le **Pays d'origine** de votre organisation. Il doit s'agir du pays où la majeure partie de l'activité Internet est enregistrée.
   - Spécifiez une **Taille maximale du fichier de téléchargement**. Lorsque la taille maximale est atteinte, les données collectées par WebCatcher sont envoyées automatiquement et un nouveau fichier est créé.
   - Le champ **Heure de début chaque jour** vous permet d'indiquer l'heure à laquelle WebCatcher doit envoyer chaque jour les données collectées lorsque la taille maximale définie pour ce fichier n'a pas été atteinte.

4. (*Websense Web Security Gateway Anywhere*) Pour activer ou mettre à jour la connexion entre les parties sur sites et hybrides de votre solution Web Security :

   - Entrez l'**Adresse électronique de contact** de vos administrateurs Web Security. Il s'agit généralement d'un alias d'e-mail de groupe fréquemment surveillé. Les alertes relatives aux problèmes du filtrage hybride sont envoyées à cette adresse. Le fait de ne pas répondre à une alerte de façon appropriée peut entraîner la déconnexion temporaire de votre service hybride.
   - Entrez le **Pays** et le **Fuseau horaire** de vos administrateurs.

   Le service hybride ne filtre pas les utilisateurs tant que ces informations n'ont pas été fournies et validées. Pour plus d'informations, consultez la section *Configuration du filtrage hybride*, page 203.

5. Lorsque vos modifications sont terminées, cliquez sur **OK**. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Base de données principale Websense

Rubriques connexes :

- *Mises à jour en temps réel de la base de données*, page 28
- *Real-Time Security Updates™*, page 28
- *Configuration des téléchargements de la base de données*, page 28
- *Vérification de l'état du téléchargement de la base de données principale*, page 366
- *Reprise des téléchargements de la base de données principale*, page 367

La Base de données principale de Websense héberge les définitions des catégories et des protocoles qui constituent la base du filtrage du contenu Internet (voir *Filtrage des catégories et des protocoles*, page 50).

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

Une version limitée de la base de données de filtrage est installée en même temps que Websense, mais il est conseillé de télécharger la Base de données principale complète dès que possible afin de profiter de la totalité des capacités de filtrage Internet. Pour télécharger la Base de données principale pour la première fois, saisissez votre clé d'abonnement dans TRITON - Web Security. Vous avez pour cela deux possibilités :

- Lorsque vous y êtes invité(e) à votre première connexion
- Dans la page **Paramètres > Général > Compte** (voir *Configuration des informations de votre compte*, page 24)

Si Websense doit passer par un proxy pour effectuer ce téléchargement, utilisez également la page **Paramètres > Général > Téléchargement de la base de données** pour configurer les paramètres du serveur proxy (voir *Configuration des téléchargements de la base de données*, page 28).

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

Après le téléchargement initial, Websense télécharge les modifications apportées à la base de données en fonction du planning défini (voir *Configuration des téléchargements de la base de données*, page 28). La Base de données principale étant fréquemment mise à jour, par défaut, ses téléchargements sont planifiés pour intervenir chaque jour.

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

Pour déclencher un téléchargement de la base de données à tout moment, ou pour consulter l'état et la date du dernier téléchargement ou le numéro de version de la base de données actuelle, ouvrez l'onglet **Système** du Tableau de bord Web Security, puis cliquez sur l'option **Téléchargement de la base de données** dans la barre d'outils située en haut du panneau de contenu.

Mises à jour en temps réel de la base de données

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

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

Les mises à jour les plus récentes sont énumérées à la page **Etat > Alertes** (voir *Vérification de l'état actuel du système*, page 385).

Real-Time Security Updates™

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

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

Le service de filtrage vérifie la présence de mises à jour de sécurité toutes les 5 minutes, mais ces mises à jour étant bien plus petites que celles de la base de données complète, elles ne perturbent généralement pas l'activité normale du réseau.

Pour activer le service Real-Time Security Updates, ouvrez la page **Paramètres > Général > Téléchargement de la base de données** (voir *Configuration des téléchargements de la base de données*, page 28).

Configuration des téléchargements de la base de données

Rubriques connexes :

- *Configuration des informations de votre compte*, page 24
- *Base de données principale Websense*, page 27
- *Vérification de l'état du téléchargement de la base de données principale*, page 366

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

1. (*Websense Web Security, Web Security Gateway et Web Security Gateway Anywhere*) Sélectionnez **Enable real-time security updates (Activer les mises à jour de sécurité en temps réel)** (par défaut) pour que Websense vérifie la présence de mises à jour de sécurité de la Base de données principale toutes les 5 minutes. Lorsqu'une mise à jour de sécurité est détectée, elle est immédiatement téléchargée.
2. Les mises à jour de sécurité en temps réel protègent rapidement votre réseau contre toute vulnérabilité relative aux attaques de type phishing (identification des fraudes), aux applications malveillantes et au code viral infectant les applications ou les sites Web.
3. Sélectionnez les **Jours de téléchargement** pour les téléchargements automatiques.
   - Lorsque le service Real-Time Security Updates est activé, tous les jours de téléchargement sont sélectionnés. Les téléchargements sont effectués automatiquement tous les jours afin de s'assurer que la base de données standard la plus récente est disponible pour les mises à jour de sécurité.
   - Pour que Websense poursuive le filtrage sans interruption, vous devez télécharger la base de données principale au moins une fois tous les 14 jours.
   - Si vous désactivez tous les jours de téléchargement, Websense tente automatiquement de télécharger la base de données lorsque celle-ci a plus de *7 jours*.
4. À côté de **Télécharger entre**, sélectionnez les heures de début et de fin de la période au cours de laquelle Filtering Service doit tenter de télécharger les mises à jour de la Base de données principale. Par défaut, le téléchargement est effectué entre 21:00 et 06:00 (heure de l'ordinateur Filtering Service).
   - Websense sélectionne une heure aléatoire au cours de cette période pour contacter le serveur de la Base de données principale. Pour configurer des alertes en cas d'échec du téléchargement, consultez *Configuration des alertes système*, page 380.
   - Chaque fois qu'il redémarre, Filtering Service vérifie la présence de mises à jour de la Base de données principale. La mise à jour peut alors commencer immédiatement sans attendre la période définie.

   Remarque

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

5. Si Websense doit accéder à Internet par l'intermédiaire d'un serveur proxy ou d'un pare-feu pour télécharger la Base de données principale, sélectionnez **Utiliser un serveur proxy ou un pare-feu**. Saisissez ensuite :
   - L'**adresse IPv4 ou le nom d'hôte** du serveur proxy ou du pare-feu
   - Le **Port** par lequel le téléchargement de la base de données doit passer (8080 par défaut)
6. Si le serveur proxy ou le pare-feu configuré ci-dessus exige une authentification pour accéder à Internet, sélectionnez **Utiliser l'authentification**, puis entrez le **Nom d'utilisateur** et le **Mot de passe** que Websense doit utiliser pour accéder à Internet.

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

Par défaut, le nom d'utilisateur et le mot de passe sont codés au format du jeu de caractères défini dans les paramètres régionaux de l'ordinateur Policy Server. Cet encodage peut être configuré manuellement via la page **Paramètres** > **Général** > **Services d'annuaire** (voir *Paramètres avancés de l'annuaire*, page 78).

Qu'est-ce que WebCatcher ?

WebCatcher est une fonctionnalité en option qui collecte les URL non reconnues et liées à la sécurité, puis les envoie aux laboratoires Websense Security Labs. La catégorisation des URL non catégorisées est alors vérifiée, et les URL liées à la sécurité sont analysées afin de déterminer leur potentialité en matière de menaces Internet. (La journalisation des URL complètes n'est pas obligatoire pour le traitement de WebCatcher.) Les résultats de l'analyse servent à mettre à jour la Base de données principale, ce qui améliore le filtrage.

> **Remarque**
> Dans un environnement à plusieurs instances de Web Security Log Server, WebCatcher n'est activé qu'une seule fois, via la page **Paramètres** > **Général** > **Comptes** de TRITON - Web Security.

Les informations envoyées à Websense Security Labs ne contiennent que les URL et aucun renseignement sur les utilisateurs. Par exemple :

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

L'adresse IP de cet exemple correspond à l'adresse de l'ordinateur hébergeant l'URL, pas à celle du demandeur.

> **Remarque**
> Les sites intranet ne sont pas envoyés par WebCatcher. Cela comprend tous les sites des plages 10.xxx.xxx.xxx, 172.16.xxx.xxx et 192.168.xxx.xxx.

Les données de WebCatcher sont envoyées à Websense, Inc. via publication HTTP. Il vous faudra peut-être créer des rôles ou modifier votre serveur proxy ou votre pare-feu pour autoriser le trafic HTTP sortant.

Support technique de Websense

Des informations techniques sur les services et les logiciels Websense sont disponibles 24 heures sur 24 à l'adresse support.websense.com, notamment :

- La Base de connaissances de Websense (composée d'un Centre de solutions, d'une Bibliothèque technique et des forums des clients) dans laquelle vous pouvez effectuer des recherches
- Des wébinaires et des didacticiels (vidéo)
- Des documents sur les produits et des livres blancs approfondis
- Des réponses aux questions les plus fréquemment posées

Pour toute autre question, ouvrez l'onglet **Contacter le Support technique** en haut de la page.

Les informations de la page de contact permettent d'identifier des solutions, d'ouvrir un ticket d'incident en ligne et d'appeler le Support technique de Websense par téléphone.

Pour une réponse téléphonique plus rapide, utilisez votre **N° de compte de support technique**, indiqué dans la section Profil du portail MyWebsense.

Dans le cas d'un contact téléphonique, veuillez préparer :

- Votre clé d'abonnement Websense
- Votre accès à la console de gestion de vos solutions (par exemple, la console TRITON, Appliance Manager, Content Gateway Manager)
- Votre accès à l'ordinateur exécutant les outils de génération de rapports et le serveur de base de données (Microsoft SQL Server ou SQL Server Express)
- Des informations sur l'architecture de votre réseau, ou l'accès à une personne disposant de ces connaissances

2 Tableau de bord de Web Security

L'onglet **Threats (Menaces)** de la page **État > Tableau de bord** s'affiche en premier lorsque vous vous connectez à TRITON - Web Security. Cet onglet présente des informations sur l'activité suspecte éventuellement liée à la présence de contenu malveillant avancé dans votre réseau.

- Le type d'informations et la quantité de détails dépendent de votre niveau d'abonnement. Web Security Gateway ou Web Security Gateway Anywhere est exigé, par exemple pour afficher des informations sur les menaces sortantes et pour fournir des données d'analyse détaillées à propos des menaces. Voir *Tableau de bord Threats (Menaces)*, page 35.
- Contrairement aux autres onglets du Tableau de bord Web Security, vous ne pouvez ni ajouter ni supprimer des éléments dans le tableau de bord Threats (Menaces).

Les éléments du tableau de bord sont visibles pour les Super administrateurs et les administrateurs délégués autorisés à afficher des rapports dans le Tableau de bord Web Security (voir *Modification des rôles*, page 337).

- L'accès des administrateurs délégués au tableau de bord Menaces est configuré indépendamment de l'accès aux tableaux de bord Risques, Usage et Système.
- Les administrateurs délégués autorisés à accéder au tableau de bord Threats (Menaces) peuvent également être autorisés à consulter les détails d'analyse associés au contenu malveillant avancé. Voir *Examen des données d'analyse liées aux menaces*, page 41.

Lorsqu'un administrateur se connecte pour la première fois à TRITON - Web Security, puis quitte le tableau de bord au cours de sa navigation, le bouton **Save and Deploy (Enregistrer et déployer)** s'active, et ce que des modifications aient été ou non apportées aux paramètres par défaut du tableau de bord pour le compte de l'administrateur.

Une fois ces paramètres initiaux enregistrés, le bouton Save and Deploy (Enregistrer et déployer) ne s'active lors de la sortie du tableau de bord que si des graphiques ont été ajoutés, supprimés ou modifiés.

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. Voir *Tableau de bord Risques*, page 41.
- L'onglet **Usage** donne des informations sur les modèles de trafic de votre réseau, notamment des informations sur la bande passante et des résumés du filtrage. Voir *Tableau de bord Usage*, page 42.

- 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 du filtrage Internet de votre réseau. Voir *Tableau de bord Système*, page 43.

Les tableaux de bord Risques, Usage et Système peuvent chacun présenter jusqu'à 12 éléments (graphiques, résumés de l'état ou compteurs) simultanément. La plupart des graphiques de ces tableaux de bord peuvent être personnalisés, par exemple pour modifier la période utilisée (aujourd'hui, les 7 derniers jours, les 30 derniers jours, etc.) ou le format d'affichage (histogramme empilé, aire empilée, courbes multi-séries, etc.). Vous pouvez inclure plusieurs versions d'un même graphique dans un onglet (par exemple, portant sur des périodes différentes).

- Les éléments des tableaux de bord sont mis à jour toutes les 2 minutes.

  Tous les éléments de l'onglet sont également mis à jour dès que l'un d'entre eux est modifié. Par exemple, lorsque vous modifiez la période d'un graphique, les données de tous les éléments de la page sont mises à jour.
- Le jeu d'éléments de tableau de bord disponible dépend de votre type d'abonnement. Les graphiques liés au filtrage hybride, par exemple, sont disponibles uniquement pour Web Security Gateway Anywhere.
- Pour ajouter un élément dans l'onglet, cliquez sur **Add Charts (Ajouter des graphiques)**, puis consultez la section *Ajout d'éléments dans un onglet du tableau de bord*, page 44, pour obtenir des instructions.
- Pour supprimer un élément de l'onglet, cliquez sur l'icône Options () dans la barre de titre de l'élément en question, puis sélectionnez **Supprimer**.
- Un clic sur un graphique en secteurs, à barres ou de courbes ouvre généralement un rapport d'investigation présentant davantage de détails. Certains graphiques liés à la sécurité sont eux reliés au tableau de bord Threats (Menaces).

La barre d'outils du tableau de bord contient jusqu'à 4 boutons :

- Le bouton **Téléchargement de la base de données**, uniquement disponible pour les Super administrateurs, présente l'état du téléchargement de la Base de données principale et permet de déclencher ou d'interrompre un téléchargement. Voir *Vérification de l'état du téléchargement de la base de données principale*, page 366.
- Le bouton **Status Monitor (Moniteur d'état)** libère les autorisations de stratégie de l'administrateur actuel et active le mode surveillance, qui permet d'accéder aux pages suivantes sans expiration de la session :
  - État > Tableau de bord
  - État > Alertes
  - Génération de rapports > Real-Time Monitor

  Voir *Mode Status Monitor (Moniteur d'état) de Web Security*, page 46.
- Le bouton **Add Charts (Ajouter des graphiques)** permet aux administrateurs de personnaliser l'affichage de l'onglet du tableau de bord sélectionné en ajoutant des éléments dans la page. Voir *Ajout d'éléments dans un onglet du tableau de bord*, page 44.
- Le bouton **Imprimer** présente la version imprimable des graphiques affichés sur la page dans une fenêtre secondaire. Pour imprimer la page, servez-vous des options de votre navigateur.

Tableau de bord Threats (Menaces)

Rubriques connexes :

- *Tableau de bord de Web Security*, page 33
- *Examen des détails des événements suspects*, page 37
- *Affectation d'un niveau de gravité à une activité suspecte*, page 39
- *Examen des détails des incidents suspects*, page 39
- *Examen des données d'analyse liées aux menaces*, page 41

L'onglet **Threats (Menaces)** du Tableau de bord Web Security permet de surveiller et d'examiner l'activité suspecte détectée dans votre réseau.

- 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.

La vue initiale du tableau de bord Menaces contient les éléments suivants :

- **Top Security Destinations (Principales destinations de sécurité)** présente les principaux pays visés par le trafic réseau suspect ou qui hébergent les sites associés à une activité suspecte.
- L'élément **Security Events by Type (Événements de sécurité par type)** présente le nombre de requêtes de sites (destinations) bloquées ou autorisées (ou les deux) dans les principales catégories de sécurité associées aux menaces dangereuses.
- L'élément **Suspicious Event Summary (Résumé des événements suspects)** donne des informations sur les événements représentant une menace pour votre réseau.

La commande **État**, située en haut et à droite de l'onglet, indique si les données de l'onglet Threats (Menaces) sont mises à jour automatiquement.

- Si l'état indique **Running (En cours d'exécution)**, cliquez sur **Pause** pour interrompre la mise à jour des données pendant que vous examinez les résultats.
- Si l'état indique **Paused (En pause)**, cliquez sur **Démarrer** pour actualiser le tableau de bord et récupérer les nouvelles données collectées pendant l'interruption des mises à jour.

D'autres commandes situées en haut de l'onglet vous permettent de limiter les informations affichées dans les graphiques et le tableau récapitulatif aux éléments suivants :

- Période (Aujourd'hui, 7 derniers jours, 30 derniers jours, etc.)
  - Les détails de date indiqués sous la liste déroulante présentent les dates de début et de fin utilisées pour le calcul de la période sélectionnée.
  - Configurez la période maximale disponible dans la page Paramètres > Génération de rapports > Tableau de bord (voir *Configuration des rapports du tableau de bord*, page 418).

    Avec Microsoft SQL Server Express, la période maximale est de 30 jours et n'est pas modifiable.

- Gravité (Critique, Élevée, Moyenne ou Faible)

  Pour plus d'informations sur les catégories associées à chaque niveau de gravité, cliquez sur le lien **Severity Mapping (Mappage de la gravité)**.
- Action (Tout, Autorisée ou Bloquée)
- Direction (Toutes, Entrantes ou Sortantes)

Vous pouvez également utiliser la carte Top Event Destinations (Principales destinations des événements) et le graphique Security Events by Category (Événements de sécurité par catégorie) pour affiner encore davantage les informations affichées dans le tableau de synthèse au bas de la page.

- Cliquez sur un point de la carte pour afficher uniquement le trafic associé à ce pays dans le tableau Suspicious Event Summary (Synthèse des événements suspects).

  La taille du point reflète le nombre d'incidents associés à ce pays. Survolez un point avec votre souris pour afficher une info-bulle présentant le nom du pays. (Survoler une zone bleue sans point affiche le nom du continent.)
- Cliquez sur une catégorie dans le graphique pour afficher uniquement le trafic associé à cette catégorie dans le tableau.

  Chaque catégorie du graphique est représentée par une couleur différente. Pour afficher une info-bulle présentant le nom de la catégorie, survolez une barre ou un segment avec votre souris.

Par défaut :

- La carte Top Event Destinations (Principales destinations de sécurité) présente les 20 principaux pays d'où provient l'activité suspecte ou auxquels celle-ci est envoyée.
- Le graphique Security Events By Category (Événements de sécurité par catégorie) présente les 5 principales catégories associées à l'activité suspecte détectée dans votre réseau, au format histogramme empilé.

Pour modifier les informations de la carte ou du graphique :

- Cliquez sur l'icône **Options**, puis sélectionnez **Modifier**.
- Utilisez la liste **Top (Principaux)** (des deux éléments) ou **Chart type (Type de graphique)** (graphique Security Events by Category (Événements de sécurité par catégorie)) pour actualiser l'affichage.

  La modification de la valeur « top (principaux) » ou du type de graphique n'affecte pas les informations affichées dans le tableau de synthèse.

Les diverses options du tableau Suspicious Event Summary (Synthèse des événements suspects) vous permettent d'identifier des événements spécifiques à examiner.

- Le champ Rechercher vous permet de localiser les événements associés à un nom d'utilisateur, une adresse IP ou un nom d'hôte (si disponible ; requiert Content Gateway).

  Pour arrêter le filtrage du tableau en fonction du terme indiqué dans le champ Rechercher, cliquez sur **Effacer**.
- Chacun des filtres (heure, gravité, action, direction, pays, catégorie) actuellement appliqués dans le tableau de synthèse est répertorié. Pour supprimer un filtre et développer les informations affichées dans le tableau, désactivez la case à cocher accolée à ce filtre.
- Cliquez sur un nom d'utilisateur, une adresse IP ou un nom d'hôte (si disponible) pour afficher un rapport détaillé. Voir *Examen des détails des événements suspects*, page 37.

Vous pouvez personnaliser le tableau Suspicious Event Summary (Synthèse des événements suspects) de manière à afficher ou masquer les colonnes suivantes. Les colonnes affichées par défaut sont désignées par un astérisque (*).

Colonne	Description
Gravité*	Indiquée par une icône « S » sur un fond bleu (S). Présente la gravité (Critique, Élevée, Moyenne ou Faible) affectée à l'événement.
Forensics* (Analyses)	Indiquée par une icône en forme de loupe ( ). Indique si l'événement comprenait une tentative d'envoi de fichiers. Web Security Gateway ou Gateway Anywhere uniquement
Utilisateur*	Nom d'utilisateur (le cas échéant) associé à l'activité
Adresse IP	Adresse IP de l'ordinateur dans lequel l'activité a été détectée
Périphérique*	Nom de l'ordinateur dans lequel l'activité a été détectée Web Security Gateway ou Gateway Anywhere uniquement
Catégorie*	Catégorie de Base de données principale attribuée à l'activité
Last Attempt* (Dernière tentative)	Horodatage de l'événement le plus récent présentant l'ensemble des caractéristiques affichées dans la ligne
Pays*	Indiqué par l'abréviation « CC » (pour « Country Code » en anglais ou code de pays en français). Présente les deux lettres du code du pays de destination de l'événement (cible). Lorsque plusieurs destinations sont associées à un événement, la mention « Multiple » s'affiche.
Direction	Indique si l'activité suspecte concernait du trafic entrant ou sortant La détection des menaces sortantes requiert Web Security Gateway ou Gateway Anywhere.
Incidents*	Nombre d'incidents présentant l'ensemble des caractéristiques affichées dans la ligne, à l'exception de la dernière tentative

Pour ajouter ou retirer des colonnes dans le graphique, cliquez sur le lien **Personnaliser** situé au-dessus du tableau. Activez ou désactivez ensuite la case à cocher accolée au nom d'une colonne pour l'ajouter ou la retirer dans le tableau.

Pour exporter le contenu du tableau dans un fichier CSV, cliquez sur **Export to CSV (Exporter au format CSV)**. Sélectionnez la période pour laquelle vous souhaitez exporter les données des événements, puis cliquez sur **Exporter**.

Examen des détails des événements suspects

La page **Tableau de bord > Threats (Menaces) > Event Details (Détails de l'événement)** vous permet de rechercher des incidents d'activité suspecte. Cette page permet d'afficher les incidents liés à :

- Un nom d'utilisateur, une adresse IP ou un périphérique spécifique sélectionné dans le tableau Suspicious Event Summary (Synthèse des événements suspects) du tableau de bord Threats (Menaces). (Les informations relatives au nom du périphérique sont fournies par Content Gateway et ne sont pas disponibles lorsque d'autres intégrations sont utilisées.)

- Un niveau de gravité spécifique, sélectionné par un clic sur le lien TRITON - Web Security présent dans une notification électronique d'alerte d'activité suspecte (voir *Configuration des alertes d'activité suspecte*, page 384).

En haut de la page, un tableau répertorie chaque incident associé à l'utilisateur, l'adresse IP, le nom d'hôte ou le niveau de gravité sélectionné. Ce tableau présente 10 lignes de données par page.

- Servez-vous du champ Rechercher pour affiner les résultats liés à un incident spécifique ou à un groupe d'incidents associés. Cliquez sur **Effacer** pour supprimer le filtre de recherche.
- Reportez-vous aux informations indiquées en haut et à droite de la page pour identifier la période couverte par le tableau et la date de sa dernière mise à jour.
- Pour modifier les colonnes affichées dans le tableau, cliquez sur l'option **Personnaliser** dans la barre d'outils située en haut du panneau de contenu. Le tableau détaillé présente les mêmes options de colonne que le tableau de synthèse du tableau de bord Threats (Menaces).
- Cliquez sur une ligne du tableau pour actualiser la partie inférieure de la page et obtenir d'autres détails sur l'incident sélectionné, ses menaces associées et les méthodes de détection utilisées (voir *Examen des détails des incidents suspects*, page 39).

  La section des détails sur l'incident comprend un lien conduisant à Websense ACEInsight. Servez-vous de ce lien pour afficher les informations actuelles sur cette URL et les menaces associées à l'incident.
- Lorsqu'il y a plus de 10 incidents, servez-vous des commandes de pagination situées au bas du tableau pour parcourir les données.

Les environnements Web Security Gateway et Gateway Anywhere permettent de collecter les fichiers associés à des tentatives d'intrusion dans votre réseau ou d'envoi de données sensibles à partir de votre réseau. Les données liées aux fichiers sont appelées collectivement **données d'analyse** et sont stockées dans une base de données spéciale appelée **référentiel d'analyses**.

- La collecte et le stockage des analyses sont activés par défaut.
- Configurez la collecte et le stockage des analyses dans la page Paramètres > Génération de rapports > Tableau de bord (voir *Configuration des rapports du tableau de bord*, page 418).

Lorsque la collecte des analyses est activée et que des fichiers (par exemple des feuilles de calcul, des documents ou des fichiers compressés) sont associés à un incident, une icône s'affiche dans la colonne Forensics (Analyses) du tableau de détails de l'événement. Lorsque vous sélectionnez un incident incluant des données d'analyse, les informations relatives au(x) fichier(s) associé(s) à l'incident s'affichent dans la section Forensic Data (Données d'analyse) (voir *Examen des données d'analyse liées aux menaces*, page 41).

Avertissement

Faites bien attention lorsque vous ouvrez un fichier associé à un incident suspect. Si le fichier est corrompu par un programme malveillant, ce dernier peut infecter l'ordinateur utilisé pour étudier l'incident.

Notez également que les fichiers collectés peuvent contenir des données fortement confidentielles.

Pour exporter les informations des événements dans un fichier CSV, cliquez sur l'option **Exporter** dans la barre d'outils située en haut du panneau de contenu. L'exportation porte sur tous les événements associés à des menaces enregistrés au cours de la **période** sélectionnée, pas seulement sur l'utilisateur, l'adresse IP, le nom d'hôte ou le niveau de gravité actuellement affiché dans la page.

Affectation d'un niveau de gravité à une activité suspecte

La Base de données principale de Websense attribue un niveau de gravité aux événements associés à des menaces en fonction de la catégorie affectée à la demande.

- Les niveaux de gravité sont associés aux catégories de la Base de données principale de Websense et peuvent changer lorsque celle-ci est mise à jour.
- Les abonnements Websense Web Filter et Websense Web Security ne comprennent pas toutes les catégories des niveaux de gravité Élevé et Critique. Ces catégories peuvent s'afficher dans le tableau de bord Threats (Menaces), mais ne sont pas disponibles pour le filtrage.

Cliquez sur le lien **Severity Mapping (Mappage de la gravité)**, situé en haut du tableau de bord Threats (Menaces), pour obtenir la liste des catégories associées à un niveau de gravité. La liste indique les catégories non disponibles pour le filtrage dans le cadre de votre abonnement.

Examen des détails des incidents suspects

Lorsqu'un administrateur sélectionne un incident dans le tableau situé en haut de la page Threats (Menaces) > Event Details (Détails de l'événement), tous les détails relatifs à l'incident s'affichent dans la zone située sous ce tableau. Les détails disponibles peuvent varier selon :

- Le type d'incident détecté. Par exemple :
  - Une demande sortante d'URL affectée à une catégorie bloquée par la Base de données principale n'inclut généralement pas le nom, le but ou le type de la menace, car la demande est bloquée avant même que l'analyse Content Gateway n'ait été effectuée.
  - Une demande qui n'inclut pas de tentative de transfert de fichier n'inclut pas de données d'analyse.
- L'intégration fournissant au service de filtrage les informations relatives à la demande Internet. Par exemple :
  - Seul Content Gateway transmet le nom d'hôte, le nom, le but, le type de la menace et les informations sur la catégorie d'analyse.
  - Toutes les intégrations ne transmettent pas les informations relatives au protocole, à la méthode ou au type de contenu.
- Si des tentatives de transfert de fichiers étaient associées à l'incident. (Seul Content Gateway fournit ce type de données d'analyse.) Voir *Examen des données d'analyse liées aux menaces*, page 41.

Les détails suivants sur l'incident peuvent être affichés dans la page :

Champ	Description
Gravité	Critique, Élevée, Moyenne ou Faible Voir *Affectation d'un niveau de gravité à une activité suspecte*, page 39.
Catégorie	Base de données principale ou catégorie personnalisée affectée à l'URL de destination
Threat Name (Nom de la menace)	Nom associé au logiciel malveillant, au trafic « zombie » ou à tout autre activité suspecte (si applicable)
Threat Intent (But de la menace)	Objectif visé par la menace (enregistrement de séquences de touches, ouverture d'une porte dérobée dans le réseau, etc.)
Plate-forme	Système d'exploitation visé par la menace (Windows, Android, etc.)
Type de risque	Classification du logiciel malveillant (cheval de Troie, ver, menace persistante avancée, etc.)
Action	Action attribuée à la requête (Autoriser ou Bloquer)
Raison	Raison pour laquelle l'action Autoriser ou Bloquer a été appliquée (par exemple, la catégorie affectée à l'URL)
Incident Time (Heure de l'incident)	Date et heure de l'incident
Lien ACEInsight	Lien conduisant au site ACEInsight.com, qui permet d'élargir les recherches sur l'URL ou la menace
Utilisateur	Utilisateur demandant l'URL (lorsqu'il a été identifié)
Adresse IP source	Adresse IP à l'origine de la demande
Périphérique	Nom de l'ordinateur à l'origine de la demande (requiert Content Gateway ; lorsque le nom d'hôte n'est pas disponible, l'adresse IP source est répétée)
Adresse IP de destination	Adresse IP de l'URL demandée
Port	Port utilisé pour communiquer avec l'URL demandée
Protocole	Protocole utilisé pour demander l'URL
Direction	Indique si l'incident impliquait une connexion entrante ou sortante
Méthode	Indique si la demande était une requête GET ou POST
Type de contenu	Valeur indiquée dans le champ « Content-Type » de l'en-tête HTTP associé à la demande (par exemple, texte/html, image/gif ou application/javascript)
Octets envoyés	Nombre d'octets envoyés à partir de l'ordinateur source
Octets reçus	Nombre d'octets renvoyés par l'URL cible (destination) Si la demande a été bloquée, le résultat est 0.
Pays	Pays hébergeant l'URL de destination
URL complète	URL complète (domaine, chemin, chaîne CGI et fichier) du site visé
Active Policy (Stratégie active)	Stratégie utilisée pour filtrer la demande
Catégorie de base de données	Catégorie attribuée à la requête par la Base de données principale de Websense

Champ	Description
Scanning Category (Catégorie d'analyse)	Catégorie attribuée à la requête par l'analyse Content Gateway (peut correspondre à celle de la Base de données principale)
Rôle	Rôle d'administration déléguée responsable de la stratégie utilisée pour filtrer la demande

Examen des données d'analyse liées aux menaces

Lorsqu'un administrateur sélectionne un incident incluant des données d'analyse dans la page Threats (Menaces) > Event Details (Détails de l'événement), les détails relatifs aux tentatives de transfert de fichiers s'affichent dans la section des données d'analyse située sous le tableau. Ces détails d'analyse comprennent les éléments suivants :

Champ	Description
Source	Utilisateur ou adresse IP à l'origine de la demande
Destination	Adresse IP de l'ordinateur cible
Data Security Incident ID (ID de l'incident Data Security)	Numéro ID de l'incident Websense Data Security associé à l'incident. Ce numéro permet d'étudier plus précisément l'incident dans TRITON - Data Security (requiert une solution Web Security Gateway Anywhere ou Websense Data Security).
Fichiers	Nom et taille du ou des fichiers associés à l'incident. Le nom de fichier est un lien qui permet d'ouvrir le véritable fichier. **AVERTISSEMENT** : faites bien attention lorsque vous ouvrez un fichier collecté. En effet, il peut contenir un logiciel malveillant susceptible d'infecter l'ordinateur utilisé pour étudier l'incident. Ce fichier peut également contenir des données confidentielles.
Parameters and Body (Paramètres et corps)	Présente les paramètres CGI et les détails du corps HTML de la requête HTTP utilisée pour envoyer ou récupérer le fichier Le nombre de paramètres et les détails inclus dans le corps de la requête varient fortement d'un incident à l'autre.

Tableau de bord Risques

Rubriques connexes :

- *Tableau de bord Système*, page 43
- *Tableau de bord Threats (Menaces)*, page 35
- *Tableau de bord Usage*, page 42
- *Ajout d'éléments dans un onglet du tableau de bord*, page 44

L'onglet **Risques** du Tableau de bord Web Security permet de surveiller les demandes d'URL autorisées et bloquées dans la classe Risques de sécurité. Les graphiques suivants s'affichent par défaut :

- Le graphique **30-Day Risk Trends (Tendance des risques sur 30 jours)** présente les tendances des requêtes bloquées pour des catégories de sécurité et de responsabilité légale spécifiques sur une période de 30 jours comprenant le jour en cours. Lorsque vous cliquez sur une courbe de tendances :
  - Pour les catégories liées à la sécurité (telles que Logiciels espions), le tableau de bord Threats (Menaces) s'affiche pour autoriser un examen plus poussé.
  - Pour les autres catégories (par exemple, Adulte), un rapport d'investigation s'affiche avec des informations plus détaillées.
- Le graphique **Clients with Security Risks (Clients présentant des risques de sécurité)** présente les ordinateurs qui ont accédé aux sites de la classe Risques de sécurité. Vous pouvez éventuellement vous assurer ensuite que ces ordinateurs ne sont pas infectés par des virus ou des logiciels espion.
- Le graphique **Top Security Risk Categories (Principales catégories de Risques de sécurité)** présente les catégories de Risques de sécurité ayant reçu le plus de demandes afin de vous aider à déterminer si vos stratégies de filtrage protègent efficacement votre réseau.
- Le graphique **Classes de risque** présente le nombre de requêtes autorisées et bloquées pour chaque classe de risque (voir *Classes de risque*, page 54) afin de vous aider à évaluer l'efficacité des stratégies existantes.
- Le graphique **Top Uncategorized (Principaux sites non catégorisés)** présente les URL non classées par la Base de données principale Websense que les utilisateurs consultent le plus souvent. Ouvrez la page **Tâches courantes > Recatégoriser l'URL** pour attribuer une URL à une catégorie filtrée.
- (*Web Security Gateway et Gateway Anywhere*) Le graphique **Analytics: Security Risks (Analyses : Risques de sécurité)** présente le nombre de requêtes que l'analyse Content Gateway a affecté à de nouvelles catégories parce que leur contenu a été modifié ou que leur site a été compromis.

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

Tableau de bord Usage

Rubriques connexes :

- *Tableau de bord Système*, page 43
- *Tableau de bord Risques*, page 41
- *Tableau de bord Threats (Menaces)*, page 35
- *Ajout d'éléments dans un onglet du tableau de bord*, page 44

L'onglet **Usage** de Web Security vous permet de surveiller les tendances générales de l'activité Internet dans votre organisation. Les graphiques suivants s'affichent par défaut :

- Le graphique **Top Blocked Users (Principaux utilisateurs bloqués)** présente les utilisateurs qui ont demandé le plus de sites bloqués.

- Le graphique **Top Requested Categories (Principales catégories demandées)** présente les catégories les plus demandées par les utilisateurs, en donnant des précisions sur les problèmes potentiels affectant la sécurité, la bande passante ou la productivité. Cliquez sur ce graphique pour afficher un rapport d'investigation et obtenir des informations détaillées.
- **Le graphique Enforcement Summary (Résumé de l'application)** présente les demandes récemment autorisées, les demandes récemment bloquées pour les sites appartenant à la classe Risques de sécurité et les autres demandes bloquées.
- (*Web Security Gateway et Gateway Anywhere*) Le graphique **Web 2.0 Categories (Catégories Web 2.0)** présente les principales catégories affectées aux URL Web 2.0 demandées, mesurées par requête.
- (*Web Security Gateway et Gateway Anywhere*) Le graphique **Web 2.0 URL Bandwidth (Bande passante : URL Web 2.0)** présente les URL Web 2.0 qui consomment le plus de bande passante.
- (*Web Security Gateway et Gateway Anywhere*) **Analytics: Top Categories (Analyses : Catégories principales)** présente les principales catégories auxquelles des URL ont été affectées après que l'analyse ait déterminé qu'elles ne convenaient plus à leur catégorie d'origine.

Cliquez sur un graphique ou un élément (sauf 30-Day Activity Summary (Synthèse d'activité sur 30 jours)) pour afficher un rapport d'investigation et obtenir des informations détaillées.

Tableau de bord Système

Rubriques connexes :

- *Tableau de bord Threats (Menaces)*, page 35
- *Tableau de bord Risques*, page 41
- *Tableau de bord Usage*, page 42
- *Ajout d'éléments dans un onglet du tableau de bord*, page 44

L'onglet **Système** du Tableau de bord Web Security vous permet de surveiller l'état de votre déploiement Web Security. Les éléments suivants s'affichent par défaut :

- L'élément **Health Alert Summary (Résumé sur les alertes d'état)** présente les messages d'alerte et d'état des composants Web Security. Si une erreur ou un avertissement s'affiche dans le résumé, cliquez sur le message d'alerte pour ouvrir la page Alertes, qui vous présente des informations plus détaillées (voir *Vérification de l'état actuel du système*, page 385).

  Les informations du Résumé sur les alertes d'état sont mises à jour toutes les 30 secondes.
- **Activité utilisateur : Zoom Trend : (Tendance - Zoom)** présente le volume de demandes Internet filtrées et traitées dans la Base de données d'activité pour la période sélectionnée.
  - Pour sélectionner une section du graphique et l'examiner de plus près, cliquez et faites glisser votre curseur. Vous pouvez effectuer cette opération à plusieurs reprises pour affiner encore davantage les périodes à examiner.

- Lorsque le zoom est maximal, un point de données s'affiche pour chaque période de 10 minutes (par exemple, 12:00:00, 12:10:00, 12:20:00).

  Dans la vue par défaut du graphique (macro), chaque point de données peut être basé sur un échantillon de plusieurs points de données à intervalle de 10 minutes au sein de la section sélectionnée dans le graphique. Par conséquent, il est possible que les chiffres indiqués dans la vue macro ne correspondent pas exactement à ceux indiqués pour un zoom inférieur.
- Cliquez sur **Zoom Out (Zoom arrière)** pour revenir à l'échelle précédente.
- Cliquez sur **Reset Chart (Réinitialiser le graphique)** pour revenir au niveau de détails par défaut.

- L'élément **Protocol Bandwidth Use (Bande passante par protocole)** présente les protocoles consommant le plus de bande passante au sein de votre réseau.
- L'élément **Filtering Service Status (État du service de filtrage)** présente l'état de chaque instance de Filtering Service associée au serveur Policy Server actuel.

  Cliquez sur l'adresse IP du service Filtering Service pour obtenir plus d'informations sur l'instance de ce service, notamment sur ses connexions à Network Agent et Content Gateway. Voir *Vérification des détails du service Filtering Service*, page 366.
- (*Web Security Gateway Anywhere*) **Hybrid Bandwidth Summary (Résumé de la bande passante hybride)** présente la bande passante consommée par les requêtes Internet des utilisateurs filtrés par le service hybride.
- (*Web Security Gateway Anywhere*) **Hybrid Requests (Requêtes hybrides)** présente le nombre de requêtes effectuées par les utilisateurs de votre organisation que le service hybride a autorisées ou bloquées.

Ajout d'éléments dans un onglet du tableau de bord

La page **État > Tableau de bord > Add Chart (Ajouter un graphique)** vous permet d'ajouter des éléments dans le tableau de bord Risques, Usage ou Système.

Notez que vous ne pouvez ni ajouter ni retirer des éléments dans le tableau de bord Menaces.

Pour commencer, servez-vous de la liste déroulante **Add elements to tab (Ajouter des éléments à un onglet)** pour sélectionner un onglet, puis sélectionnez l'élément à ajouter dans la liste **Éléments du tableau de bord**.

- Vous pouvez ajouter un élément dans n'importe quel onglet.
- Chaque onglet peut afficher jusqu'à 12 éléments.
- Les éléments déjà présents dans l'onglet sélectionné sont désignés par une icône en forme de cercle bleu.
- Vous pouvez ajouter plusieurs copies d'un même élément dans un onglet (par exemple, avec une période différente).

Lorsque vous sélectionnez un élément dans la liste, un exemple de ce dernier apparaît dans le panneau **Aperçu**. Vous pouvez utiliser le panneau d'aperçu pour modifier le **Nom** du graphique et, le cas échéant, le **Type de graphique**, la **Période** et la valeur **Top (Principales)** (par exemple, principales catégories 1 à 5 ou les 16 à 20 premiers utilisateurs).

- **Chart type (Type de graphique)** : la plupart des graphiques peuvent être affichés sous forme de courbes, colonnes et barres multi-séries ou d'histogramme empilés ou non. Certains peuvent être affichés sous forme de graphique à barres, de courbe ou de graphique en secteurs. Les différents types disponibles dépendent des données affichées.
- **Période** : la plupart des graphiques peuvent porter sur une période variable allant de la date du jour (période de 24 heures commençant à minuit le jour même) à 30 jours ou plus, en passant par les 7 derniers jours. Lorsque la période maximale des graphiques du tableau de bord est étendue, les graphiques peuvent également afficher les 180 ou 365 derniers jours.
  - Avec Microsoft SQL Server Express, la période maximale des graphiques du tableau de bord est de 30 jours et n'est pas modifiable.
  - L'utilisation de la période maximale par défaut (30 jours) peut améliorer les performances du tableau de bord.

  Pour plus d'informations sur l'extension de la période des graphiques du tableau de bord, consultez la section *Configuration des rapports du tableau de bord*, page 418.
- **Top (Principaux)** : les graphiques qui présentent des informations sur les principaux utilisateurs, les principales catégories, URL, etc., peuvent généralement afficher jusqu'à 5 valeurs. Vous pouvez choisir d'afficher les 5 valeurs principales ou les valeurs 6 à 10, 11 à 15 ou 16 à 20.

Lorsque vos modifications sont terminées, cliquez sur **Ajouter**. L'onglet du tableau de bord est immédiatement mis à jour.

Si vous avez déjà modifié un graphique et que vous souhaitez recommencer, cliquez sur **Restaurer les valeurs par défaut** pour réinitialiser la période, le type et les principales valeurs (le cas échéant) par défaut du graphique.

Deux éléments du tableau de bord ne s'affichent par défaut dans aucun onglet mais peuvent être ajoutés :

- **30-Day Value Estimates (Estimations des valeurs sur 30 jours)** permet d'évaluer les économies de temps et de bande passante réalisées grâce à Websense sur une période de 30 jours (date du jour comprise).

  Pour savoir comment l'estimation a été calculée, placez votre souris sur l'élément **Temps** ou **Bande passante** (sous Économies) (voir *Économies de temps et de bande passante*, page 45). Pour personnaliser le calcul, utilisez la page Add Charts (Ajouter des graphiques).
- **Activity Today (Activité du jour)** donne quelques exemples de la protection dont votre réseau a bénéficié le jour même grâce au filtrage Websense. Selon votre type d'abonnement, les informations peuvent porter sur les sites Malveillants, Adulte et Logiciels espions bloqués et sur les sites analysés ou analysés et recatégorisés par Content Gateway.

  Cet élément indique également le nombre total de requêtes traitées jusque-là, le nombre total de requêtes bloquées et le nombre de mises à jour de bases de données traitées en temps réel.

Économies de temps et de bande passante

Les solutions Websense Web Security permettent de réduire les pertes de temps et de bande passante associées aux activités Internet non productives.

Les **Estimations de l'utilité** ne s'affichent pas par défaut, mais peuvent être ajoutées dans le Tableau de bord Web Security afin d'évaluer les économies réalisées en termes de temps et de bande passante. Ces valeurs sont calculées comme suit :

- Économies de temps : multiplication du **temps moyen par visite** par le nombre de **sites bloqués**. Au départ, Websense utilise une valeur par défaut, telle que le nombre moyen de secondes qu'un utilisateur passe à consulter un site Web demandé. La valeur des sites bloqués représente le nombre total de demandes bloquées au cours de la période disponible (jusqu'à la période maximale configurée dans la page Paramètres > Génération de rapports > Tableau de bord).
- Économies de bande passante : multiplication de la **bande passante moyenne par visite** par le nombre de **sites bloqués**. Au départ, Websense utilise une valeur par défaut, telle que le nombre moyen d'octets consommés par le site Web moyen. La valeur des sites bloqués représente le nombre total de demandes bloquées au cours de la période disponible (jusqu'à la période maximale configurée dans la page Paramètres > Génération de rapports > Tableau de bord).

Pour voir comment une valeur est calculée, survolez son compteur avec votre souris. Pour modifier les chiffres utilisés par le calcul, cliquez sur **Add Charts (Ajouter des graphiques)** pour sélectionner le graphique **Value Estimates (Estimations de l'utilité)** dans la liste, puis saisissez les nouvelles mesures moyennes de temps et de bande passante à utiliser dans le calcul :

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

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir au tableau de bord.

Mode Status Monitor (Moniteur d'état) de Web Security

Pour des raisons de sécurité, une session TRITON - Web Security prend fin après 30 minutes d'inactivité. Vous pouvez toutefois passer en mode Status Monitor (Moniteur d'état) pour surveiller les données de filtrage et d'alerte sans que votre session n'expire.

- Pour passer en mode Status Monitor (Moniteur d'état) dans TRITON - Web Security, vous devez vous déconnecter des autres modules TRITON.
- En mode Status Monitor (Moniteur d'état), les informations des pages État > Tableau de bord, État > Alertes et Génération de rapports > Real-Time Monitor continuent à être mises à jour normalement jusqu'à ce que vous fermiez le navigateur ou que vous vous déconnectiez.

Pour passer en mode Status Monitor (Moniteur d’état), commencez par enregistrer ou annuler les modifications en cours, puis :

- Sélectionnez le mode **Status Monitor (Moniteur d’état)** dans la liste déroulante **Rôle** de la barre d’outils Web Security.
- Cliquez sur le bouton **Status Monitor (Moniteur d’état)** de la barre d’outils située en haut de la page État > Tableau de bord ou État > Alertes.

Pour arrêter la surveillance de l’état de Web Security, déconnectez-vous de TRITON - Web Security ou fermez votre navigateur.

3 Filtres de l’utilisation Internet

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 50
- *Fonctionnement des filtres*, page 59
- *Configuration des paramètres de filtrage de Websense*, page 67
- *Stratégies de filtrage Internet*, page 89
- *Réglage des stratégies de filtrage*, page 247

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

- **Filtres de catégories**, utilisés pour imposer des actions (autoriser, bloquer) sur des catégories de sites Web
- **Filtres de protocoles**, utilisés pour imposer des actions à des applications Internet et à des protocoles non HTTP

> **Remarque**
> Dans les environnements Websense Web Security Gateway Anywhere, le filtrage hybride n’impose pas l’application de filtres de protocoles.

- Un planning qui détermine à quel moment chaque filtre est imposé

Le filtrage basé sur les stratégies vous permet d’attribuer divers niveaux d’accès Internet à vos clients (par exemple, utilisateurs, groupes ou adresses IP de votre réseau). Commencez par créer des filtres pour définir des restrictions précises pour l’accès à Internet, puis exploitez ces filtres pour élaborer une stratégie.

Dans le cas d'une première installation, Websense crée une stratégie **Par défaut** et l'utilise pour commencer la surveillance des demandes Internet dès qu'une clé d'abonnement a été saisie (voir *La stratégie Par défaut*, page 90). Au départ, la stratégie par défaut autorise toutes les demandes.

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

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

- Un filtre de catégories bloquant l'accès à tous les sites Web à l'exception de ceux des catégories Commerce et économie, Enseignement et Actualités et médias
- Un second filtre de catégories autorisant tous les sites Web à l'exception de ceux qui constituent un risque pour la sécurité ou réservés aux adultes
- Un troisième filtre de catégories qui surveille l'accès aux sites Web sans les bloquer (voir *Création d'un filtre de catégories*, page 60)

Pour accompagner ces filtres de catégories, vous pouvez définir :

- Un filtre de protocoles qui bloque les groupes de protocoles Messagerie instantanée/ Chat, Partage de fichiers en P2P, Antiblocage de proxy et Médias en temps réel
- Un second filtre de protocoles qui autorise tous les protocoles non HTTP sauf ceux qui sont associés aux risques de sécurité et à l'antiblocage de proxy
- Un troisième filtre de protocoles qui autorise tous les protocoles non HTTP (voir *Création d'un filtre de protocoles*, page 63)

Dès que vous avez défini un jeu de filtres correspondant aux règles d'accès à Internet de votre organisation, vous pouvez les ajouter aux stratégies et les appliquer à vos clients (voir *Stratégies de filtrage Internet*, page 89).

Filtrage des catégories et des protocoles

La Base de données principale de Websense classe les sites Web similaires (identifiés par leurs URL et leurs adresses IP) dans des **catégories**. Chaque catégorie à un nom descriptif, tel que Section pour adultes, Jeux de hasard ou Partage de fichiers P2P. Vous pouvez également créer vos propres catégories personnalisées afin de regrouper des sites qui intéressent particulièrement votre organisation (voir *Création d'une catégorie personnalisée*, page 257). Combinées, les catégories de la Base de données principale et les catégories définies par l'utilisateur constituent la base du filtrage Internet.

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

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

websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

Pour suggérer l’ajout d’un site à la Base de données principale ou le déplacement d’un site dans une autre catégorie, cliquez sur **Suggérer une nouvelle catégorie** dans le panneau de raccourcis droit de TRITON - Web Security. Vous êtes alors invité(e) à vous connecter au portail MyWebsense, puis dirigé(e) vers l’outil de recherche, qui vous permet d’identifier la catégorie actuellement attribuée à un site et de demander une nouvelle catégorie.

Lorsque vous créez un **filtre de catégories** dans TRITON - Web Security, vous choisissez les catégories qui doivent être bloquées ou autorisées.

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

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

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

websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php

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

Remarque

Dans les déploiements Websense Web Filter et Web Security, l’agent Network Agent doit être installé pour que le filtrage à base de protocoles puisse s’effectuer.

Websense Web Security Gateway et Gateway Anywhere permettent de filtrer les protocoles non HTTP qui effectuent une mise en tunnel via les ports HTTP sans utiliser Network Agent. Pour plus d’informations, consultez *Détection des protocoles mis en tunnel*, page 186.

Dans les environnements Websense Web Security Gateway Anywhere, le filtrage hybride n’impose pas l’application des filtres de protocoles.

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

Nouvelles catégories et nouveaux protocoles de la Base de données principale

Lorsque de nouveaux protocoles et de nouvelles catégories sont ajoutés à la base de données principale, une action de filtrage par défaut est affectée à chacun d'eux, par exemple **Autoriser** ou **Bloquer** (voir *Actions de filtrage*, page 57).

- L'action par défaut est appliquée dans tous les filtres actifs de catégories et de protocoles (voir *Fonctionnement des filtres*, page 59). Pour modifier le mode de filtrage des catégories ou des protocoles, vous pouvez :
  - Modifier chaque filtre actif individuellement. Utilisez cette option lorsque vous voulez attribuer aux différents groupes de clients des niveaux d'accès distincts à cette catégorie ou ce protocole.
  - Modifier les attributs de la catégorie ou du protocole pour appliquer la même action dans tous les filtres. Voir *Modification du filtrage global des catégories*, page 256, et *Modification du filtrage global des protocoles*, page 267.
- L'action par défaut repose sur le renvoi d'informations relatives au caractère professionnel approprié des sites ou des protocoles concernés.

Vous pouvez également configurer Websense de sorte qu'il génère une alerte système et vous avertisse à chaque ajout de nouvelles catégories ou de nouveaux protocoles dans la base de données principale. Pour plus d'informations, consultez *Alertes*, page 377.

Catégories spéciales

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

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

  Les mises à jour de la catégorie Événements spéciaux sont ajoutées dans la base de données principale pendant les téléchargements planifiés. Les sites sont ajoutés dans cette catégorie pour une courte période, après quoi ils sont soit déplacés vers une autre catégorie, soit retirés de la base de données principale.
- La catégorie **Productivité** a pour objectif d'éviter les comportements générant des pertes de temps.
  - Publicités
  - Téléchargement de logiciels et de freewares
  - Messagerie instantanée
  - Tableaux d'affichage et forums électroniques
  - Courtage en ligne
  - Sites rémunérateurs
- La catégorie **Largeur de bande** a pour objectif d'économiser la bande passante du réseau.
  - Vidéo de formation

- Vidéo de divertissement
- Radio et TV sur Internet
- Téléphonie Internet
- Partage de fichiers en P2P
- Stockage/Sauvegarde réseau personnels
- Médias en temps réel
- Surveillance
- Vidéo virale

Websense Web Security, Web Security Gateway et Web Security Gateway Anywhere incluent des catégories de sécurité supplémentaires :

- La catégorie **Sécurité** se concentre sur les sites Internet qui contiennent du code malveillant, capable de contourner les logiciels antivirus.
  - Commande et contrôle malveillants avancés (requiert Content Gateway)
  - Contenu malveillant avancé (requiert Content Gateway)
  - Réseaux zombies
  - Chargements avec cryptage personnalisé (requiert Content Gateway)
  - Fichiers contenant des mots de passe (requiert Content Gateway)
  - Enregistreurs de frappe
  - Contenu iFrame avec code malveillant
  - Lien contenant du code malveillant
  - Sites Web dangereux
  - Phishing et autres escroqueries
  - Documents potentiellement exploités (requiert Content Gateway)
  - Logiciels indésirables
  - Logiciels espion
  - Lien vers du contenu suspect
- **Protection étendue** se concentre sur les sites Web potentiellement malveillants.
  - **DNS dynamique** inclut les sites qui masquent leur identité à l’aide de services DNS dynamiques, souvent associés à des menaces persistantes et sophistiquées.
  - **Exposition élevée** contient des sites qui masquent leur vraie nature ou leur véritable identité, ou qui incluent des éléments suggérant un objectif malveillant latent.
  - **Nouvelles exploitations** contient des sites connus pour héberger du code d’exploit connu et potentiel.
  - **Contenu à risques** regroupe des sites susceptibles de renfermer du contenu inutile ou peu utile.

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

Lorsque les chercheurs en sécurité de Websense détectent une menace potentielle dans un site, celui-ci est ajouté dans la catégorie Protection étendue jusqu'à ce que nos chercheurs soient sûrs à 100 % de la catégorisation finale de ce site.

Classes de risque

Rubriques connexes :

- *Attribution de catégories aux classes de risque*, page 396
- *Rapports de présentation*, page 131
- *Rapports d'investigation*, page 152

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

Les classes de risques sont essentiellement utilisées dans la génération des rapports. Certains graphiques du Tableau de bord Web Security illustrent l'activité Internet par classe de risques et vous permettent de générer une présentation ou des rapports d'investigation triés par classe de risques.

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

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

- Une catégorie peut apparaître dans plusieurs classes de risques ou n'être attribuée à aucune.
- Les regroupements peuvent changer régulièrement dans la base de données principale. Lorsqu'une notification vous signale l'ajout d'une nouvelle catégorie dans la Base de données principale, il est généralement utile d'en vérifier l'affectation de classe par défaut.

Responsabilité légale

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

Largeur de bande > Partage de fichiers en P2P

Jeux de hasard

Illégal ou douteux

Technologies de l'information > Piratage et Antiblocage par proxy

Militantisme, extrémisme

Racisme, haine

Mauvais goût

Violence

Armes

Perte de bande passante réseau

Largeur de bande (y compris Vidéo de formation, Vidéo de divertissement, Radio et TV sur Internet, Téléphonie Internet, Partage de fichiers en P2P, Stockage/Sauvegarde réseau personnels, Médias en temps réel, Surveillance et Vidéo virale)

Divertissement > Services de téléchargement MP3 et audio

Productivité > Publicités, Téléchargement de logiciels et de freewares

Contrôles du Web social - Facebook > Chargement de vidéos Facebook

Contrôles du Web social - YouTube > Chargement de vidéos YouTube

Utilisation professionnelle

Bande passante > Vidéo de formation

Commerce et économie (y compris Services Financiers, Applications métier hébergées)

Enseignement > Matériaux éducatifs, Matériaux de référence

Gouvernement (y compris Armée)

Contrôles du Web social - LinkedIn (y compris Connexions LinkedIn, Carrière LinkedIn, Courrier LinkedIn, Mises à jour LinkedIn)

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

Voyage

Véhicules

Risques pour la sécurité

Largeur de bande > Partage de fichiers en P2P

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

Technologies de l'information > Piratage, Antiblocage par proxy, Web et courrier indésirable

Domaine mis à l'écart

Productivité >Téléchargement de logiciels et de freewares

Sécurité (y compris Réseaux « zombies », Enregistreurs de frappe, Contenu iFrame avec code malveillant, Lien vers du code malveillant, Sites Web dangereux, Phishing et autres escroqueries, Logiciels potentiellement indésirables, Logiciels espion, Lien vers du contenu suspect) [*Websense Web Security*]

Commande et contrôle malveillants avancés, Contenu malveillant avancé, Chargements avec cryptage personnalisé, Fichiers contenant des mots de passe et Documents potentiellement exploités sont également inclus avec Web Security Gateway et Gateway Anywhere.

Perte de productivité

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

Section pour adultes > Éducation sexuelle

Groupes activistes/Associations

Bande passante > Vidéo de divertissement, Radio et TV sur Internet, Partage de fichiers en P2P, Médias en temps réel, Surveillance et Vidéo virale

Perte de productivité

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

Enseignement (y compris Institutions culturelles et Institutions scolaires)

Divertissement (y compris Services de téléchargement MP3 et audio)

Jeux de hasard

Jeux

Gouvernement > Partis politiques

Santé

Technologies de l'information > Web et courrier indésirable, Hébergement Web

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

Recherche d'emploi

Actualités et médias (y compris Journaux alternatifs)

Domaine mis à l'écart

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

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

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

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

Contrôles du Web social - Facebook (y compris Facebook Apps, Facebook Chat, Commentaires Facebook, Événements Facebook, Amis Facebook, Jeux Facebook, Groupes Facebook, Courrier Facebook, Chargement de photo Facebook, Publication Facebook, Questions Facebook, Chargement de vidéo Facebook)

Contrôles du Web social - LinkedIn (y compris Connexions LinkedIn, Carrière LinkedIn, Messagerie LinkedIn, Mises à jour LinkedIn)

Contrôles du Web social - Twitter (y compris Suivi Twitter, Courrier Twitter, Publication Twitter)

Contrôles du Web social - Divers (y compris Publication Craigslist, Commentaires WordPress, Publication WordPress)

Contrôles du Web social - YouTube (y compris Commentaires YouTube, Partage YouTube, Chargement de vidéo YouTube)

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

Événements spéciaux

Sports (y compris Chasse, clubs de tir)

Voyage

Véhicules

Les Super administrateurs peuvent modifier les catégories attribuées à chaque classe de risques à la page **Paramètres > Général > Classe de risques** (voir *Attribution de catégories aux classes de risque*, page 396).

Groupes de protocoles de sécurité

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

- Le groupe de protocoles **Trafic malveillant** comprend le protocole **Réseaux zombies**, conçu pour bloquer le trafic de contrôle et de commande généré par un « bot » tentant de se connecter par le biais d'un réseau « zombie » à des fins malveillantes.
- Le groupe de protocoles **Trafic malveillant (Blocage impossible)** sert à identifier le trafic susceptible d'être associé à du code malveillant.
  - **Vers de messagerie** surveille le trafic SMTP sortant susceptible d'être généré par une attaque de vers de messagerie.
  - **Autre** surveille le trafic entrant ou sortant susceptible d'être lié à des applications malveillantes.

Le groupe de protocoles Trafic malveillant est bloqué par défaut et peut être configuré dans vos filtres de protocoles (voir *Modification d'un filtre de protocoles*, page 64). Les protocoles Trafic malveillant (Blocage impossible) peuvent être journalisés pour la génération de rapports, mais aucune autre action de filtrage ne peut être appliquée.

Actions de filtrage

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

- **Bloquer** la demande. Les utilisateurs reçoivent une page ou un message de blocage et ne peuvent pas afficher le site ou exploiter l'application Internet.
- **Autoriser** la demande. Les utilisateurs peuvent afficher le site ou exploiter l'application Internet.
- Évaluer l'utilisation actuelle de la **Bande passante** avant de bloquer ou d'autoriser la demande. Lorsque cette action est activée et que l'utilisation de la bande passante atteint un seuil défini, les prochaines demandes Internet pour une catégorie ou un protocole spécifique sont bloquées. Voir *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.

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

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

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

  Le délai par défaut peut être modifié à la page **Paramètres** > **Général** > **Filtrage**.

- **Contingent** : les utilisateurs reçoivent une page de blocage qui leur demande s'ils souhaitent utiliser du temps contingenté pour consulter ce site. Si l'utilisateur clique sur **Utiliser du temps contingenté**, il peut consulter le site.

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

  - Si l'utilisateur demande d'autres sites de temps contingenté pendant une période de **session** par défaut (10 minutes par défaut), il peut consulter ces sites sans recevoir d'autres pages de blocage.
  - Le temps contingenté **total** est affecté quotidiennement. Une fois écoulé, chaque client doit attendre le jour suivant pour accéder au site des catégories de temps contingenté. Le temps contingenté quotidien par défaut (60 minutes) est défini à la page **Paramètres** > **Général** > **Filtrage**. Les affectations de temps contingenté quotidien peuvent également être accordées aux clients sur une base individuelle. Pour plus d'informations, consultez *Utilisation de temps contingenté pour limiter l'accès à Internet*, page 58.

Important

Dans les déploiements Filtering Service multiples, Websense State Server est requis pour que l'application des actions Confirmer et Contingent s'effectue correctement. Pour plus d'informations, consultez *Policy Server, Filtering Service et State Server*, page 368.

- **Bloquer des mots-clés** : lorsque vous définissez des mots-clés et activez leur blocage, les utilisateurs qui demandent un site dont l'URL contient un mot-clé bloqué ne peuvent pas y accéder. Voir *Filtrage par mots-clés*, page 258.
- **Bloquer des types de fichiers** : lorsque le blocage de types de fichiers est activé, les utilisateurs qui tentent de télécharger un fichier dont le type est bloqué reçoivent une page de blocage et ce fichier n'est pas téléchargé. Voir *Gestion du trafic en fonction du type de fichiers*, page 273.

Utilisation de temps contingenté pour limiter l'accès à Internet

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

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

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

1. L'utilisateur
2. L'ordinateur ou le client réseau

3. Les groupes auxquels l'utilisateur appartient

   Si l'utilisateur est membre de plusieurs groupes, Websense accorde le temps contingenté en fonction du paramètre **Utiliser un blocage plus restrictif** de la page **Paramètres > Général > Filtrage** (voir *Configuration des paramètres de filtrage de Websense*, page 67).

4. Le temps contingenté par défaut

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

Cela est dû au fait que les applets sont entièrement téléchargées dans les ordinateurs client et s'exécutent comme les applications, sans nouvel échange avec le serveur hôte d'origine. Toutefois, si l'utilisateur clique sur le bouton Actualiser du navigateur, Websense détecte la communication au serveur hôte et bloque la demande en fonction des restrictions de temps contingenté applicables.

Filtrage de la recherche

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

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

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

Websense, Inc. gère une base de données de moteurs de recherche prenant en charge les capacités de filtrage des recherches. Lorsqu'un moteur de recherche est ajouté ou supprimé dans la base de données, une alerte est générée (voir *Alertes*, page 377).

Le filtrage des recherches est activé dans la page **Paramètres > Général > Filtrage**. Pour plus d'informations, consultez *Configuration des paramètres de filtrage de Websense*, page 67.

Fonctionnement des filtres

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 50
- *Stratégies de filtrage Internet*, page 89
- *Création d'un filtre de catégories*, page 60
- *Création d'un filtre de protocoles*, page 63
- *Création d'un filtre d'accès limité*, page 249

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

La page Filtres comprend 3 sections principales :

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

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

  Websense Web Security Gateway permet de filtrer les protocoles non HTTP qui effectuent une mise en tunnel via les ports HTTP sans utiliser Network Agent. Pour plus d'informations, consultez *Détection des protocoles mis en tunnel*, page 186.

  Dans les environnements Websense Web Security Gateway Anywhere, le service hybride ne filtre pas les protocoles.
- Les **Filtres d'accès limité** définissent une liste restrictive de sites Web autorisés (voir *Limitation des utilisateurs à une liste définie d'URL*, page 247).

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

- Pour revoir ou modifier un filtre existant de catégories, de protocoles ou d'accès limité, cliquez sur son nom. Pour plus d'informations, consultez les sections suivantes :
  - *Modification d'un filtre de catégories*, page 61
  - *Modification d'un filtre de protocoles*, page 64
  - *Modification d'un filtre d'accès limité*, page 250
- Pour créer un nouveau filtre de catégories, de protocoles ou d'accès limité, cliquez sur **Ajouter**. Pour plus d'informations, consultez les sections suivantes :
  - *Création d'un filtre de catégories*, page 60
  - *Création d'un filtre de protocoles*, page 63
  - *Création d'un filtre d'accès limité*, page 249

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

Si vous avez créé des rôles d'administration déléguée (voir *Administration déléguée et génération de rapports*, page 323), les Super administrateurs peuvent copier les filtres qu'ils ont créés pour d'autres rôles afin que les administrateurs délégués puissent les exploiter.

Pour copier des filtres pour un autre rôle, cochez la case accolée à leur nom, puis cliquez sur **Copier dans le rôle**. Pour plus d'informations, consultez *Copie de filtres et de stratégies vers des rôles*, page 252.

Création d'un filtre de catégories

Rubriques connexes :

- *Fonctionnement des filtres*, page 59
- *Modification d'un filtre de catégories*, page 61

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

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

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

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

   Les restrictions de caractères qui s'appliquent aux noms des filtres s'appliquent également à leurs descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).
3. Sélectionnez une entrée dans la liste déroulante pour choisir d'utiliser un modèle ou de copier un filtre existant. Pour plus d'informations sur les modèles, consultez *Modèles de filtres de catégories et de protocoles*, page 66.
4. Pour voir et modifier le nouveau filtre, cliquez sur **OK**. Le filtre est ajouté dans la liste **Filtres de catégories** de la page Filtres.

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

Modification d'un filtre de catégories

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 50
- *Actions de filtrage*, page 57
- *Utilisation de temps contingenté pour limiter l'accès à Internet*, page 58
- *Fonctionnement des filtres*, page 59
- *Fonctionnement des catégories*, page 254

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

Important

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

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

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

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

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

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

1. Sélectionnez une entrée dans la liste **Catégories** pour voir des informations sur cette catégorie ou pour modifier l'action de filtrage qui lui est associée.
2. Avant de modifier l'action appliquée à une catégorie, utilisez la section des détails (à droite de la liste Catégories) pour vérifier les attributs spéciaux associés à cette catégorie.
   - Pour afficher la liste des URL recatégorisées éventuellement affectées à la catégorie, cliquez sur **Afficher les URL personnalisées dans cette catégorie**. Voir *Redéfinition du filtrage pour des sites spécifiques*, page 260.
   - Pour afficher la liste des mots-clés affectés à la catégorie, cliquez sur **Afficher les mots-clés dans cette catégorie**. Voir *Filtrage par mots-clés*, page 258.
   - Pour afficher la liste des expressions régulières utilisées pour définir des URL personnalisées ou des mots-clés pour cette catégorie, cliquez sur **Afficher les expressions régulières dans cette catégorie**.
3. Servez-vous des boutons situés au bas de la liste des catégories pour modifier l'action appliquée à la catégorie sélectionnée. Pour plus d'informations sur les actions disponibles, consultez *Actions de filtrage*, page 57.

   Les administrateurs délégués ne peuvent pas modifier l'action affectée aux catégories verrouillées par un Super administrateur.
4. Servez-vous des cases à cocher situées au bas de la liste Catégories pour appliquer des actions de filtrage avancées à la catégorie sélectionnée :
   - Pour modifier la façon dont les mots-clés sont utilisés dans le filtrage de la catégorie sélectionnée, activez ou désactivez la case à cocher **Bloquer des mots-clés**. *Filtrage par mots-clés*, page 258
   - Pour indiquer si les utilisateurs peuvent accéder à certains types de fichiers provenant des sites de la catégorie sélectionnée, activez ou désactivez la case à cocher **Bloquer des types de fichiers**. Voir *Gestion du trafic en fonction du type de fichiers*, page 273.

     Si vous avez choisi de bloquer certains types de fichiers, sélectionnez un ou plusieurs types de fichiers à bloquer.

     Pour appliquer les paramètres de types de fichiers sélectionnés à l'ensemble des catégories autorisées dans le filtre, cliquez sur **Apply to All Categories (Appliquer à toutes les catégories)**.

> **Warning**
>
> Avec Websense Web Security Gateway et Gateway Anywhere, l'application du blocage des types de fichiers à toutes les catégories peut fortement affecter les performances.
>
> Tous les fichiers dont l'extension ne correspond pas au type bloqué sont analysés de sorte que le véritable type de fichier soit identifié, y compris les fichiers texte tels que les fichiers HTML et CSS.

- Pour spécifier si l'accès au site de la catégorie est limité en fonction de certains seuils de bande passante, activez ou désactivez la case à cocher **Bloquer avec Bandwidth Optimizer**. Voir *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.

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

  Pour appliquer les paramètres de bande passante sélectionnés à l'ensemble des catégories autorisées dans le filtre, cliquez sur **Apply to All Categories (Appliquer à toutes les catégories)**.

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

Pour activer un nouveau filtre de catégories, ajoutez-le à une stratégie et attribuez cette dernière à des clients. Voir *Stratégies de filtrage Internet*, page 89.

Création d'un filtre de protocoles

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 50
- *Actions de filtrage*, page 57
- *Modification d'un filtre de protocoles*, page 64
- *Fonctionnement des protocoles*, page 264

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

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

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

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

   Les restrictions de caractères qui s'appliquent aux noms des filtres s'appliquent également à leurs descriptions, à deux exceptions près : Les descriptions peuvent inclure des points (.) et des virgules (,).
3. Sélectionnez une entrée dans la liste déroulante pour choisir d'utiliser un modèle (voir *Modèles de filtres de catégories et de protocoles*, page 66) ou de copier un filtre existant.
4. Pour voir et modifier le nouveau filtre, cliquez sur **OK**. Le filtre est ajouté dans la liste **Filtres de protocoles** de la page Filtres.

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

Modification d’un filtre de protocoles

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 50
- *Création d’un filtre de protocoles*, page 63
- *Actions de filtrage*, page 57
- *Fonctionnement des protocoles*, page 264
- *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270

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

Important

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

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

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

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

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

La partie inférieure de la page présente la liste des protocoles et les actions actuellement appliquées à chacun d’eux.

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

1. Sélectionnez un protocole dans la liste **Protocoles**. Les actions de filtrage avancées liées au protocole sélectionné s’affichent à droite de la liste.

2. Servez-vous des boutons **Autoriser** et **Bloquer** situés au bas de la liste Protocoles pour modifier l'action appliquée au protocole sélectionné.

   > **Remarque**
   >
   > Websense peut bloquer les demandes de protocole de type TCP, mais pas celles de type UDP.
   >
   > Certaines applications utilisent à la fois des messages de type TCP et UDP. Si une demande initiale d'application est effectuée sur le réseau via TCP, mais que les données suivantes sont envoyées via UDP, Websense bloque la demande TCP initiale, puis le trafic UDP qui s'ensuit.
   >
   > Les demandes UDP peuvent être journalisées comme bloquées, même lorsqu'elles sont autorisées.

   Pour appliquer la même action aux autres protocoles du groupe de protocoles sélectionné, cliquez sur **Appliquer au groupe**.

3. Si vous souhaitez que les informations relatives à l'utilisation du protocole sélectionné soient disponibles pour les alertes ou les rapports, cochez la case **Journaliser les données de protocole**.
4. Pour imposer des limites de bande passante à l'utilisation de ce protocole, cliquez sur **Bloquer avec Bandwidth Optimizer** et définissez les seuils de bande passante à utiliser. Pour plus d'informations, consultez *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.
5. Après avoir modifié le filtre, cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Filtres. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Pour activer un nouveau filtre de protocoles, ajoutez-le à une stratégie et attribuez cette dernière à des clients (voir *Stratégies de filtrage Internet*, page 89).

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

Filtres de catégories et de protocoles définis par Websense

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

Les filtres de catégories prédéfinis sont :

- De base

- Sécurité de base
- Bloquer tout
- Par défaut
- Surveiller uniquement
- Autoriser tout
- Strict Security (Sécurité stricte)

Les filtres de catégories Bloquer tout et Autoriser tout n'apparaissent pas dans la liste de la page Filtres, mais peuvent être ajoutés à des stratégies. Ces filtres jouent un rôle particulier dans le filtrage et ne peuvent être ni supprimés ni modifiés. Lorsqu'une demande Internet est filtrée, Websense commence par vérifier si le filtre Bloquer tout ou Autoriser tout s'applique, avant de vérifier les autres filtres (voir *Filtrage d'un site*, page 98).

Les filtres de protocoles prédéfinis sont :

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

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

Les filtres de catégories et de protocoles Par défaut peuvent être modifiés, mais ne peuvent pas être supprimés. Dans les environnements mis à niveau, si la stratégie Par défaut présente des différences, les filtres Par défaut sont utilisés pour filtrer les demandes pendant les périodes auxquelles aucun filtre n'est appliqué.

Modèles de filtres de catégories et de protocoles

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

Websense comprend 5 modèles de filtres de catégories :

- **Surveiller uniquement** et **Autoriser tout** autorisent toutes les catégories.
- **Bloquer tout** bloque toutes les catégories.
- **De base** bloque les catégories généralement bloquées et autorise le reste.
- **Par défaut** applique les actions Bloquer, Autoriser, Continuer et Contingent aux catégories.
- **Strict Security (Sécurité stricte)** étend le modèle Par défaut en bloquant deux autres catégories de sécurité et en ajoutant le type de fichier des exécutables dans une troisième catégorie.
- **Sécurité de base** bloque uniquement les catégories par défaut de la classe Risques de sécurité (voir *Classes de risque*, page 54).

Websense comprend également 3 modèles de filtres de protocoles :

- **Surveiller uniquement** et **Autoriser tout** autorisent tous les protocoles.

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

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

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

Pour obtenir des instructions sur l'utilisation d'un modèle pour créer un nouveau filtre, consultez les sections *Création d'un filtre de catégories*, page 60, et *Création d'un filtre de protocoles*, page 63.

Configuration des paramètres de filtrage de Websense

Rubriques connexes :

- *Filtrage des catégories et des protocoles*, page 50
- *Pages de blocage*, page 115
- *Accès par mot de passe*, page 84
- *Remplacement de compte*, page 84
- *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270
- *Filtrage par mots-clés*, page 258

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

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

1. Pour spécifier comment les utilisateurs sont filtrés lorsque plusieurs stratégies de groupe s'appliquent, activez ou désactivez l'option **Utiliser la stratégie de groupe la plus restrictive** (voir *Ordre du filtrage*, page 95).
   - Lorsque cette option est activée, la stratégie assurant le filtrage le plus restrictif est utilisée. En d'autres termes, si une stratégie de groupe applicable bloque l'accès à une catégorie alors qu'une autre en autorise l'accès, la demande de l'utilisateur pour un site de cette catégorie est bloquée.
   - Lorsque cette option n'est pas activée, le paramètre le plus permissif est utilisé.

2. Sélectionnez l'une des **options de recherche de mots-clés** suivantes (voir *Filtrage par mots-clés*, page 258).

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

3. Dans le champ **Délai d'attente d'accès par mot de passe**, entrez le nombre maximal de secondes (3600 au maximum, 60 par défaut) pendant lesquelles un utilisateur peut accéder aux sites de toutes les catégories après avoir sélectionné un accès par mot de passe (voir *Accès par mot de passe*, page 84).
4. Dans le champ **Délai de prolongation**, entrez le nombre maximal de secondes (3600 au maximum, 60 par défaut) pendant lesquelles un utilisateur qui clique sur Continuer peut accéder aux sites des catégories régies par l'action Confirmer (voir *Actions de filtrage*, page 57).
5. Dans le champ **Account override timeout (Expiration du remplacement de compte)**, saisissez le délai maximal en minutes (jusqu'à 3 600, par défaut 5) pendant lequel l'utilisateur est filtré par la stratégie affectée au compte de remplacement (voir *Remplacement de compte*, page 84).
6. Dans le champ **Durée de la session de temps contingenté**, entrez l'intervalle (60 minutes maximum, 10 par défaut) durant lequel les utilisateurs peuvent visiter les sites des catégories limitées par du temps contingenté (voir *Utilisation de temps contingenté pour limiter l'accès à Internet*, page 58).

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

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

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

Sous **State Server**, indiquez l'**adresse IPv4 ou le nom d'hôte** et le **Port** lorsque :

- Votre environnement inclut plusieurs instances de Websense Filtering Service, et
- Vous utilisez les actions de temps contingenté ou de confirmation, l'accès par mot de passe ou le remplacement de compte.

State Server suit les sessions de temps contingenté, de confirmation, d'accès par mot de passe et de remplacement de compte des clients pour vérifier que les durées de session sont correctement affectées aux différentes instances de Filtering Service (voir *Policy Server, Filtering Service et State Server*, page 368).

Après avoir saisi les détails de connexion à State Server, cliquez sur **Vérifier l'état** pour vérifier la connexion. Configurez les informations de connexion à State Server pour chaque instance de Policy Server présente dans votre déploiement.

Sous **Bandwidth Optimizer**, entrez les informations nécessaires pour filtrer l'utilisation d'Internet en fonction de la bande passante disponible. Pour plus d'informations sur le filtrage basé sur la bande passante, consultez *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.

> **Remarque**
>
> Dans les environnements Websense Web Security Gateway Anywhere, le filtrage hybride n'utilise pas les paramètres Bandwidth Optimizer. Les demandes qui passent par le service hybride ne sont pas limitées en fonction de la bande passante.

1. Pour spécifier un **débit de connexion à Internet**, procédez de l'une des manières suivantes :
   - Sélectionnez un débit standard dans la liste déroulante.
   - Entrez le débit du réseau en Kbits/s dans le champ de texte.
2. Saisissez les seuils à appliquer par défaut lorsque le filtrage basé sur la bande passante est utilisé. Notez que, lorsque des seuils sont définis alors qu'aucun filtre de catégories ou de protocoles n'impose le filtrage basé sur la bande passante, l'utilisation de la bande passante n'est pas limitée.
   - **Réseau** : lorsque le trafic réseau total atteint ce pourcentage de bande passante totale disponible, commence à imposer le filtrage basé sur la bande passante, conformément à la configuration des filtres actifs.
   - **Protocole** : lorsque le trafic associé à un protocole spécifique (tel que HTTP ou MSN Messenger) atteint ce pourcentage de bande passante totale disponible, commence à limiter l'accès à ce protocole, conformément à la configuration des filtres actifs.
3. (*Websense Web Security Gateway*) Content Gateway peut collecter des informations sur la bande passante consommée par le trafic HTTP et les protocoles qui effectuent une mise en tunnel via HTTP en vue d'une utilisation dans les rapports. Pour activer cette option, cochez la case **Include bandwidth data collected by Websense Content Gateway (Inclure les données de bande passante collectées par Websense Content Gateway)**.

Utilisez la section **Messages de blocage** pour saisir l'URL ou le chemin de la page de blocage HTML alternative que vous avez créée pour le cadre supérieur des messages de blocage de type navigateur (voir *Création de messages de blocage alternatifs*, page 125) ou pour configurer Websense Web Security Gateway Anywhere de sorte qu'un lien conduisant à ACEInsight soit inclus dans les pages de blocage.

- Des pages distinctes peuvent être utilisées pour les différents protocoles : **FTP**, **HTTP** (y compris **HTTPS**) et **Gopher**.

  Pour utiliser le message de blocage par défaut fourni par Websense, ou une version personnalisée de ce message, ne renseignez pas ces champs (voir *Personnalisation du message de blocage*, page 121).

- Dans les environnements Websense Web Security Gateway Anywhere :
  - Les messages de blocage personnalisés définis dans les champs ci-dessus ne s'appliquent pas aux demandes envoyées au filtrage hybride.

    À la place, utilisez la page Paramètres > Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur) pour personnaliser la page de blocage hybride (voir *Personnalisation des pages de blocage du service hybride*, page 217).
  - Lorsqu'un utilisateur clique sur le lien ACEInsight, l'URL à laquelle l'utilisateur tente d'accéder est envoyée à ACEInsight et une page Web présente l'analyse ACEInsight.

    L'URL envoyée à ACEInsight est tronquée pour ne pas inclure la chaîne CGI (susceptible de comprendre un nom d'utilisateur ou un mot de passe). Par conséquent, ACEInsight n'analyse pas le contenu protégé par mot de passe et peut renvoyer des résultats différents de ceux de Content Gateway.

    Le lien ACEInsight ne s'affiche pas dans les pages de blocage hybride.

Sous **Filtrage de la recherche**, sélectionnez **Activer le filtrage de la recherche** afin que Websense active un paramètre intégré à certains moteurs de recherche, de sorte que les images miniatures et autres contenus explicites associés à des sites bloqués ne s'affichent pas dans les résultats de la recherche (voir *Filtrage de la recherche*, page 59).

Les moteurs de recherche qui prennent cette fonction en charge s'affichent au-dessous de la case à cocher.

Lorsque la configuration des paramètres du filtrage est terminée, cliquez sur **OK** pour mettre en cache les modifications apportées. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

4 Clients

Vous pouvez personnaliser la manière dont Websense filtre les demandes provenant d'utilisateurs ou d'ordinateurs spécifiques en les ajoutant en tant que **clients** dans TRITON - Web Security. Si vous utilisez le filtrage Web sur site, vos clients peuvent être :

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

> **Remarque**
>
> Dans les déploiements Websense Web Security Gateway Anywhere, le filtrage hybride peut appliquer des stratégies aux utilisateurs ou aux groupes, et aux emplacements filtrés (voir *Fonctionnement des clients du filtrage hybride*, page 86).

Au départ, Websense filtre tous les clients de la même manière, à l'aide de la stratégie **Par défaut** (voir *La stratégie Par défaut*, page 90). Lorsque vous ajoutez un client dans la page Clients de TRITON - Web Security, vous pouvez lui affecter une stratégie de filtrage spécifique.

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

1. Application de la stratégie attribuée à **l'utilisateur** à l'origine de la demande. Si cette stratégie n'a pas de filtre planifié au moment de la demande, la prochaine stratégie applicable est utilisée.
2. Lorsque aucune stratégie spécifique à l'utilisateur n'est détectée, ou lorsque la stratégie ne présente pas de filtre actif au moment de la demande, le système recherche une stratégie attribuée à **l'ordinateur** (en premier) ou au **réseau** (en second) d'où provient la demande.
3. Lorsque aucune stratégie spécifique à l'ordinateur ou au réseau n'est détectée, ou lorsque la stratégie ne présente pas de filtre actif au moment de la demande, le système recherche une stratégie attribuée à un **groupe** auquel l'utilisateur appartient. Si l'utilisateur appartient à plusieurs groupes, Websense tient compte de toutes les stratégies de groupes qui s'appliquent (voir *Ordre du filtrage*, page 95).
4. En l'absence d'une stratégie de groupe, le système recherche une stratégie affectée au **domaine** (UO) de l'utilisateur.
5. Lorsque aucune stratégie applicable n'est détectée, ou lorsque la stratégie ne présente pas de filtre de catégories au moment de la demande, le système applique la stratégie **Par défaut** affectée au rôle attribué au client.

Pour plus d'informations sur le traitement des requêtes par Websense Filtering Service, consultez la section *Filtrage d'un site*, page 98.

Pour des informations sur la configuration de Filtering Service pour établir les priorités entre les stratégies de groupes et de domaines par rapport aux stratégies à base d'adresses IP (ordinateurs et réseaux), consultez la section *Priorités des stratégies de groupe et de domaine*, page 97.

Pour des informations sur l'application des stratégies de filtrage aux clients par le service hybride, consultez la section *Ordre du filtrage*, page 95.

Fonctionnement des clients

Rubriques connexes :

- *Clients*, page 71
- *Fonctionnement avec des ordinateurs et des réseaux*, page 73
- *Fonctionnement avec des utilisateurs et des groupes*, page 74
- *Ajout d'un client*, page 81
- *Modifications des paramètres des clients*, page 83

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

Si vous êtes administrateur délégué, ajoutez des clients dans la page Clients à partir de la liste de vos clients gérés. Ceci vous permet d'appliquer des stratégies aux clients. Pour obtenir des instructions, consultez la section *Ajout d'un client*, page 81.

Les clients sont divisés en 3 groupes :

- **Annuaire**, qui comprend les utilisateurs, les groupes et les domaines (UO) de votre service d'annuaire (voir *Fonctionnement avec des utilisateurs et des groupes*, page 74)
- **Réseaux**, plages d'adresses IPv4 ou IPv6 au sein du réseau filtré pouvant être gérées par une seule et même stratégie (voir *Fonctionnement avec des ordinateurs et des réseaux*, page 73)
- **Ordinateurs**, ordinateurs individuels du réseau filtré, identifiés par leur adresse IPv4 ou IPv6 (voir *Fonctionnement avec des ordinateurs et des réseaux*, page 73)

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

- Le nom du client, son adresse IP ou la plage d'adresses IP à laquelle il appartient
- La **stratégie** actuellement affectée à ce client. La stratégie **Par défaut** est utilisée jusqu'à ce que vous en affectiez une autre (voir *Stratégies de filtrage Internet*, page 89).
- Si ce client peut utiliser ou non les options **accès par mot de passe** (voir *Accès par mot de passe*, page 84) ou **remplacement de compte** (voir *Remplacement de compte*, page 84) pour consulter ou tenter de consulter les sites bloqués
- Si ce client dispose d'une quantité personnalisée de **temps contingenté** attribuée (voir *Utilisation de temps contingenté pour limiter l'accès à Internet*, page 58)

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

Pour modifier les paramètres des stratégies des clients, d'accès par mot de passe, de temps contingenté ou d'authentification, sélectionnez un ou plusieurs clients dans la liste, puis cliquez sur **Éditer**. Pour plus d'informations, consultez la section *Modifications des paramètres des clients*, page 83.

Pour ajouter un client, ou pour appliquer une stratégie à un client géré qui n'apparaît pas encore dans la page Clients, cliquez sur **Ajouter**, puis passez à la section *Ajout d'un client*, page 81, pour plus d'informations.

Si vous avez créé des rôles d'administration déléguée (voir *Administration déléguée et génération de rapports*, page 323), les Super administrateurs peuvent déplacer leurs clients vers d'autres rôles. Commencez par cocher la case accolée à l'entrée du client, puis cliquez sur **Déplacer vers le rôle**. Lorsqu'un client est déplacé vers un rôle d'administration déléguée, la stratégie et les filtres qui lui sont appliqués sont copiés dans ce rôle. Pour plus d'informations, consultez la section *Déplacements de clients vers des rôles*, page 86.

Si vous avez configuré Websense pour qu'il communique avec un service d'annuaire de type LDAP, le bouton **Gérer les groupes LDAP personnalisés** s'affiche dans la barre d'outils en haut de la page. Cliquez sur ce bouton pour ajouter ou modifier les groupes en fonction d'un attribut LDAP (voir *Fonctionnement des groupes LDAP personnalisés*, page 80).

Pour retirer un client de TRITON - Web Security, sélectionnez-le, puis cliquez sur **Supprimer**.

Fonctionnement avec des ordinateurs et des réseaux

Rubriques connexes :

- *Fonctionnement des clients*, page 72
- *Fonctionnement avec des utilisateurs et des groupes*, page 74
- *Ajout d'un client*, page 81
- *Attribution d'une stratégie aux clients*, page 95

Dans TRITON - Web Security, un **ordinateur** correspond à l'adresse IP (par exemple, 10.201.3.1 ou fd3a:918a:71a1:bcaa::0011) associée à un ordinateur filtré. Un **réseau** correspond à la plage d'adresses IP (par exemple, 10.201.3.2 à 10.201.3.44 ou fd3a:918a:71a1:bcaa::1111 à fd3a:918a:71a1:bcaa::1211) associée à un groupe d'ordinateurs filtrés.

- Dans les déploiements Websense Web Security Gateway Anywhere, le filtrage hybride n'applique pas de stratégies à des ordinateurs et des réseaux individuels. Pour des informations sur l'application de stratégies à des emplacements filtrés, consultez la section *Fonctionnement des clients du filtrage hybride*, page 86.
- Avant d'appliquer des stratégies à des ordinateurs et des réseaux IPv6, désactivez temporairement les adresses IPv6 dans les ordinateurs concernés. Pour plus de détails, visitez le portail support.websense.com.

Vous pouvez affecter des stratégies à des clients ordinateurs et réseaux de la même façon que pour les clients utilisateurs, groupes et domaines.

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

Lorsque vous affectez une stratégie à un ordinateur ou à un réseau, elle s'applique quelle que soit la personne connectée à l'ordinateur filtré, **sauf** si vous avez affecté une stratégie à l'utilisateur connecté. Lorsque vous utilisez des composants de filtrage sur site, la stratégie de l'ordinateur ou du réseau est prioritaire sur toutes les autres stratégies de groupe susceptibles de s'appliquer à l'utilisateur. (Dans les déploiements Websense Web Security Gateway Anywhere, le filtrage hybride applique la stratégie de groupe avant celle de l'ordinateur ou du réseau. Voir *Fonctionnement des clients du filtrage hybride*, page 86.)

Fonctionnement avec des utilisateurs et des groupes

Rubriques connexes :

- *Fonctionnement des clients*, page 72
- *Services d'annuaire*, page 75
- *Fonctionnement des groupes LDAP personnalisés*, page 80
- *Fonctionnement avec des ordinateurs et des réseaux*, page 73
- *Ajout d'un client*, page 81
- *Attribution d'une stratégie aux clients*, page 95

Pour appliquer des stratégies à desutilisateurs individuels et à des groupes de votre réseau, configurez Websense pour qu'il accède à votre service d'annuaire et récupère les informations des objets de cet annuaire (utilisateurs, groupes, domaines et unités d'organisation).

Le logiciel Websense peut communiquer avec Windows Active Directory en mode mixte ou natif, et avec Novell eDirectory ou Oracle (anciennement Sun Java) Directory Server Enterprise Addition. Le protocole LDAP (Lightweight Directory Access Protocol) permet d'accéder à ces annuaires.

- Lorsque vous utilisez un service d'annuaire de type LDAP, les noms d'utilisateur en double ne sont pas pris en charge. Assurez-vous que le même nom d'utilisateur n'apparaisse pas dans plusieurs domaines.
- Si vous utilisez Windows Active Directory ou Oracle Directory Server, les noms d'utilisateur associés à des mots de passe vides ne sont pas pris en charge. Assurez-vous que des mots de passe aient été attribués à tous les utilisateurs.

Websense User Service transmet les informations provenant du service d'annuaire à Policy Server et Filtering Service pour les exploiter lors de l'application des stratégies de filtrage. Websense, Inc. recommande d'installer User Service dans un ordinateur Windows (bien qu'il puisse également résider dans un ordinateur Linux).

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

Services d’annuaire

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

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

Remarque

Dans les déploiements Websense Web Security Gateway Anywhere, les informations de la page Services d’annuaire servent également à renseigner la page Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées). Ceci permet au service hybride de prendre en charge le filtrage à base d’utilisateurs et de groupes. Voir *Envoi de données d’utilisateur et de groupe au service hybride*, page 220.

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

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

- *Windows Active Directory (en mode mixte)*, page 76
- *Windows Active Directory (en mode natif)*, page 76
- *Novell eDirectory et Oracle (Sun Java) Directory Server*, page 78

Warning

Dans les déploiements Websense Web Security Gateway Anywhere, le filtrage hybride prend en charge Windows Active Directory (en mode natif), Oracle Directory Server et Novell eDirectory.

Dès que la configuration est terminée, User Service communique avec le service d’annuaire pour autoriser le filtrage à base d’utilisateurs et de groupes. User Service met en cache les informations des utilisateurs et des groupes qu’il collecte toutes les 3 heures au maximum. Si vous modifiez des entrées (utilisateurs, groupes ou unités d’organisation) dans votre service d’annuaire, utilisez le bouton **Clear Cache (Effacer le cache)**, situé sous User Service Cache (Cache de User Service), pour contraindre User Service à actualiser son mappage des utilisateurs et des groupes immédiatement. Notez que le filtrage basé sur les utilisateurs peut ralentir pendant une brève période lors du renouvellement du cache.

Si vous envisagez d’autoriser des administrateurs à utiliser leur compte réseau pour se connecter à TRITON - Web Security, vous devez également configurer la communication avec le service d’annuaire dans la page Paramètres > User Directory (Annuaire des utilisateurs) de TRITON. Vous devez utiliser le même annuaire pour authentifier tous les utilisateurs administratifs. Pour plus de détails, consultez l’Aide des Paramètres de TRITON.

Windows Active Directory (en mode mixte)

Si vous utilisez Active Directory en mode mixte, aucune configuration supplémentaire n'est nécessaire généralement.

Dans certains cas, vous devez fournir des informations supplémentaires dans cet écran :

- DC Agent est utilisé pour l'identification transparente (voir *DC Agent*, page 295).

  et

- User Service s'exécute dans un ordinateur Linux.

Si ceci correspond à votre configuration, Websense peut communiquer avec un serveur Windows Internet Name Server (WINS) pour résoudre les noms de domaine en adresses IP de contrôleurs de domaine (voir *User Service sous Linux*, page 461).

Pour activer cette communication, utilisez les champs situés sous Windows Active Directory (en mode mixte) pour fournir les renseignements suivants :

1. Le nom du compte d'un **administrateur** autorisé à accéder au service d'annuaire
2. Le **Mot de passe** de ce compte
3. Les informations du **Domaine** de ce compte
4. L'adresse IP ou le nom d'hôte d'un **serveur WINS** présent dans votre réseau

Notez que vous pouvez également effectuer cette procédure dans la page Paramètres > Identification des utilisateurs > DC Agent lorsque vous configurez une instance de DC Agent. Il est inutile d'effectuer cette configuration aux deux endroits.

Si votre installation n'utilise pas cette configuration, les champs des identifiants de connexion administratifs sont désactivés.

Windows Active Directory (en mode natif)

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

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

1. Cliquez sur **Ajouter**, à côté de la liste des serveurs de catalogue global. La page Ajouter un serveur de catalogue global apparaît.
2. Fournissez l'**adresse IPv4 ou le nom d'hôte** du serveur de catalogue global :
   - Si plusieurs serveurs de catalogue global sont configurés pour le basculement, entrez le nom de domaine DNS.
   - Si vos serveurs de catalogue global ne sont pas configurés pour le basculement, entrez l'adresse IPv4 ou le nom d'hôte (si la résolution de noms est activée dans votre réseau) du serveur à ajouter.
3. Entrez le numéro de **Port** que Websense doit utiliser pour communiquer avec le catalogue global (par défaut, **3268**).

4. Vous pouvez éventuellement entrer le **Contexte racine** qui permettra de localiser les informations des utilisateurs. Si vous entrez une valeur, ce contexte doit être valide dans votre domaine.
   - Si vous avez défini le port de communication 3268 ou 3269, le contexte racine n'est pas nécessaire. Si le contexte racine est vide, User Service commence sa recherche au plus haut niveau du service d'annuaire.
   - Si le port spécifié est 389 ou 636, vous devez fournir un contexte racine.

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

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

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

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

   - Si vous activez Nom distinctif complet, entrez le nom distinctif sous forme de chaîne dans le champ **Nom distinctif de l'utilisateur** (par exemple, *cn=Admin, cn=Utilisateurs, ou=InfoSysteme, dc=societe, dc=net*), puis le **Mot de passe** de ce compte.
6. Cliquez sur **Tester la connexion** pour vérifier que Websense peut se connecter à l'annuaire à l'aide des informations de compte fournies.
7. Cliquez sur **OK** pour revenir à la page Services d'annuaire.
8. Reprenez la procédure ci-dessus pour chaque serveur de catalogue global.
9. Cliquez sur **Paramètres avancés de l'annuaire**, puis passez à la section *Paramètres avancés de l'annuaire*, page 78.

Novell eDirectory et Oracle (Sun Java) Directory Server

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

1. Entrez l'**adresse IPv4 ou le nom d'hôte** du serveur de l'annuaire.
2. Entrez le numéro de **Port** que Websense doit utiliser pour communiquer avec l'annuaire. La valeur par défaut est 389.
3. Si votre service d'annuaire exige des droits d'administrateur pour un accès en lecture seule, entrez le **Nom distinctif de l'administrateur**.
4. Entrez le **Contexte racine** dont Websense doit se servir pour rechercher les informations sur les utilisateurs. Par exemple *o=domaine.com*.
   - Pour Oracle Directory Server, il est obligatoire de fournir un contexte racine, mais ce renseignement est facultatif pour Novell eDirectory.
   - Limiter le contexte accroît la vitesse et l'efficacité de la récupération des informations des utilisateurs.

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

5. Fournissez le **Mot de passe** du compte d'administrateur saisi précédemment.
6. Cliquez sur **Tester la connexion** pour vérifier que Websense peut se connecter au serveur de l'annuaire à l'aide des informations de compte fournies.
7. Cliquez sur **Paramètres avancés de l'annuaire**, puis passez à la section *Paramètres avancés de l'annuaire*, page 78.

Paramètres avancés de l'annuaire

Rubriques connexes :

- *Windows Active Directory (en mode natif)*, page 76
- *Novell eDirectory et Oracle (Sun Java) Directory Server*, page 78

Ces paramètres permettent de définir :

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

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

1. Si vous utilisez des types de classes d'objets personnalisés (noms d'attribut) dans votre service d'annuaire, cochez la case **Utiliser des filtres personnalisés**. Les chaînes de filtre par défaut sont énumérées sous cette case à cocher.
2. Modifiez les chaînes de filtre existantes en les remplaçant par les types de classes d'objets propres à votre annuaire. Par exemple, si votre annuaire utilise un type de classes d'objets tel que **dept** au lieu de **ou** (unité d'organisation), insérez une nouvelle valeur dans le champ Filtre de recherche de domaine.

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

Attribut	Description
Attribut d'ID de connexion utilisateur	Identifie les noms de connexion des utilisateurs
Attribut de prénom	Identifie le nom donné à chaque utilisateur
Attribut de nom	Identifie le nom de famille de chaque utilisateur
Attribut de groupe	Identifie le nom des groupes
Attribut MemberOf	Spécifie que l'utilisateur ou le groupe est membre d'un autre groupe Si vous utilisez Novell eDirectory, ceci correspond à l'attribut **groupMembership**.
Filtre de recherche d'utilisateur	Détermine comment User Service recherche les utilisateurs
Filtre de recherche de groupe	Détermine comment User Service recherche les groupes
Filtre de recherche de domaine	Détermine comment User Service recherche les domaines et les unités d'organisation
Filtre de recherche de groupes d'utilisateurs	Détermine comment User Service associe des utilisateurs à des groupes

3. Pour sécuriser les communications entre Websense et votre service d'annuaire, activez l'option **Utiliser SSL**.
4. Pour définir le jeu de caractères utilisé par Websense pour coder les informations LDAP, activez **UTF-8** ou **MBCS**.

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

Fonctionnement des groupes LDAP personnalisés

Rubriques connexes :

- *Fonctionnement avec des utilisateurs et des groupes*, page 74
- *Services d'annuaire*, page 75
- *Ajout ou modification d'un groupe LDAP personnalisé*, page 81

La page **Gérer les groupes LDAP personnalisés** permet de gérer les groupes personnalisés en fonction des attributs définis dans votre service d'annuaire. Cette option est uniquement disponible si vous avez configuré Websense pour qu'il communique avec un service d'annuaire de type LDAP.

Important

Lorsque vous ajoutez des groupes LDAP dans TRITON - Web Security, leurs définitions sont stockées par le serveur Policy Server actif et n'affectent pas les autres instances de Policy Server. Pour ajouter des groupes LDAP personnalisés dans plusieurs serveurs Policy Server, utilisez TRITON - Web Security pour vous connecter à chaque serveur Policy Server et saisissez les informations nécessaires.

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

- Pour ajouter un groupe, cliquez sur **Ajouter** (voir *Ajout ou modification d'un groupe LDAP personnalisé*, page 81).
- Pour modifier une entrée de la liste, cliquez sur le nom de son groupe (voir *Ajout ou modification d'un groupe LDAP personnalisé*).
- Pour retirer une entrée, sélectionnez-la, puis cliquez sur **Supprimer**.

Lorsque la modification des groupes LDAP personnalisés est terminée, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page précédente. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout ou modification d’un groupe LDAP personnalisé

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

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

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

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

   ```
   (WorkStatus=tempspartiel)
   ```

   Dans cet exemple, **WorkStatus** est un attribut d’utilisateur qui indique le statut de l’emploi, et **tempspartiel** une valeur indiquant que l’utilisateur est un employé à temps partiel.
3. Cliquez sur **OK** pour revenir à la page Gérer les groupes LDAP personnalisés. La nouvelle entrée ou l’entrée modifiée apparaît dans la liste.
4. Ajoutez ou modifiez une autre entrée ou cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page précédente. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout d’un client

Rubriques connexes :

- *Fonctionnement des clients*, page 72
- *Fonctionnement avec des ordinateurs et des réseaux*, page 73
- *Fonctionnement avec des utilisateurs et des groupes*, page 74
- *Recherche dans le service d’annuaire*, page 82
- *Modifications des paramètres des clients*, page 83

La page **Gestion des stratégies > Clients > Ajouter des clients** permet d’ajouter des clients utilisateur, groupe, ordinateur et réseau dans TRITON - Web Security de manière à pouvoir ensuite leur affecter une stratégie.

Si vous êtes connecté(e) avec un rôle d’administration déléguée, vous ne pouvez ajouter que les clients qui apparaissent dans votre liste de clients gérés. Pour les rôles de gestion des stratégies et de génération de rapports, la procédure d’ajout de clients gérés dans la page Clients exige de leur attribuer une stratégie. (Les rôles de génération de rapports d’investigation n’ont pas cette obligation.)

1. Identifiez un ou plusieurs clients :
   - Pour ajouter un client utilisateur, groupe ou domaine (OU), parcourez l'arborescence **Annuaire** pour rechercher des entrées dans votre service d'annuaire. Si vous utilisez un service d'annuaire de type LDAP, vous pouvez également cliquer sur **Rechercher** pour activer un outil de recherche d'annuaire (voir *Recherche dans le service d'annuaire*, page 82).
   - Pour ajouter un client ordinateur ou réseau, entrez une **adresse IP** ou une **plage d'adresses IP** au format IPv4 ou IPv6.

     Deux plages réseau ne peuvent pas se chevaucher, mais un client réseau peut inclure une adresse IP identifiée séparément en tant que client ordinateur. Dans le cas d'un tel chevauchement, la stratégie affectée à l'ordinateur est prioritaire sur celle affectée au réseau.
2. Cliquez sur la flèche (>) pour ajouter chaque client à la liste **Clients sélectionnés**.

   Pour retirer une entrée de la liste Clients sélectionnés, sélectionnez le client, puis cliquez sur **Supprimer**.
3. Sélectionnez une **Stratégie** à affecter à tous les clients de la liste Clients sélectionnés.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Les clients sont ajoutés dans la liste appropriée de la page **Gestion des stratégies** > **Clients**. Pour modifier la stratégie affectée à un ou plusieurs clients, ou pour configurer d'autres paramètres de clients, sélectionnez chaque entrée de client, puis cliquez sur **Éditer**. Pour plus d'informations, consultez la section *Modifications des paramètres des clients*, page 83.

Recherche dans le service d'annuaire

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

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

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

   Dans le cas d'un vaste service d'annuaire, l'option **Tous** peut entraîner des recherches très longues.
4. Utilisez la liste **Rechercher** pour spécifier le mode de recherche :
   - Sélectionnez **Entries containing search string (Entrées contenant la chaîne de recherche)** pour localiser toutes les entrées de l'annuaire qui contiennent le terme de recherche saisi.
   - Sélectionnez **Exact search string only (Chaîne de recherche exacte uniquement)** pour localiser seulement l'entrée d'annuaire qui correspond précisément au terme recherché.

5. Dans l'arborescence du **Contexte de recherche**, spécifiez dans quelle partie de l'annuaire doit porter la recherche. Plus le contexte est précis, plus la recherche est rapide.
6. Cliquez sur **Ok**.

   La liste des résultats de la recherche s'affiche.
7. Sélectionnez une ou plusieurs entrées dans ces résultats, puis cliquez sur la flèche droite (>) pour ajouter chaque sélection en tant que client ou administrateur.
   - Cliquez sur **Nouvelle recherche** pour entrer d'autres critères de recherche.
   - Cliquez sur **Parcourir** pour cesser d'utiliser la recherche et naviguer dans l'arborescence de l'annuaire pour identifier des utilisateurs.
8. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Modifications des paramètres des clients

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

1. Sélectionnez une **Stratégie** à appliquer aux clients sélectionnés. La stratégie Par défaut régit les clients jusqu'à ce qu'une autre stratégie leur soit affectée.
2. Sous **Block Page Override Options (Options de contournement des pages de blocage)**, indiquez si ce client a la possibilité de contourner (ou de tenter de contourner) une page de blocage pour afficher un site demandé.
   - Cochez la case **Enable password override (Activer l'accès par mot de passe)** pour permettre aux clients sélectionnés d'entrer un mot de passe que vous spécifiez pour accéder à tout site bloqué pendant la période configurée dans la page Paramètres > Général > Filtrage (60 secondes, par défaut). Voir *Accès par mot de passe*, page 84.

     Saisissez ce mot de passe, puis confirmez-le.

     Vous pouvez activer cette option pour certains utilisateurs qui ont parfois besoin d'accéder à des sites habituellement non autorisés par la stratégie d'utilisation acceptable de votre organisation.

     Pour supprimer le droit d'accès par mot de passe d'un client, cliquez sur **Désactivé**.
   - Cochez la case **Enable account override (Activer le remplacement de compte)** pour permettre aux clients sélectionnés de saisir un nom de connexion réseau et un mot de passe pour tenter d'accéder à un site bloqué en appliquant une autre stratégie à leurs requêtes. Si sa requête est autorisée par la nouvelle stratégie, l'utilisateur peut accéder au site pendant la période configurée dans la page Paramètres > Général > Filtrage (5 minutes, par défaut). Voir *Remplacement de compte*, page 84.

     Vous pouvez activer cette option pour les ordinateurs partagés (de type borne ou kiosque) généralement régis par une stratégie basée sur l'adresse IP qui permet aux utilisateurs de se connecter via un compte Invité. Les utilisateurs ont alors la possibilité de saisir leurs identifiants réseau dans la page de blocage pour savoir si leur stratégie actuelle autorise l'accès à un site bloqué sur un ordinateur partagé.

Si la stratégie de l'utilisateur bloque également ce site, l'utilisateur reçoit une seconde page de blocage.

3. Pour affecter une quantité personnalisée de **Temps contingenté** aux clients sélectionnés, cliquez sur **Personnalisé** et entrez le nombre de minutes de temps contingenté à affecter.

   Pour réinitialiser les paramètres de temps contingenté par défaut, cliquez sur **Par défaut**.
4. Cliquez sur **OK** pour mettre 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)**.

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

Accès par mot de passe

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

Lorsqu'un administrateur active l'option de l'accès par mot de passe, il crée également ce mot de passe. Lorsque des clients avec droits d'accès par mot de passe demandent un site bloqué, la page de blocage de Websense comprend un champ de saisie pour ce mot de passe. Ces clients peuvent alors saisir ce mot de passe pour accéder aux sites bloqués pendant une durée limitée.

Important

Dans les déploiements à plusieurs instances de Filtering Service, Websense State Server est requis pour allouer correctement la durée de l'accès par mot de passe. Pour plus d'informations, consultez la section *Policy Server, Filtering Service et State Server*, page 368.

Dans la page **Paramètres** > **Général** > **Filtrage**, configurez la durée pendant laquelle les clients avec droits d'accès par mot de passe peuvent accéder aux sites bloqués en saisissant leur mot de passe (voir *Configuration des paramètres de filtrage de Websense*, page 67).

Pour accorder des droits d'accès par mot de passe à des clients spécifiques, utilisez la page **Gestion des stratégies** > **Clients** (voir *Ajout d'un client*, page 81, ou *Modifications des paramètres des clients*, page 83).

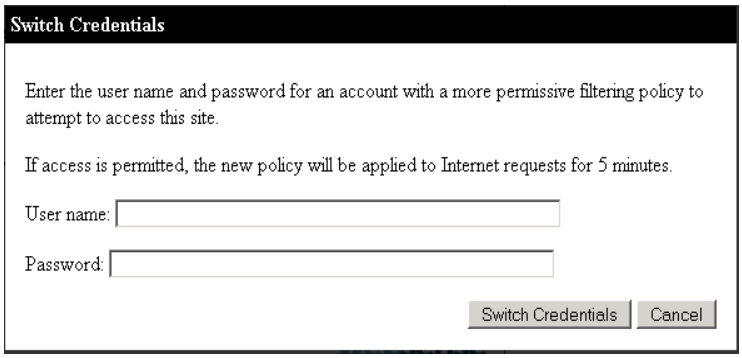
Remplacement de compte

Le Remplacement de compte autorise les utilisateurs à changer les identifiants de connexion employés pour appliquer une stratégie à une requête.

Si, par exemple, des utilisateurs accèdent à Internet à partir d'un ordinateur de type kiosque, ou à partir d'un ordinateur auquel ils se connectent à l'aide d'un compte local au lieu d'un compte réseau, les administrateurs peuvent associer les autorisations de remplacement de compte au client ordinateur ou réseau (adresse IP).

Des autorisations de remplacement de compte peuvent également être accordées aux clients de l'annuaire (utilisateurs, groupes et domaines [unités d'organisation]).

Lorsque les requêtes d'un utilisateur sont bloquées par la stratégie active et que des autorisations de remplacement de compte sont accordées au client filtré (qu'il s'agisse d'une adresse IP ou d'un client de l'annuaire), la page de blocage comprend un bouton **Entrer de nouveaux identifiants**. L'utilisateur peut alors fournir un nom d'utilisateur et un mot de passe.



Dès que l'utilisateur clique sur **Switch Credentials (Changer d'identifiants de connexion)**, Websense identifie la stratégie affectée au nouveau compte et l'applique à la requête.

- Si la nouvelle stratégie autorise cette requête, l'utilisateur peut accéder au site.
- Si la nouvelle stratégie bloque cette requête, l'utilisateur reçoit une autre page de blocage.

En d'autres termes, à la différence de l'accès par mot de passe, l'option de remplacement de compte ne garantit pas l'accès à un site bloqué. À l'inverse, cette option change la stratégie utilisée pour filtrer la requête.

La nouvelle stratégie s'applique aux requêtes supplémentaires provenant de cet ordinateur pendant la période spécifiée dans la page **Paramètres > Général > Filtrage** (5 minutes, par défaut). Voir *Configuration des paramètres de filtrage de Websense*, page 67.

Important

Dans les déploiements à plusieurs instances de Filtering Service, Websense State Server est requis pour allouer correctement la durée du remplacement de compte. Pour plus d'informations, consultez la section *Policy Server, Filtering Service et State Server*, page 368.

Si, après avoir changé d'identifiants avec succès, l'utilisateur souhaite quitter cet ordinateur avant la fin de la durée du remplacement de compte, la session de remplacement peut être interrompue manuellement en saisissant l'URL suivante :

```
http://<adresse_IP_Filtering_Service>:15871/cgi-bin/
cancel_user_account_overrider.cgi
```

Vous pouvez configurer cette URL en tant que favori de navigateur dans les ordinateurs qui utilisent l'option de remplacement de compte.

Déplacements de clients vers des rôles

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

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

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

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

   Un message contextuel indique que les clients sélectionnés sont en cours de déplacement. Le processus de déplacement peut prendre un certain temps.
3. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Si des administrateurs délégués du rôle sélectionné sont connectés avec un accès aux stratégies pendant ce processus de déplacement, ils devront se déconnecter de TRITON - Web Security et se reconnecter à nouveau pour voir les nouveaux clients dans leurs listes de Clients gérés.

Fonctionnement des clients du filtrage hybride

Dans les déploiements Websense Web Security Gateway Anywhere, le service hybride peut filtrer les requêtes Internet provenant des adresses IP externes (emplacements) que vous configurez, et les requêtes des utilisateurs situés dans des emplacements non reconnus (hors site, par exemple) qui se connectent au service hybride.

Le filtrage hybride peut appliquer les stratégies (créées dans TRITON - Web Security) aux éléments suivants :

- Les utilisateurs, groupes et domaines (OU) définis dans un service d'annuaire LDAP pris en charge

  Pour ce faire, Websense Directory Agent doit être installé et configuré (voir *Identification des utilisateurs du filtrage hybride*, page 311).

- Les emplacements filtrés, identifiés dans la page Hybrid Configuration (Configuration hybride) > Filtered Locations (Emplacements filtrés). Tout emplacement est identifié par l'adresse IP externe, la plage d'adresses IP ou le sous-réseau d'un ou plusieurs ordinateurs servant de passerelle ou de pare-feu.

Le filtrage hybride n'applique **pas** de stratégies aux ordinateurs clients individuels de votre réseau.

Les clients de l'annuaire (utilisateurs, groupes et unités d'organisation) filtrés par le service hybride sont identifiés dans la page Gestion des stratégies > Clients de TRITON - Web Security, comme ceux qui sont filtrés par des composants sur site.

Appliquer une stratégie à un emplacement filtré revient à appliquer une stratégie à un client ordinateur ou réseau :

1. Ajoutez l'emplacement dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Filtered Locations (Emplacements filtrés) (voir *Définition des emplacements filtrés*, page 205).
2. Ajoutez l'adresse IP ou la plage qui apparaît dans la page Filtered Locations (Emplacements filtrés) en tant que client ordinateur ou réseau dans la page Gestion des stratégies > Clients (voir *Fonctionnement avec des ordinateurs et des réseaux*, page 73).
3. Appliquez ensuite une stratégie à cette adresse ou cette plage.

Comme pour le filtrage sur site, chaque fois qu'aucune stratégie ne s'applique à l'utilisateur, au groupe ou à l'emplacement, la stratégie Par défaut est appliquée.

5 Stratégies de filtrage Internet

Rubriques connexes :

- *Filtres de l'utilisation Internet*, page 49
- *Clients*, page 71
- *La stratégie Par défaut*, page 90
- *Fonctionnement des stratégies*, page 91
- *Ordre du filtrage*, page 95

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

- Filtres de catégories, utilisés pour appliquer des actions (autoriser, bloquer) à des catégories d'URL (voir *Filtrage des catégories et des protocoles*, page 50)
- Filtres d'accès limité, utilisés pour autoriser l'accès à une liste restreinte d'URL uniquement (voir *Limitation des utilisateurs à une liste définie d'URL*, page 247)
- Filtres de protocoles, utilisés pour appliquer des actions aux protocoles Internet (voir *Filtrage des catégories et des protocoles*, page 50)
- Un planning qui détermine à quel moment chaque filtre de catégories, de protocoles et d'accès limité est imposé

Une nouvelle installation du logiciel ou du dispositif Websense comprend trois stratégies prédéfinies :

- **Par défaut** filtre l'accès à Internet de tous les clients non régis par une autre stratégie. Websense commence à imposer cette stratégie dès la saisie d'une clé d'abonnement (voir *La stratégie Par défaut*, page 90).
- **Illimité** fournit un accès illimité à Internet. Cette stratégie n'est appliquée à aucun client par défaut.
- **Exemple - Utilisateur standard** montre comment plusieurs filtres de catégories et de protocoles peuvent être appliqués dans une stratégie pour assurer différents niveaux de restriction de filtrage selon les moments. Cette stratégie est présentée dans le didacticiel de démarrage rapide pour les nouveaux utilisateurs dans la procédure de modification d'une stratégie et de son application aux clients.

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

La stratégie Par défaut

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 89
- *Fonctionnement des stratégies*, page 91
- *Ordre du filtrage*, page 95

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

Remarque

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

Au fur et à mesure que vous créez et appliquez des stratégies de filtrage supplémentaires, la stratégie Par défaut continue de filtrer l'accès à Internet des clients non régis par une autre stratégie.

La stratégie Par défaut doit assurer le filtrage Internet (imposer une combinaison de filtres de catégories ou d'accès limité et de filtres de protocoles) 24 heures sur 24, 7 jours sur 7.

Important

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

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

Fonctionnement des stratégies

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 89
- *Création d'une stratégie*, page 92
- *Modification d'une stratégie*, page 93
- *Filtres de l'utilisation Internet*, page 49
- *Réglage des stratégies de filtrage*, page 247

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

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

- Pour ajouter une stratégie, cliquez sur **Ajouter**, puis consultez la section *Création d'une stratégie*, page 92, pour plus d'informations.
- Pour modifier une stratégie, cliquez sur son nom dans la liste, puis consultez la section *Modification d'une stratégie*, page 93, pour plus d'informations.
- Pour retirer une stratégie, cochez la case accolée à son nom, puis cliquez sur **Supprimer**.
- Pour découvrir les clients filtrés par la stratégie, cliquez sur un nombre dans la colonne Utilisateurs, Réseaux ou Ordinateurs. Les informations sur les clients s'affichent dans une fenêtre contextuelle.

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

Si vous avez créé des rôles d'administration déléguée (voir *Administration déléguée et génération de rapports*, page 323), les Super administrateurs peuvent copier les stratégies qu'ils ont créées pour d'autres rôles afin que les administrateurs délégués les utilisent. Les filtres imposés par la stratégie sont également copiés.

> **Remarque**
>
> Les administrateurs délégués étant régis par le verrouillage du filtre, lorsque les filtres Autoriser tout sont copiés, la copie reçoit un nouveau nom et les restrictions du verrouillage du filtre sont appliquées. À la différence du filtre d'origine, le filtre copié peut être modifié.

Pour copier des stratégies vers un autre rôle, cochez la case accolée au nom de la stratégie, puis cliquez sur **Copier dans le rôle**. Cette opération peut durer plusieurs minutes. Pour plus d'informations, consultez la section *Copie de filtres et de stratégies vers des rôles*, page 252.

Création d'une stratégie

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 89
- *Fonctionnement des stratégies*, page 91
- *Modification d'une stratégie*, page 93
- *Fonctionnement des filtres*, page 59
- *Limitation des utilisateurs à une liste définie d'URL*, page 247

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

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

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

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

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

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

   Utilisez la page Modifier la stratégie pour définir la nouvelle stratégie. Voir *Modification d'une stratégie*, page 93.

Modification d'une stratégie

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 89
- *Fonctionnement des stratégies*, page 91
- *Création d'une stratégie*, page 92
- *Fonctionnement des filtres*, page 59
- *Limitation des utilisateurs à une liste définie d'URL*, page 247

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

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

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

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

Pour affecter cette stratégie à d'autres clients, cliquez sur **Appliquer aux clients** dans la barre d'outils située en haut de la page, puis consultez la section *Attribution d'une stratégie aux clients*, page 95.

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

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

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

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

   Pour ajouter un nouveau filtre à imposer dans cette stratégie, sélectionnez **Ajouter un filtre de catégorie** ou **Ajouter un filtre d'accès limité**. Pour obtenir des instructions, consultez *Création d'un filtre de catégories*, page 60, ou *Création d'un filtre d'accès limité*, page 249.

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

   Pour ajouter un nouveau filtre à imposer dans cette stratégie, sélectionnez **Ajouter un filtre de protocoles**. Pour obtenir des instructions, consultez la section *Création d'un filtre de protocoles*, page 63.

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

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

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

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

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

Type de filtre	Boutons
filtre de catégories	• Servez-vous des boutons **Autoriser**, **Bloquer**, **Confirmer** ou **Temps contingenté** pour modifier l'action appliquée aux catégories sélectionnées (voir *Actions de filtrage*, page 57). • Pour modifier l'action appliquée à une catégorie parente et à toutes ses sous-catégories, commencez par modifier l'action appliquée à la catégorie parente, puis cliquez sur **Appliquer aux sous-catégories**. • Pour activer le blocage des mots-clés, le blocage de types de fichiers ou le blocage en fonction de la bande passante, cliquez sur **Avancé**.
Filtre d'accès limité	• Utilisez le bouton **Ajouter des sites** et **Ajouter des expressions** pour ajouter des éléments autorisés (URL, adresses IP ou expressions régulières) au filtre (voir *Limitation des utilisateurs à une liste définie d'URL*, page 247). • Pour retirer un site du filtre, cochez la case accolée à son URL, son adresse IP ou son expression, puis cliquez sur **Supprimer**.
filtre de protocoles	• Servez-vous des boutons **Autoriser** ou **Bloquer** pour modifier l'action appliquée aux protocoles sélectionnés (voir *Actions de filtrage*, page 57). • Pour modifier l'action appliquée à tous les protocoles d'un groupe de protocoles, modifiez l'action appliquée à l'un des protocoles du groupe, puis cliquez sur **Appliquer au groupe**. • Pour journaliser les données du protocole sélectionné ou pour activer le blocage en fonction de la quantité de bande passante, cliquez sur **Avancé**.

Lorsque la modification d'une stratégie est terminée, cliquez sur **OK** pour mettre en cache vos modifications. 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

Rubriques connexes :

- *Stratégies de filtrage Internet*, page 89
- *Création d'une stratégie*, page 92
- *Modification d'une stratégie*, page 93
- *Clients*, page 71
- *Ajout d'un client*, page 81

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

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

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

Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour inviter Websense à commencer à utiliser la nouvelle stratégie pour filtrer les requêtes des clients sélectionnés.

Ordre du filtrage

Plusieurs critères, appliqués dans un ordre spécifique, permettent de déterminer si les données Internet demandées doivent être autorisées, limitées ou bloquées.

Pour chaque requête reçue, les solutions Websense Web Security :

1. Vérifient la conformité de l'abonnement, en s'assurant qu'il est actif et que le nombre de clients abonnés n'est pas dépassé
2. Déterminent la stratégie ou l'exception devant s'appliquer, en recherchant dans l'ordre suivant :
   - Le logiciel sur site (Websense Filtering Service) :
     a. La stratégie ou les exceptions attribuée(s) à **l'utilisateur**
     b. La stratégie ou les exceptions attribuée(s) attribuée à **l'adresse IP** (ordinateur ou réseau) de l'ordinateur utilisé
     c. Les stratégies ou les exceptions attribuées aux **groupes** dont l'utilisateur est membre
     d. Les stratégies ou les exceptions attribuées au **domaine** (OU) de l'utilisateur

e. La stratégie **Par défaut**

> **Remarque**
> Vous pouvez configurer Filtering Service pour établir les priorités entre les stratégies de groupes et de domaines par rapport aux stratégies à base d'adresses IP, si nécessaire. Voir *Priorités des stratégies de groupe et de domaine*, page 97.

- (*Websense Web Security Gateway Anywhere*) Pour les utilisateurs filtrés par le service hybride :
  a. La stratégie ou les exceptions attribuée(s) à **l'utilisateur**
  b. La stratégie ou les exceptions attribuée(s) aux **groupes** dont l'utilisateur est membre
  c. La stratégie ou les exceptions attribuée(s) au **domaine** (OU) de l'utilisateur
  d. La stratégie ou les exceptions attribuée(s) à l'**adresse IP** externe (emplacement filtré) d'où provient la requête
  e. La stratégie **Par défaut**

  La première stratégie ou exception applicable détectée est utilisée.

3. Filtrent la requête en fonction des restrictions de la stratégie ou des exceptions

Il arrive parfois qu'un utilisateur appartienne à plusieurs groupes ou domaines et qu'aucune stratégie de priorité supérieure ne s'applique. Dans ce cas, la solution de sécurité Web Websense vérifie les stratégies attribuées à chacun des groupes de l'utilisateur.

- Si tous les groupes ont la même stratégie, Websense filtre la requête en fonction de celle-ci.
- Si l'un des groupes est associé à une stratégie différente, Websense filtre la requête en fonction du paramètre **Utiliser un blocage plus restrictif**, configuré dans la page **Paramètres > Général > Filtrage**.
  - Si l'option **Utiliser un blocage plus restrictif** est activée, et que l'une des stratégies applicables bloque l'accès à la catégorie demandée, Websense bloque le site.
  - Si cette option n'est pas activée, et que l'une des stratégies applicables autorise l'accès à la catégorie demandée, Websense autorise le site.

  Si l'une des stratégies applicables impose un filtre d'accès limité, l'option **Utiliser un blocage plus restrictif** peut avoir un effet imprévu. Voir *Filtres d'accès limité et priorités du filtrage*, page 248.
- Si l'un des groupes a une stratégie différente et qu'aucune des stratégies potentiellement applicables n'impose le blocage des types de fichiers, les paramètres du blocage des types de fichiers sont ignorés.

Priorités des stratégies de groupe et de domaine

Dans certains cas, les organisations préfèrent que les stratégies d'annuaire (appliquées aux utilisateurs, aux groupes et aux domaines) soient prioritaires sur celles appliquées aux adresses IP (ordinateurs et réseaux).

Cela peut se produire, par exemple, lorsque les stratégies à base de groupes sont largement exploitées dans l'organisation, et que l'option Remplacement de compte (voir *Remplacement de compte*, page 84) est appliquée aux adresses IP du réseau. Lorsque la priorité de filtrage par défaut est appliquée, la stratégie à base d'adresses IP remplace toutes les stratégies à base de groupes, ce qui peut provoquer de fréquents échecs du remplacement de compte. Lorsque les stratégies à base de groupes et de domaines sont prioritaires, ce problème est évité.

Pour configurer Filtering Service pour établir les priorités des stratégies d'annuaire (en d'autres termes, pour utiliser l'ordre de recherche Utilisateur > Groupe > Domaine > Ordinateur > Réseau pour identifier la stratégie à appliquer à une requête) :

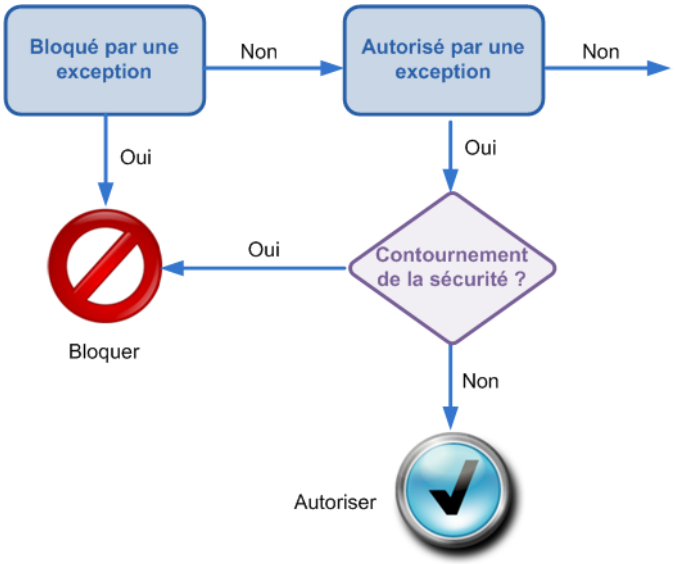
1. Dans l'ordinateur Filtering Service, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
2. Ouvrez le fichier **eimserver.ini** dans un éditeur de texte.
3. Localisez la section **[FilteringManager]** dans ce fichier et ajoutez le paramètre suivant :

   ```
   UserGroupIpPrecedence=true
   ```

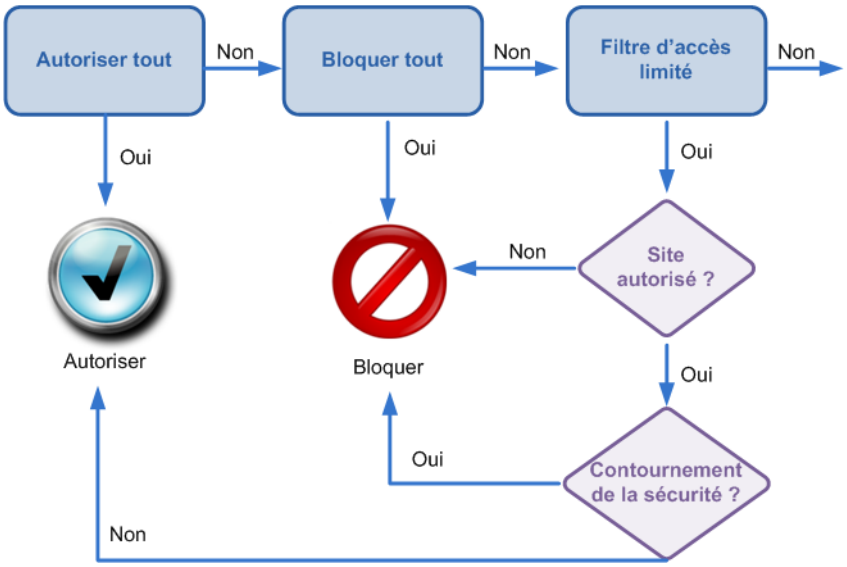
4. Enregistrez et fermez le fichier.
5. Redémarrez Filtering Service.
   - *Sous Windows* : utilisez la boîte de dialogue Services Windows pour redémarrer **Websense Filtering Service**.
   - *Sous Linux* : utilisez la commande /opt/Websense/WebsenseDaemonControl pour redémarrer **Filtering Service**.

Filtrage d'un site

Le logiciel de sécurité Web Websense évalue les restrictions de stratégie comme suit pour déterminer si le site demandé doit être autorisé ou bloqué. (Pour les déploiements Websense Web Security Gateway Anywhere, notez que la logique indiquée ici concerne le logiciel sur site et non le service hybride.)



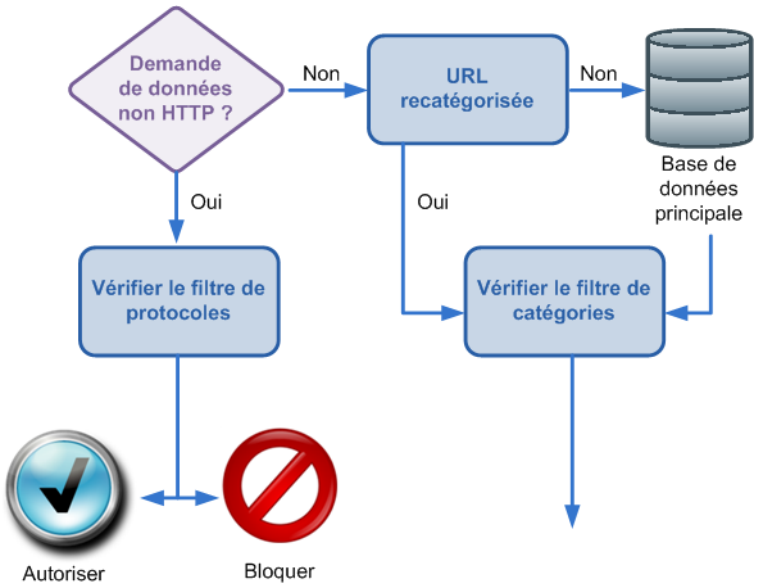
1. Le logiciel vérifie si le site fait l'objet d'une **exception**.
   - S'il existe une **exception de blocage**, le site est bloqué.
   - S'il existe une **exception d'autorisation**, le site est autorisé.
   - Si le site ne fait l'objet d'aucune exception, le logiciel passe à l'étape 2.



2. Le logiciel détermine le **filtre de catégories** ou le **filtre d'accès limité** appliqué par la stratégie pour l'heure et la date en cours.
   - Si le filtre de catégories actif est **Autoriser tout**, il autorise le site.

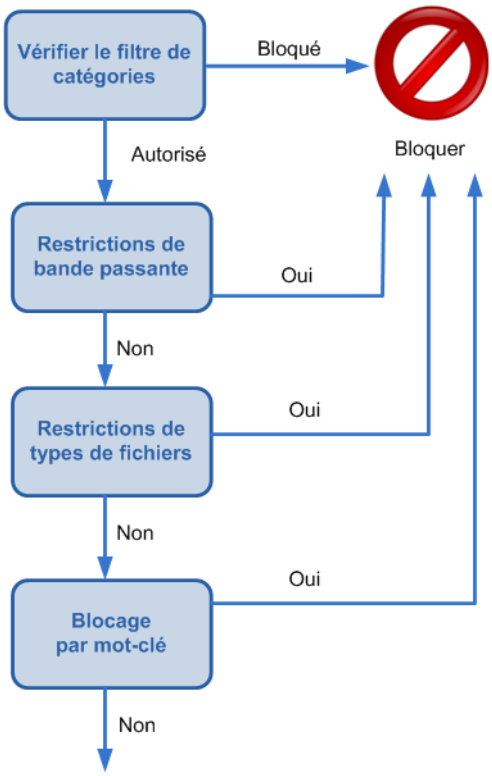
- Si le filtre de catégories actif est **Bloquer tout**, il bloque le site.
- Si le filtre est **d'accès limité**, il vérifie si le filtre contient l'URL ou l'adresse IP. Dans l'affirmative, il autorise le site. Dans le cas contraire, il bloque le site.
- Si un autre filtre de catégories s'applique, il passe à l'étape 3.

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



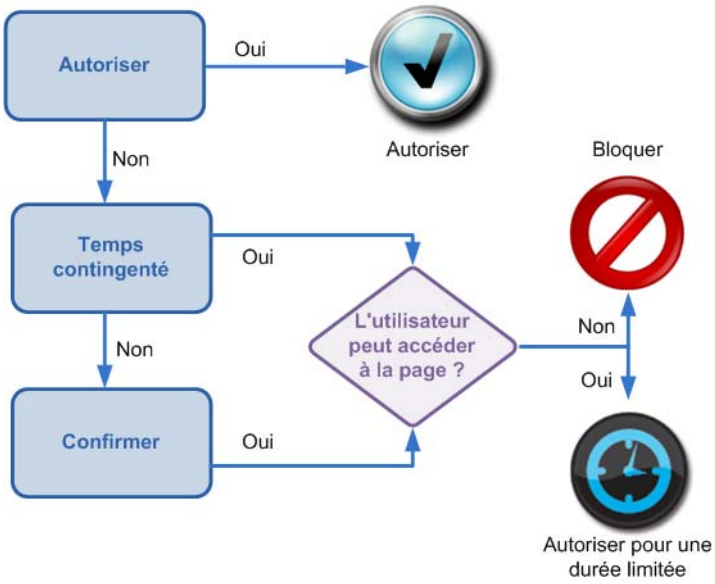
3. Il vérifie le **filtre de protocoles** actif et détermine si des protocoles non HTTP sont associés à la requête.
   - Dans l'affirmative, il applique les paramètres de filtrage de protocoles aux données susceptibles d'être transmises.
   - Sinon, il passe à l'étape 4.
4. Il tente d'associer le site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

- S'il ne peut pas établir de correspondance, il classe le site dans la catégorie Divers/Non catégorisées et passe à l'étape 6.



6. Il vérifie le filtre de catégories d'URL actif et identifie l'action appliquée à la catégorie contenant le site demandé.
   - Si l'action est **Bloquer**, il bloque le site.
   - Si une autre action s'applique, il passe à l'étape 7.
7. Il vérifie les paramètres de **Bandwidth Optimizer** dans le filtre de catégories actif (voir *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270).
   - Si la bande passante consommée actuellement dépasse les limites configurées, il bloque le site.
   - Si la bande passante consommée actuellement ne dépasse pas les limites spécifiées, ou si aucune action basée sur la bande passante ne s'applique, il passe à l'étape 8.
8. Il recherche les restrictions de **type de fichiers** appliquées à la catégorie active (voir *Gestion du trafic en fonction du type de fichiers*, page 273).
   - Si le site contient des fichiers dont les extensions sont bloquées, il bloque l'accès à ces fichiers. Si le site lui-même contient un type de fichier bloqué, il bloque l'accès au site.
   - Si le site ne contient pas de fichiers dont les extensions sont bloquées, il passe à l'étape 9.
9. Il recherche des **mots-clés** dans l'URL et le chemin CGI, si le blocage des mots-clés est activé (voir *Filtrage par mots-clés*, page 258).
   - S'il trouve un mot-clé bloqué, il bloque le site.

- S’il ne trouve pas de mot-clé bloqué, il passe à l’étape 10.



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

Websense continue ainsi jusqu’à ce que le site demandé soit bloqué ou explicitement autorisé. À ce stade, aucun autre filtrage n’est tenté. Par exemple, si le site demandé appartient à une catégorie bloquée et contient un mot-clé bloqué, Websense bloque le site au niveau de la catégorie sans vérifier le filtre du mot-clé. Log Server enregistre alors la requête en tant que bloquée du fait de la catégorie bloquée, pas du fait d’un mot-clé.

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

6 Exceptions aux stratégies de filtrage

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 évolutions contextuelles.

Par exemple :

- Autorisez l'accès de tous les employés au site Web d'un fournisseur approuvé, même lorsque la stratégie Par défaut bloque l'accès à la catégorie Shopping.
- Bloquez l'accès de tous les clients du rôle Étudiants à une URL non catégorisée qui démontre une hausse suspecte du trafic lors de l'examen de ce site Web.
- Autorisez l'accès à un blog de conception aux trois membres de l'équipe chargée du marketing Web, tout en maintenant le blocage général des accès à la catégorie Blogs et sites personnels.
- Bloquez l'accès d'un utilisateur spécifique à une liste d'URL sur demande du service des ressources humaines.

Pour obtenir des instructions simples sur l'exécution des tâches courantes, consultez la section *Raccourcis des exceptions*, page 110.

Pour obtenir des informations détaillées sur les informations que vous pouvez inclure dans une exception, consultez la section *Gestion des exceptions de filtrage*, page 103.

Gestion des exceptions de filtrage

Rubriques connexes :

- *Ajout ou modification d'une exception de filtrage*, page 106
- *Modification simultanée de plusieurs exceptions de filtrage*, page 109

La page **Gestion des stratégies > Exceptions** vous permet d'afficher, de modifier ou de supprimer des exceptions existantes et d'en ajouter de nouvelles.

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. Pour plus d'informations sur le classement des exceptions dans la liste, consultez la section *Organisation des exceptions*, page 105.

- Lorsque l'exception bloque ou autorise une URL ou une expression régulière unique, celle-ci est répertoriée dans la liste. Si ce n'est pas le cas, cliquez sur le lien de la colonne URL pour obtenir la liste complète des URL affectées.
- Si l'exception affecte :
  - Un client unique, l'adresse IP, la plage d'adresses ou le nom d'affichage de ce client est répertorié dans la liste
  - Un rôle unique, le nom de ce dernier s'affiche au format « Rôle [Nom_Rôle] »
  - Tous les clients de tous les rôles, le terme « Global » s'affiche

    Les exceptions globales que les administrateurs délégués peuvent remplacer sont désignées par une icône dans la colonne Clients (voir *Contournement d'une exception de filtrage*, page 108).
  - Plusieurs clients spécifiques, le nombre de clients s'affiche. Cliquez sur le lien pour obtenir la liste complète des clients concernés.

La liste des exceptions présente également les informations suivantes :

Colonne	Description
Type	Affiche une icône pour indiquer que les URL de l'exception sont : • Bloquées () • Autorisées () • Autorisées avec le remplacement de sécurité désactivé ()
Dernière modification	Présente la date de la dernière modification de l'exception
Expire	Indique si l'exception est associée ou non à une date d'expiration et, dans l'affirmative, présente cette date
Active	Indique si l'exception est actuellement utilisée dans le filtrage (Active) ou non (Inactive)

La liste déroulante **Filtre** vous permet de n'afficher que les exceptions présentant les caractéristiques définies. Les filtres suivants sont disponibles :

Filtre	Description
Autorisé	Exceptions qui autorisent des URL
Bloqué	Exceptions qui bloquent des URL
Active	Exceptions actuellement utilisées dans le filtrage
Inactive	Exceptions actuellement non utilisées dans le filtrage
Will Expire (Expire le)	Exceptions dont la date d'expiration a été définie
Expiré	Exceptions inactives, car parvenues à expiration
Never Expires (N'expire jamais)	Exceptions définies pour toujours rester actives
Global	Exceptions s'appliquant à tous les clients de tous les rôles

Filtre	Description
Tous les clients d'un rôle	Exceptions s'appliquant à tous les clients d'un rôle d'administration déléguée spécifique (y compris le rôle Super administrateur)
Clients spécifiques	Exceptions s'appliquant à un ou plusieurs clients spécifiques

Vous pouvez également utiliser les champs **Rechercher** pour affiner l'affichage des exceptions :

1. Servez-vous de la liste déroulante pour indiquer dans quelles colonnes du tableau les recherches doivent porter.
2. Entrez tout ou partie de la chaîne à identifier.
3. Cliquez sur **Rechercher**.
4. Pour revenir à la vue précédente, cliquez sur **Clear Search Results (Effacer les résultats de la recherche)**.

Pour créer une nouvelle exception, cliquez sur **Ajouter**. Pour obtenir des instructions, consultez la section *Ajout ou modification d'une exception de filtrage*, page 106.

Pour modifier une exception existante, cliquez sur son nom ou cochez la case accolée à une ou plusieurs exceptions, puis cliquez sur **Modifier**. Pour obtenir des instructions, consultez *Ajout ou modification d'une exception de filtrage*, page 106, ou *Modification simultanée de plusieurs exceptions de filtrage*, page 109.

Pour retirer une exception, cochez la case accolée à son nom, puis cliquez sur **Supprimer**.

Organisation des exceptions

L'ordre d'affichage des exceptions dans la page Gestion des stratégies > Exceptions dépend du rôle de l'administrateur.

Dans le cas des Super administrateurs, les exceptions sont regroupées comme suit :

1. Exceptions globales (affectant tous les clients de tous les rôles)
2. Exceptions affectant des clients spécifiques dans la page Clients du rôle Super administrateur
3. Exceptions incluant un ou plusieurs clients auxquels aucun rôle n'a été explicitement affecté (qui ne s'affichent pas dans la page Clients ni dans l'une des listes de clients gérés)
4. Exceptions s'appliquant au rôle Super administrateur dans son intégralité
5. Exceptions s'appliquant aux clients spécifiques d'un autre rôle d'administration déléguée
6. Exceptions s'appliquant à un rôle d'administration déléguée dans son intégralité

Dans le cas des administrateurs délégués des autres rôles, les exceptions sont regroupées comme suit :

1. Exceptions affectant des clients spécifiques du rôle
2. Exceptions affectant le rôle dans son intégralité (exceptions globales comprises)

Dans chaque groupe, les exceptions s'affichent par ordre alphabétique.

Ajout ou modification d'une exception de filtrage

La page **Gestion des stratégies > Exceptions > Ajouter une exception** ou **Modifier une exception** vous permet de créer ou de mettre à jour une exception prioritaire sur le filtrage basé sur la stratégie appliquée à certains des clients qui accèdent à des sites spécifiques.

1. Entrez ou actualisez le **Nom** unique et descriptif de l'exception. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

2. Dans le champ **URL**, entrez la liste des URL ou des adresses IP que l'exception doit autoriser ou bloquer.
   - Si vous entrez une URL au format **domaine.com**, la correspondance entre le domaine et ses sous-domaines (*www.domaine.com*, *sous-domaine.domaine.com*) est établie.
   - Si vous entrez une URL au format **www.domaine.com** :
     - La correspondance avec http://www.domaine.com **est** établie.
     - La correspondance avec http://domaine.com n'est **pas** établie.
     - La correspondance avec http://sous-domaine.domaine.com n'est **pas** établie.

   Entrez une URL ou une adresse IP par ligne.
3. Définissez les **Clients** affectés par cette exception.
   - Les Super administrateurs peuvent créer :
     - Des exceptions **globales** s'appliquant à tous les clients de tous les rôles

       Lorsque vous activez cette option, choisissez également d'activer ou non l'option **Allow delegated administrators to create exceptions that override this exception (Autoriser les administrateurs délégués à créer des exceptions prioritaires sur cette exception)** (voir *Contournement d'une exception de filtrage*, page 108).
     - Des exceptions s'appliquant à **Tous les clients d'un rôle**

       Lorsque vous activez cette option, sélectionnez un rôle dans liste déroulante.
     - Des exceptions s'appliquant à des **Clients spécifiques d'un rôle quelconque**

       Lorsque vous activez cette option, deux listes vous sont proposées. L'une, à gauche, présente tous les clients déjà **définis** : ajoutés en tant que clients gérés dans un rôle d'administration déléguée, ajoutés dans la page Clients de l'un des rôles, ou ajoutés à une exception. L'autre, à droite, présente les clients **Sélectionnés** pour cette exception.

       Les champs de recherche qui s'affichent au-dessus de chaque liste vous permettent de localiser rapidement les clients à ajouter ou à supprimer.

Pour ajouter à l'exception un client qui n'apparaît pas dans la liste de gauche, cliquez sur **Add Other Clients (Ajouter d'autres clients)**, puis ajoutez des clients de type utilisateur, groupe, ordinateur (adresse IPv4 ou IPv6) ou réseau (plage d'adresses IPv4 ou IPv6).

Important

Si vous sélectionnez des clients membres de plusieurs rôles, l'exception est automatiquement divisée lors de sa création afin qu'une nouvelle exception soit créée pour chaque rôle affecté.

Par exemple, si vous définissez une exception intitulée « Autoriser liste Craigs » s'appliquant aux clients des rôles Super administrateur, RH et Installations, trois exceptions sont créées lorsque vous cliquez sur OK.

- Les exceptions destinées aux rôles RH et Installations sont désignées par une icône. Survolez cette icône avec votre souris pour identifier le rôle affecté par l'exception.
- L'exception destinée au rôle Super administrateur n'est pas annotée.

- Les administrateurs délégués peuvent créer des exceptions s'appliquant à **Tous les clients gérés de ce rôle** ou à des **Clients spécifiques de ce rôle**.

  Si vous activez cette dernière option, deux listes vous sont proposées. L'une, à gauche, présente tous les clients **Définis** dans votre liste de clients gérés et dans la page Clients. L'autre, à droite, présente les clients **Sélectionnés** pour cette exception.

  - Les champs de recherche qui s'affichent au-dessus de chaque liste vous permettent de localiser rapidement les clients à ajouter.
  - Si un client n'apparaît pas dans la liste des **clients Définis**, il est probable qu'il soit membre d'un groupe, d'une unité d'organisation ou d'un réseau (plage d'adresses IP) défini(e) en tant que client géré dans votre rôle. Pour ajouter un tel client, cliquez sur **Add Other Clients (Ajouter d'autres clients)**, puis spécifiez l'utilisateur, le groupe ou l'adresse IPv4 ou IPv6 à ajouter.

4. Définissez le **Type** de l'exception. Ce paramètre détermine si le système doit **Bloquer** ou **Autoriser** les URL répertoriées pour les clients spécifiés.
5. Définissez la date à laquelle l'exception **Expire**.
   - Si vous sélectionnez **Jamais**, l'exception est utilisée jusqu'à sa suppression ou jusqu'à ce que vous ajoutiez une autre date d'expiration.
   - Si vous sélectionnez **Après**, entrez une date d'expiration au format mm/jj/aaa ou cliquez sur l'icône du calendrier pour sélectionner une date. Lorsque le jour sélectionné se termine, l'exception expire à minuit (selon l'heure définie dans l'ordinateur Filtering Service).
6. Déterminez l'**État** de l'exception. Par défaut, l'exception est **Active** et est utilisée pour le filtrage dès que vous mettez en cache vos modifications et que vous les enregistrez. Si vous ne voulez pas que l'exception soit utilisée pour l'instant, désactivez cette case à cocher.

7. Par défaut, lorsqu'une URL est associée à une catégorie de risques de sécurité (par exemple Sites Web dangereux ou Logiciels espions), les exceptions autorisées sont ignorées et l'URL est filtrée en fonction de la stratégie active (voir *Définition de la priorité de la catégorisation Risques de sécurité*, page 262) :
   - Lorsqu'un filtre de catégorie bloque la catégorie, la requête est bloquée.
   - Lorsqu'un filtre de catégorie autorise la catégorie, la requête est autorisée.
   - Lorsqu'un filtre d'accès limité est utilisé, la requête est bloquée.

   Pour contourner cette fonctionnalité de sécurité, cliquez sur **Avancé**, puis désactivez la case à cocher **Block URLs that become a security risk, even if they are permitted by exception (Bloquer les URL qui présentent un risque de sécurité, y compris lorsqu'une exception les autorise)**.

   Il n'est pas conseillé de modifier cette option.
8. Pour utiliser des expressions régulières afin de définir les URL que l'exception autorise ou bloque, cliquez sur **Avancé**, puis saisissez une expression par ligne dans la zone **Expressions régulières**.

   Pour valider les expressions créées, cliquez sur **Tester l'expression régulière**.

   > **Avertissement**
   > Utiliser un grand nombre d'expressions régulières, ou des exceptions mal définies ou trop génériques, peut fortement réduire les performances du filtrage.

9. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Exceptions. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Contournement d'une exception de filtrage

Rubriques connexes :

- *Ajout ou modification d'une exception de filtrage*, page 106
- *Lorsque plusieurs exceptions s'appliquent, laquelle est prioritaire ?*, page 109

Par défaut, lorsqu'un Super administrateur crée une exception, celle-ci est prioritaire sur toute autre exception créée par un administrateur délégué.

Par exemple :

- Une exception de Super administrateur global bloque le site **monsite.com**, tandis qu'une exception d'administrateur délégué autorise le site **monsite.com** pour certains clients gérés.

  L'URL est alors bloquée par défaut.
- Une exception de Super administrateur global autorise le site **autresite.com**, tandis qu'une exception d'administrateur délégué bloque ce même site.

L'URL est alors autorisée par défaut.

Lorsqu'ils créent une exception, les Super administrateurs ont toutefois la possibilité d'activer l'option **Allow delegated administrators to create exceptions that override this exception (Autoriser les administrateurs délégués à créer des exceptions contournant cette exception)**. Lorsque cette option est activée, les exceptions des administrateurs délégués sont prioritaires sur celle du Super administrateur.

Par exemple :

- Une exception de Super administrateur global autorise le site **siteexemple.com**, tandis qu'une exception d'administrateur délégué bloque le site **siteexemple.com** pour le rôle d'administration déléguée.

  L'URL est bloquée pour les clients du rôle d'administration déléguée.
- Une exception de Super administrateur global bloque le site **exemple.com**, tandis qu'une exception d'administrateur délégué autorise le site **exemple.com** pour un client géré.

  L'URL est alors autorisée pour ce client géré.

Les exceptions de Super administrateur qui peuvent être contournées sont désignées par une icône () dans la colonne Clients de la page de Gestion des stratégies > Exceptions.

Lorsque plusieurs exceptions s'appliquent, laquelle est prioritaire ?

Par défaut, les exceptions de Super administrateur sont prioritaires sur les exceptions créées par les administrateurs délégués. Par conséquent, lorsqu'une exception de Super administrateur bloque une URL, tandis qu'une exception d'administrateur délégué l'autorise, la requête est **bloquée**.

Toutefois, si le Super administrateur configure l'exception de manière à autoriser le contournement par l'administrateur délégué (voir *Contournement d'une exception de filtrage*, page 108), l'exception créée par ce dernier est prioritaire. Ainsi, lorsqu'une exception de Super administrateur bloque une URL, alors qu'une exception d'administrateur délégué l'autorise, la requête est **autorisée**.

Lorsque plusieurs exceptions équivalentes peuvent s'appliquer à une requête (par exemple, lorsque plusieurs exceptions de Super administrateur incluent la même URL) :

- Filtering Service consultant d'abord la liste des exceptions bloquées, lorsqu'une même exception est à la fois bloquée et autorisée, la requête est **bloquée**.
- En présence de plusieurs exceptions bloquées, la première exception détectée est appliquée.
- Lorsqu'il n'y a pas d'exception bloquée et qu'il existe plusieurs exceptions autorisées, la première exception autorisée est appliquée.

Après avoir créé une exception, servez-vous de l'outil Tester le filtrage (voir *Tester le filtrage*, page 283) pour vérifier que les requêtes des clients sont filtrées comme prévu.

Modification simultanée de plusieurs exceptions de filtrage

La page **Gestion des stratégies > Exceptions > Edit Exceptions (Modifier les exceptions)** permet de modifier simultanément plusieurs exceptions de filtrage.

Lorsque vous modifiez plusieurs exceptions, vous pouvez modifier uniquement le type d'exception (autorisée ou bloquée), les paramètres d'expiration (n'expire jamais ou date d'expiration), l'état (active ou inactive) ou les paramètres de contournement de sécurité (si les URL d'une exception autorisée sont autorisées ou bloquées lorsque le logiciel de filtrage de Websense détecte un risque de sécurité).

Cliquez sur le lien **View details of each selected exception (Afficher les détails de chaque exception sélectionnée)** situé en haut de la page pour obtenir des informations sur les exceptions que vous modifiez.

1. Vérifiez le **Type** de l'exception (Bloquer ou Autoriser). Pour apporter une modification, cliquez sur **Modifier** et choisissez un autre élément.
2. Pour mettre à jour le paramètre **Expire** de l'exception, cliquez sur **Modifier**, puis :
   - Si vous sélectionnez **Jamais**, l'exception est utilisée jusqu'à sa suppression ou jusqu'à ce que vous ajoutiez une autre date d'expiration.
   - Si vous sélectionnez **Après**, entrez une date d'expiration au format mm/jj/aaa ou cliquez sur l'icône du calendrier pour sélectionner une date.
3. Pour mettre à jour l'**État** de l'exception, cliquez sur **Modifier**, puis activez ou désactivez la case à cocher **Active**. Les exceptions inactives ne sont pas utilisées dans le filtrage.
4. Par défaut, lorsque Websense Web Security détermine qu'une URL présente un risque de sécurité (par exemple, lorsqu'elle héberge un logiciel espion ou malveillant), l'URL est bloquée, y compris lorsque l'exception l'autorise.

   Pour mettre à jour les paramètres de sécurité actuels d'une exception autorisée, cliquez sur **Avancé**, puis sur **Modifier**. Activez ou désactivez la case à cocher **Block URLs that become a security risk, even if they are permitted by exception (Bloquer les URL qui présentent un risque de sécurité, y compris lorsqu'une exception les autorise)**.

   Il n'est pas conseillé de désactiver la protection du contournement de sécurité par défaut.
5. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Exceptions. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Raccourcis des exceptions

Pour effectuer les tâches courantes le plus rapidement possible, servez-vous des raccourcis suivants.

Pour les Super administrateurs :

- *Comment bloquer ou autoriser une URL pour tous ?*, page 111
- *Comment bloquer ou autoriser une URL pour une seule personne ?*, page 111

Pour les administrateurs délégués :

- *Comment bloquer ou autoriser une URL pour l'ensemble de mon rôle d'administration déléguée ?*, page 112
- *Comment bloquer ou autoriser une URL pour l'un de mes clients gérés ?*, page 112

Pour tous les administrateurs :

- *Comment créer une URL non filtrée ?*, page 113

Comment bloquer ou autoriser une URL pour tous ?

Pour bloquer ou autoriser une URL pour tous les utilisateurs du réseau, 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 ou bloquer.
4. Par défaut, l'exception est définie pour s'appliquer à tous les clients (l'option **Globale** 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** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

Comment bloquer ou autoriser une URL pour une seule personne ?

Pour bloquer ou autoriser une URL pour un seul client du réseau, quel que soit son rôle, 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 ou bloquer.
4. Pour spécifier le client affecté par cette exception, sélectionnez **Specific clients in any role (Clients spécifiques d'un rôle quelconque)**.
5. Entrez tout ou partie du nom d'utilisateur ou de l'adresse IP dans le champ de recherche situé au-dessus de la liste **Clients définis**, puis appuyez sur **Entrée**.
   - Si le client apparaît dans les résultats de la recherche, sélectionnez-le, puis cliquez sur la flèche droite (>) pour l'envoyer dans la liste **Sélectionné**.
   - Si le client n'est pas répertorié dans les résultats de la recherche, cliquez sur **Add Other Clients (Ajouter d'autres clients)**, puis :
     - Sélectionnez un nom d'utilisateur ou de groupe dans la liste ou cliquez sur **Rechercher** pour localiser un utilisateur ou un groupe dans le répertoire des utilisateurs.
     - Entrez une adresse IP ou une plage d'adresses IP au format IPv4 ou IPv6.

     Lorsque vous avez identifié le client à ajouter, servez-vous de la flèche droite appropriée (>) pour l'envoyer dans la liste Sélectionné, puis cliquez sur **OK**.
6. Par défaut, l'exception est définie sur **Bloquer l'URL**. Pour modifier ce paramètre, définissez le **Type** sur **Autoriser**.
7. Définissez au besoin une date d'expiration.

8. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

Comment bloquer ou autoriser une URL pour l'ensemble de mon rôle d'administration déléguée ?

Pour bloquer ou autoriser une URL pour tous les clients gérés du rôle dont ils assurent la gestion, les administrateurs délégués peuvent procéder comme suit :

> **Important**
>
> Les exceptions créées par un Super administrateur peuvent être prioritaires sur celles que créent les administrateurs délégués.
>
> Si vous créez une exception qui semble ne pas être appliquée à vos clients gérés, servez-vous de l'outil **Tester le filtrage** pour voir si une autre exception remplace celle que vous avez créée (voir *Tester le filtrage*, page 283).

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 ou bloquer.
4. Par défaut, l'exception est définie pour s'appliquer à **Tous les clients gérés de ce rôle**.
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** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

Comment bloquer ou autoriser une URL pour l'un de mes clients gérés ?

Pour bloquer ou autoriser une URL pour l'un de leurs clients gérés, les administrateurs délégués peuvent procéder comme suit.

> **Important**
>
> Les exceptions créées par un Super administrateur peuvent être prioritaires sur celles que créent les administrateurs délégués.
>
> Si vous créez une exception qui semble ne pas être appliquée à vos clients gérés, servez-vous de l'outil **Tester le filtrage** pour voir si une autre exception remplace celle que vous avez créée (voir *Tester le filtrage*, page 283).

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 ou bloquer.
4. Pour spécifier le client affecté par cette exception, sélectionnez **Clients spécifiques de ce rôle**.
5. Entrez tout ou partie du nom d'utilisateur ou de l'adresse IP dans le champ de recherche situé au-dessus de la liste **Clients définis**, puis appuyez sur **Entrée**.
   - Si le client apparaît dans les résultats de la recherche, sélectionnez-le, puis cliquez sur la flèche droite (>) pour l'envoyer dans la liste **Sélectionné**.
   - Si le client est membre d'un groupe, d'une unité d'organisation ou d'un réseau (plage d'adresses IP) défini en tant que client géré dans votre rôle, mais ne s'affiche pas explicitement dans la liste Clients gérés ou dans votre page Clients, il n'apparaîtra pas dans les résultats de vos recherches.

     Dans ce cas, annulez la création de l'exception, ajoutez ce client dans votre page Clients, puis recréez l'exception. Cette fois, le client apparaîtra dans vos résultats de recherche à la page Ajouter des exceptions.
6. Par défaut, l'exception est définie sur **Bloquer l'URL**. Pour modifier ce paramètre, définissez le **Type** sur **Autoriser**.
7. Définissez au besoin une date d'expiration.
8. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

Comment créer une URL non filtrée ?

Lorsque vous effectuez une mise à niveau à partir de la version 7.6 ou d'une version antérieure, vos URL non filtrées existantes sont converties en exceptions autorisées. Les URL non filtrées créées par :

- Les Super administrateurs deviennent des exceptions globales qui autorisent l'URL ou l'expression régulière pour tous les clients de tous les rôles.
- Les administrateurs délégués deviennent des exceptions autorisées à l'échelle du rôle et autorisent l'URL ou l'expression régulière pour tous les clients d'un rôle.

Pour autoriser une URL pour tous les utilisateurs (Super administrateurs uniquement) ou pour tous les membres du rôle dont vous assurez la gestion, consultez :

- *Comment bloquer ou autoriser une URL pour tous ?*, page 111
- *Comment bloquer ou autoriser une URL pour l'ensemble de mon rôle d'administration déléguée ?*, page 112

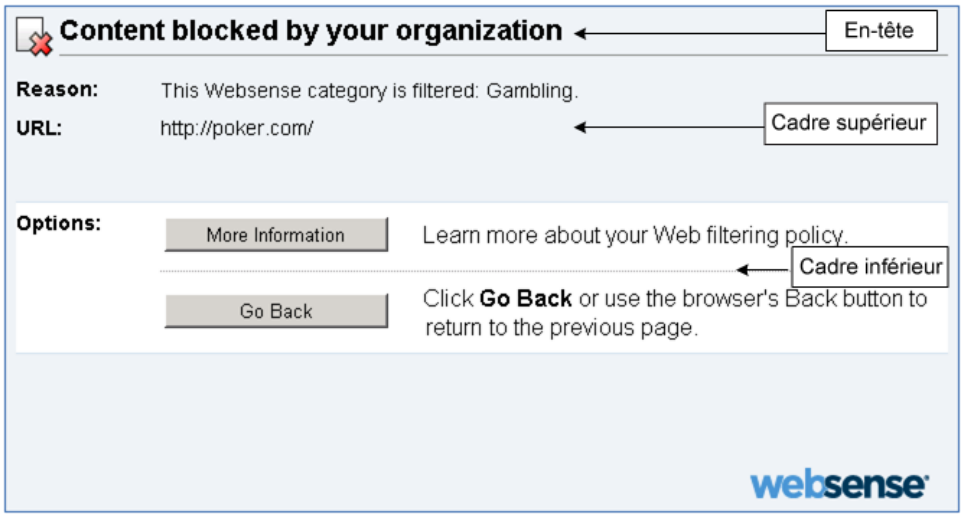
7 Pages de blocage

Rubriques connexes :

- *Blocage des publicités graphiques*, page 117
- *Blocage des pages intégrées*, page 117
- *Messages de blocage de protocoles*, page 118
- *Fonctionnement des pages de blocage*, page 119
- *Création de messages de blocage alternatifs*, page 125
- *Utilisation d'une page de blocage alternative dans un autre ordinateur*, page 126
- *Identification de la cause du blocage d'une requête*, page 127

Lorsqu'il bloque un site Web, Websense Web Security affiche une page de blocage dans le navigateur du client.

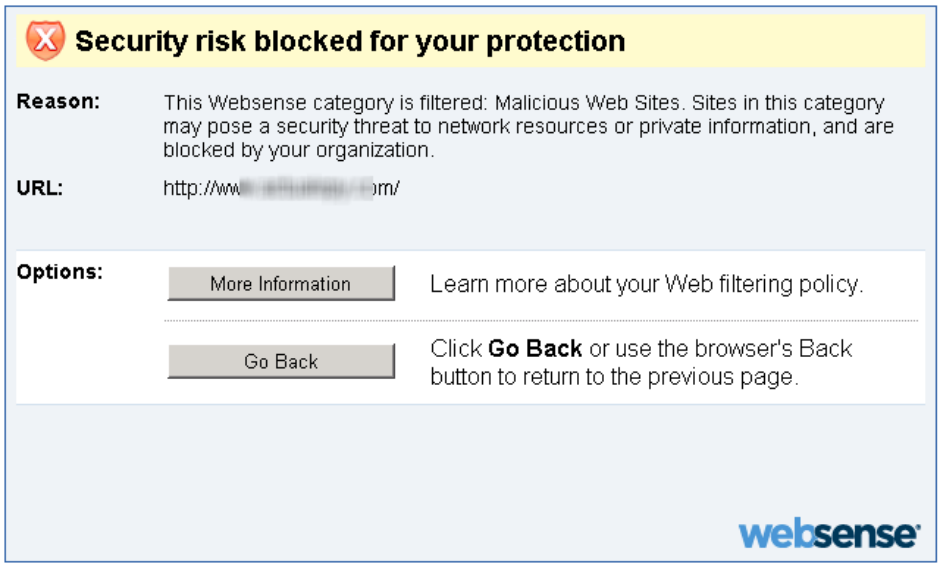
Les pages de blocage sont conçues à partir de fichiers HTML et comprennent par défaut trois sections principales.



- L'**en-tête** explique que le site est bloqué.
- Le **cadre supérieur** contient le message de blocage, l'URL demandée et la raison du blocage.

- Le **cadre inférieur** présente les options proposées à l'utilisateur, par exemple la possibilité de revenir à la page précédente, ou de cliquer sur un bouton Continuer ou Utiliser du temps contingenté pour consulter le site.

Si le site est bloqué parce qu'il appartient à une catégorie de la classe Risques pour la sécurité (voir *Classes de risque*, page 54), une page de blocage de sécurité s'affiche.



Dans les déploiements Websense Web Security Gateway et Gateway Anywhere, les Super administrateurs peuvent activer une version améliorée de la page de blocage afin d'inclure un lien qui permet d'accéder à Websense ACEInsight.

- Activez ce lien dans la page Paramètres > Général > Filtrage.
- Ce lien permet aux utilisateurs d'obtenir des informations sur les URL bloquées pour des raisons de sécurité.

Des fichiers de pages de blocage par défaut sont inclus dans Websense. Vous pouvez exploiter ces fichiers par défaut ou créer vos propres versions personnalisées.

> **Remarque**
>
> Dans les déploiements Websense Web Security Gateway Anywhere, les modifications apportées aux pages de blocage locales n'affectent pas les pages de blocage du filtrage hybride. Voir *Personnalisation des pages de blocage du service hybride*, page 217.

- Personnalisez les fichiers par défaut pour modifier le message de blocage (voir *Fonctionnement des pages de blocage*, page 119).
- Configurez Websense pour qu'il utilise des messages de blocage (par défaut ou personnalisés) hébergés dans un serveur Web distant (voir *Utilisation d'une page de blocage alternative dans un autre ordinateur*, page 126).

Blocage des publicités graphiques

Dans certains cas, Websense affiche un très petit fichier d'image vide (BlockImage.gif) à la place de la page de blocage standard ou de sécurité. Cela se produit dans les cas suivants :

- La catégorie Publicités est bloquée, et
- Un site tente d'afficher une image (par exemple un fichier GIF ou JPG) hébergée dans une URL de la catégorie Publicités.

Les publicités s'affichent souvent dans les cadres ou les iframes d'une page présentant également des informations non publicitaires. Dans ce cas, les publicités graphiques de la page prennent généralement la forme de cadres blancs (vides). Le contenu restant du site s'affiche normalement.

Dans certains cas, un site peut être composé en intégralité d'images publicitaires. Dans ce cas, le navigateur de l'utilisateur affiche une page Web blanche à la place du message de blocage standard. Les utilisateurs peuvent voir que le site a été bloqué à cause de son URL, qui ressemble à ceci :

```
http://<adresse IP de Filtering Service>:15871/cgi-bin/
blockpage.cgi?ws-session=<numéro de session>
```

Si vous préférez afficher une autre image que l'image de blocage d'un pixel par défaut, il vous suffit de remplacer le fichier par défaut :

1. Accédez au répertoire de stockage des pages de blocage dans l'ordinateur Filtering Service (C:\Program Files\Websense\Web Security\BlockPages\Images ou /opt/Websense/BlockPages/Images, par défaut).
2. Créez une copie de sauvegarde du fichier **blockImage.gif** d'origine.
3. Nommez votre image **blockImage.gif** et copiez-la dans le répertoire Images (en remplaçant le fichier d'origine).

Blocage des pages intégrées

La plupart des pages Web renferment un contenu issu de plusieurs sources (serveurs de publicités, sites de vidéos en streaming, applications de réseaux sociaux, services d'hébergement d'images, etc.). Certains sites agrègent du contenu en insérant différents éléments de plusieurs sites dans une même présentation.

Dans ce cas, les utilisateurs peuvent demander des sites qui combinent à la fois du contenu autorisé et bloqué.

Lorsqu'un cadre ou une iframe d'une page plus vaste renferme du contenu bloqué, Websense affiche une page de blocage standard ou de sécurité dans ce cadre. Lorsque le cadre en question est petit, toutefois, l'utilisateur peut ne voir qu'une petite partie de la page (pas même l'icône de blocage complète, dans certains cas), et ne pas comprendre la raison du blocage.

Pour contourner ce problème, les utilisateurs peuvent survoler la partie visible de la page de blocage avec leur souris pour afficher une petite fenêtre contextuelle de style info-bulle présentant un bref message de blocage. Un clic sur ce message permet d'afficher la page de blocage complète dans une autre fenêtre.

Pour revenir en arrière et parcourir le contenu autorisé de la page d'origine, les utilisateurs doivent fermer la fenêtre qui présente la page de blocage. Du fait des restrictions du navigateur, cliquer sur le bouton Précédent d'une page de blocage ouverte à partir d'un cadre n'a aucun effet.

Si la page de blocage qui s'affiche dans une nouvelle fenêtre propose une option Utiliser du temps contingenté ou Continuer, un clic sur ce bouton :

1. Ferme la nouvelle fenêtre (contextuelle)
2. Affiche le contenu précédemment bloqué (et uniquement ce contenu) dans la fenêtre d'origine du navigateur

Pour afficher la page d'origine, y compris le contenu précédemment bloqué, procédez de l'une des manières suivantes :

- Saisissez à nouveau l'URL du site.
- Servez-vous du bouton Précédent du navigateur pour revenir au site, puis actualisez la page.

Messages de blocage de protocoles

Rubriques connexes :

- *Fonctionnement des pages de blocage*, page 119
- *Création de messages de blocage alternatifs*, page 125
- *Utilisation d'une page de blocage alternative dans un autre ordinateur*, page 126

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

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

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

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

- Pour afficher des messages de blocage de protocoles sur les ordinateurs clients fonctionnant sous Windows NT, XP ou 200x, le service Windows Messenger doit être activé. Ce service est désactivé par défaut. Dans la boîte de dialogue Services de Windows de l'ordinateur client, vous pouvez vérifier si le service Messenger s'exécute (voir *Boîte de dialogue Services de Windows*, page 515).
- Pour afficher des messages de blocage de protocoles sur un ordinateur Windows 98, lancez **winpopup.exe**, situé dans le répertoire Windows. Exécutez cette application depuis une invite de commande ou configurez-la pour qu'elle s'exécute automatiquement en la copiant dans le dossier Startup.

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

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

Fonctionnement des pages de blocage

Rubriques connexes :

- *Messages de blocage de protocoles*, page 118
- *Personnalisation du message de blocage*, page 121
- *Création de messages de blocage alternatifs*, page 125
- *Utilisation d'une page de blocage alternative dans un autre ordinateur*, page 126

Les fichiers qui servent à créer les pages de blocage Websense sont stockés dans le répertoire suivant :

- Sous Windows :

  ```
  C:\Program Files\Websense\Web Security\BlockPages\
  <code_langue>\Default
  ```

  ou

  ```
  C:\Program Files (x86)\Websense\Web Security\BlockPages\
  <code_langue>\Default
  ```

- Sous Linux :

  ```
  /opt/Websense/BlockPages/<code_langue>/Default
  ```

> **Remarque**
>
> Dans les déploiements Websense Web Security Gateway Anywhere, ces pages de blocage ne s'appliquent qu'aux utilisateurs filtrés par le logiciel sur site. Pour personnaliser les pages fournies par le filtrage hybride, consultez la section *Personnalisation des pages de blocage du service hybride*, page 217.

Deux fichiers HTML principaux sont utilisés pour créer les pages de blocage :

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

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

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

Par ailleurs, plusieurs fichiers pris en charge servent à générer le contenu et le style du texte et les fonctions des boutons des pages de blocage :

Nom du fichier	Description
blockStyle.css	Feuille de style en cascade (CSS) contenant la plupart des styles des pages de blocage
master.css	Feuille de style en cascade (CSS) contenant les styles des fenêtres contextuelles des pages de blocage (par exemple la fenêtre contextuelle du remplacement de compte)
popup.html	Lorsqu'une page intégrée est bloquée (voir *Blocage des pages intégrées*, page 117), ce fichier sert à afficher la fenêtre contextuelle de la page de blocage en pleine page.
block.inl	Fournit les outils servant à créer le cadre de blocage de la page de blocage
blockframe.inl	Fournit d'autres informations pour les pages de blocage standard
continueframe.inl	Fournit d'autres informations sur le cadre de blocage lorsque les utilisateurs disposent de l'option Continuer
quotaframe.inl	Fournit d'autres informations sur le cadre de blocage lorsque les utilisateurs disposent de l'option Utiliser du temps contingenté
base64.js	Fichier JavaScript servant à prendre en charge le cryptage des identifiants de connexion lorsque les utilisateurs disposent d'une option Remplacement de compte. Il est préférable de ne pas modifier ni supprimer ce fichier.
master.js	Fichier JavaScript utilisé pour créer une page de blocage standard
security.js	Fichier JavaScript utilisé pour créer une page de blocage de sécurité
messagefile.txt	Contient les chaînes de texte utilisées dans les pages de blocage
WebsenseCopyright.txt	Information relatives aux droits d'auteur des pages de blocage Websense
master.wml	Fichier WML contenant des informations de blocage de base

Dans les déploiements qui incluent des composants Web DLP (Prévention de perte de données), un fichier supplémentaire (**policyViolationDefaultPage.html**) fournit le contenu de la page de blocage lorsque des composants Websense Data Security bloquent la publication du contenu sur Internet ou le téléchargement à partir du Web.

Personnalisation du message de blocage

Rubriques connexes :

- *Modification de la taille du cadre du message*, page 122
- *Modification du logo affiché sur la plage de blocage*, page 123
- *Utilisation des variables du contenu de la page de blocage*, page 123
- *Réinitialisation des pages de blocage par défaut*, page 125

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

- Modifiez l'apparence de la page de blocage pour utiliser le logo, les couleurs et le style de votre organisation.
- Ajoutez des informations sur les stratégies d'utilisation d'Internet dans votre organisation
- Proposez une méthode permettant de contacter un administrateur et d'obtenir des informations sur les stratégies d'utilisation d'Internet.

Pour créer vos propres pages de blocage personnalisées :

1. Naviguez jusqu'au répertoire de stockage des pages de blocage de Websense. Pour l'anglais :

   ```
   Websense/Web Security/BlockPages/en/Default
   ```

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

   ```
   Websense/Web Security/BlockPages/en/Custom
   ```

Remarque

Ne modifiez **pas** les fichiers des messages de blocage d'origine dans le répertoire **BlockPages/en/Default**. Copiez-les dans le répertoire **BlockPages/en/Custom** et modifiez leurs copies.

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

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

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

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

5. Certains fichiers HTML des pages de blocage utilisent des chemins codés en dur pour référencer les fichiers pris en charge utilisés pour créer la page. Si vous avez modifié la feuille de style utilisée pour mettre en forme les pages de blocage (**blockStyle.css**) ou le fichier JavaScript servant à créer les pages de blocage de sécurité (**security.js**), prenez également soin d'actualiser le chemin d'accès à ces fichiers dans vos fichiers HTML personnalisés. Par exemple :

   ```
   <link rel="stylesheet" href="/en/Custom/blockStyle.css
   type="text>
   ```

6. Enregistrez le fichier.
7. Redémarrez Websense Filtering Service (voir *Arrêt et démarrage des services Websense*, page 375, pour plus d'instructions).

Modification de la taille du cadre du message

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

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

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

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

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

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

   Vous pouvez également modifier la valeur du paramètre **height** pour modifier la hauteur du cadre.
5. Enregistrez et fermez le fichier.

6. Redémarrez Filtering Service pour implémenter ces modifications (voir *Arrêt et démarrage des services Websense*, page 375).

Modification du logo affiché sur la plage de blocage

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

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

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

   - Remplacez **wslogo_block_page.png** par le nom du fichier image contenant le logo de votre organisation.
   - Remplacez les valeurs du paramètre **title** par le nom de votre organisation.
4. Enregistrez et fermez le fichier.
5. Redémarrez Filtering Service pour implémenter ces modifications (voir *Arrêt et démarrage des services Websense*, page 375).

Utilisation des variables du contenu de la page de blocage

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

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

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

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

Ici, *WS_USERNAME* représente la variable.

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

Nom de la variable	Objectif
WS_URL	Affiche l'URL demandée
WS_BLOCKREASON	Affiche la raison pour laquelle le site a été bloqué (c'est-à-dire l'action de filtrage appliquée)
WS_ISSECURITY	Indique si le site demandé appartient à l'une des catégories de la classe Risques pour la sécurité. Si la valeur est TRUE, la page de blocage de sécurité est affichée.
WS_PWOVERRIDECGIDATA	Renseigne un champ de saisie du code HTML de la page de blocage avec les informations relatives à l'utilisation du bouton **Accès par mot de passe**
WS_QUOTA_CGIDATA	Renseigne un champ de saisie du code HTML de la page de blocage avec les informations relatives à l'utilisation du bouton **Utiliser du temps contingenté**
WS_PASSWORDOVERRID_BEGIN, WS_PASSWORDOVERRID_END	Impliqué dans l'activation de la fonction d'accès par mot de passe
WS_MOREINFO	Présente des informations détaillées (apparaissant lorsque l'utilisateur clique sur le lien **Plus d'informations**) sur le motif de blocage du site
WS_POLICYINFO	Désigne la stratégie régissant le client à l'origine de la requête
WS_MOREINFOCGIDATA	Envoie des données à Filtering Service sur l'utilisation du lien **Plus d'informations**
WS_QUOTATIME	Présente la quantité de temps contingenté restant pour le client à l'origine de la requête
WS_QUOTAINTERVALTIME	Présente la durée de la session de temps contingenté configurée pour le client à l'origine de la requête
WS_QUOTABUTTONSTATE	Indique si le bouton **Utiliser du temps contingenté** est activé ou désactivé pour une requête particulière
WS_SESSIONID	Joue le rôle d'identifiant interne associé à une requête
WS_TOPFRAMESIZE	Indique la taille (sous forme de pourcentage) de la partie supérieure d'une page de blocage envoyée par un serveur de blocage personnalisé, lorsqu'un tel serveur est configuré
WS_BLOCKMESSAGE_PAGE	Indique la source à utiliser pour le cadre supérieur d'une page de blocage
WS_CATEGORY	Présente la catégorie de l'URL bloquée
WS_CATEGORYID	Identifiant unique de la catégorie de l'URL demandée

Réinitialisation des pages de blocage par défaut

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

1. Supprimez tous les fichiers du répertoire **Websense/BlockPages/en/Custom**. Par défaut, Websense réutilisera les fichiers du répertoire Default.
2. Redémarrez Filtering Service (voir *Arrêt et démarrage des services Websense*, page 375).

Création de messages de blocage alternatifs

Rubriques connexes :

- *Fonctionnement des pages de blocage*, page 119
- *Personnalisation du message de blocage*, page 121

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

- Créez des messages de blocage distincts pour chacun des trois protocoles : HTTP, FTP et Gopher.
- Hébergez ces fichiers dans l'ordinateur Websense, ou dans votre serveur Web interne (voir *Utilisation d'une page de blocage alternative dans un autre ordinateur*, page 126).

Après avoir créé des fichiers alternatifs pour les messages de blocage, vous devez configurer Websense pour qu'il affiche ces nouveaux messages (voir *Configuration des paramètres de filtrage de Websense*, page 67). Cette procédure vous permet de définir le message utilisé pour chacun des protocoles configurables.

Utilisation d'une page de blocage alternative dans un autre ordinateur

Rubriques connexes :

- *Fonctionnement des pages de blocage*, page 119
- *Personnalisation du message de blocage*, page 121
- *Création de messages de blocage alternatifs*, page 125

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

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

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

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

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

1. Arrêtez les services Websense Filtering Service et Policy Server, dans cet ordre (voir *Arrêt et démarrage des services Websense*, page 375).
2. Dans l'ordinateur Filtering Service, localisez le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
3. Créez une copie de sauvegarde du fichier **eimserver.ini** et stockez-la dans un autre répertoire.
4. Ouvrez le fichier **eimserver.ini** dans un éditeur de texte, puis localisez la section **[WebsenseServer]** (en haut du fichier).
5. Entrez le nom d'hôte ou l'adresse IP du serveur hébergeant la page de blocage dans le format suivant :

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

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

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

Identification de la cause du blocage d'une requête

Pour examiner la raison pour laquelle une requête a été bloquée, vous pouvez utiliser les informations disponibles dans le code source de la page de blocage.

- Si la page de blocage a été envoyée par Filtering Service (pour les utilisateurs filtrés par le dispositif ou le logiciel sur site), cliquez sur **Plus d'informations**. Cliquez ensuite du bouton droit n'importe où dans le texte du message et sélectionnez **View Source (Afficher la source)**. Voir *Requête bloquée par Filtering Service*, page 127.
- Si la page de blocage a été envoyée par le filtrage hybride (dans les environnements Websense Web Security Gateway Anywhere), cliquez du bouton droit n'importe où dans le message de blocage et sélectionnez **View Source (Afficher la source)**. Voir *Requête bloquée par le filtrage hybride*, page 128.

Requête bloquée par Filtering Service

La source HTML de la page de blocage des informations complémentaires présente des renseignements sur la personne à l'origine de la demande de site et les critères utilisés pour filtrer la requête. Elle précise, en particulier :

- Le nom d'utilisateur et l'adresse IP source de la requête (si disponible) et l'heure (au format HH:MM) à laquelle la requête a eu lieu
- La stratégie appliquée à la requête, en précisant si elle a été attribuée à l'utilisateur, au groupe, au domaine, à l'ordinateur (adresse IP individuelle) ou au réseau (plage d'adresses IP)

  Si plusieurs stratégies de groupe pouvaient s'appliquer, le message indique également si le paramètre **Utiliser un blocage plus restrictif** est utilisé. Voir *Configuration des paramètres de filtrage de Websense*, page 67.
- L'aspect de la stratégie ayant entraîné le blocage de la requête (par exemple, la catégorie ou le filtre d'accès limité, le type de fichier, le mot-clé, l'utilisation de la bande passante)
- Le nom du rôle auquel cette stratégie a été affectée
- Les ressources utilisées pour classer le site (Base de données principale de Websense, mise à jour de base de données en temps réel, expression régulière incluse dans la mise à jour de la base de données en temps réel, URL personnalisée, mot-clé, analyse Websense Web Security Gateway, etc.)

Par exemple :

```
User Name: WinNT://Test/tester1 Source IP Address:
10.12.132.17 Current Time: 15:30

Ce réseau (10.12.132.0 à 10.12.132.255) est filtré par la
stratégie : role-8**Default. La stratégie inclut un filtre
de catégories ou d'accès limité pour l'heure en cours.

Cette stratégie est associée au rôle : Super administrateur.

La requête a été catégorisée par : la base de données
principale de Websense.
```

Ici, la requête a été filtrée par une stratégie (Par défaut) appliquée au réseau (plage d'adresses IP) dont était membre l'ordinateur de l'utilisateur. L'affectation de la stratégie a été effectuée dans le rôle Super administrateur et le site demandé a été catégorisé par la Base de données principale.

Requête bloquée par le filtrage hybride

La source HTML de la page de blocage envoyée par le filtrage hybride présente des informations sur le mode de catégorisation utilisé pour le site demandé et le mode d'application de la stratégie à la requête. Elle précise, en particulier :

- Le nom du rôle auquel cette stratégie a été affectée. Voir *Rôles d'administration déléguée*, page 324.
- La catégorie affectée au site
- La ou les stratégies affectées à la requête
- Si le blocage de type de fichier a été utilisé, quel type de fichier a été appliqué
- Le protocole (HTTP, HTTPS ou FTP sur HTTP) utilisé pour la requête
- Les ressources utilisées pour classer le site (Base de données principale de Websense, mise à jour de base de données en temps réel, expression régulière incluse dans la mise à jour de la base de données en temps réel, URL personnalisée, mot-clé, analyse Websense Web Security Gateway, etc.)
- Si un problème a empêché le service hybride de fournir la raison du blocage d'une requête, ou si le service hybride a rencontré une erreur lors de l'affichage de la page blocage, le champ **Exception reason (Motif de l'exception)** contient une explication et un code d'erreur numérique. Si le problème est récurrent, le Support technique de Websense peut utiliser ce code d'erreur pour le résoudre.

Par exemple :

```
Rôle : Super administrateur
Catégorie : Partage de fichiers en P2P
Stratégie : Par défaut
Domaine :
Groupe :
Type de fichier :
Réseau :
Protocole : http
Chaîne Category Reason (Motif de la catégorie) : Base de
données principale
Exception reason (Motif de l'exception) :
```

Ici, la requête a été filtrée par une stratégie (Par défaut) du rôle Super administrateur qui bloque la catégorie Partage de fichiers en P2P. Le site HTTP demandé a été catégorisé par la Base de données principale.

8 Exploitation des rapports pour évaluer l'efficacité du filtrage

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Rapports d'investigation*, page 152
- *Rapports sur activité propre*, page 177
- *Real-Time Monitor*

TRITON - Web Security offre plusieurs outils de génération de rapports qui permettent d'évaluer l'efficacité de vos stratégies de filtrage. (Log Server, composant propre à Windows, doit être installé pour pouvoir activer toutes les fonctions de génération de rapports, sauf Real-Time Monitor.)

> **Remarque**
>
> Dans les organisations qui utilisent l'administration déléguée, il est possible les fonctions de génération de rapports ne soient pas toutes disponibles pour tous les administrateurs. Voir *Administration déléguée et génération de rapports*, page 323.

- Les informations fournies par les **graphiques du Tableau de bord Web Security** sur les menaces, les risques, l'utilisation et le système vous permettent d'examiner l'activité Internet de votre réseau en un seul coup d'œil. Dans la plupart des graphiques, la période, le style des graphiques et le jeu de résultats affichés sont personnalisables. Voir *Tableau de bord de Web Security*, page 33.
- **Les rapports de présentation** présentent une liste de rapports prédéfinis, de rapports personnalisés et de modèles de rapport. Les rapports peuvent être affichés sous forme de graphiques à barres, de graphiques de tendance et de tableaux.

  Copiez l'un des rapports prédéfinis appliquant vos propres filtres pour créer un rapport personnalisé, ou créez votre propre rapport à partir d'un modèle. Pour des informations complètes, consultez la section *Rapports de présentation*, page 131.
- Les **rapports d'investigation** vous permettent de parcourir le contenu de la journalisation de façon interactive. La page principale présente un graphique à barres qui résume l'activité par classe de risques. Cliquez sur les différents éléments de la page pour actualiser le graphique ou obtenir une vue différente des données.

  Consultez la section *Rapports d'investigation*, page 152 pour plus d'informations sur les nombreuses manières d'afficher les données de l'activité Internet.

- **Real-Time Monitor** donne de précieux renseignements sur l'activité actuelle du filtrage Internet au sein de votre réseau, en présentant les URL demandées et l'action appliquée à chaque requête. Dans les déploiements Websense Web Security Gateway et Web Security Gateway Anywhere, Real-Time Monitor présente également les sites analysés par Content Gateway. Lorsqu'un site est recatégorisé dynamiquement sur la base des résultats de l'analyse, la catégorie d'origine et la catégorie actuelle sont toutes deux indiquées.

  Pour plus d'informations, consultez la section *Real-Time Monitor*, page 178.

> **Important**
>
> L'Affichage de compatibilité Internet Explorer 8 n'est **pas** pris en charge avec la console TRITON. En cas de comportement étrange de la génération des rapports ou de problème de mise en page dans Internet Explorer 8, vérifiez que le bouton Affichage de compatibilité (situé entre l'URL et le bouton Actualiser de la barre d'adresse du navigateur) n'est pas activé.

Qu'est-ce que le temps de navigation sur Internet ?

Rubriques connexes :

- *Tâches de la base de données*, page 407
- *Configuration des options du temps de navigation sur Internet*, page 414

Vous pouvez générer des rapports de présentation et d'investigation présentant le **temps de navigation sur Internet (IBT)**, c'est-à-dire le temps passé par un individu à naviguer sur des sites Internet. Aucun logiciel ne peut vous dire avec précision combien de temps un individu consulte réellement un site spécifique à partir de son ouverture. L'utilisateur peut ouvrir un site, le consulter pendant quelques secondes, puis répondre à un appel téléphonique professionnel avant de demander un autre site. L'utilisateur peut également consulter chaque site pendant quelques minutes avant de passer au suivant.

Websense comprend une tâche de Base de données d'activité qui permet de calculer le temps de navigation sur Internet (IBT), à l'aide d'une formule basée sur certaines valeurs configurables. Cette tâche s'exécutant une fois par jour, certaines informations relatives au temps de navigation peuvent ne pas figurer dans les données de journalisation réelles. Pour plus d'informations, consultez la section *Tâches de la base de données*, page 407.

Pour les calculs du temps de navigation, la session Internet commence lorsque l'utilisateur ouvre un navigateur. Elle se poursuit tant que l'utilisateur demande d'autres pages Internet au moins toutes les trois minutes. (Ce seuil de temps de lecture par défaut est configurable. Voir *Configuration des options du temps de navigation sur Internet*, page 414.)

La session Internet se termine lorsque plus de trois minutes se sont écoulées sans que l'utilisateur ne demande un autre site. Websense calcule le temps total de la session, à partir de l'heure de la première requête jusqu'à ce que trois minutes se soient écoulées après la dernière.

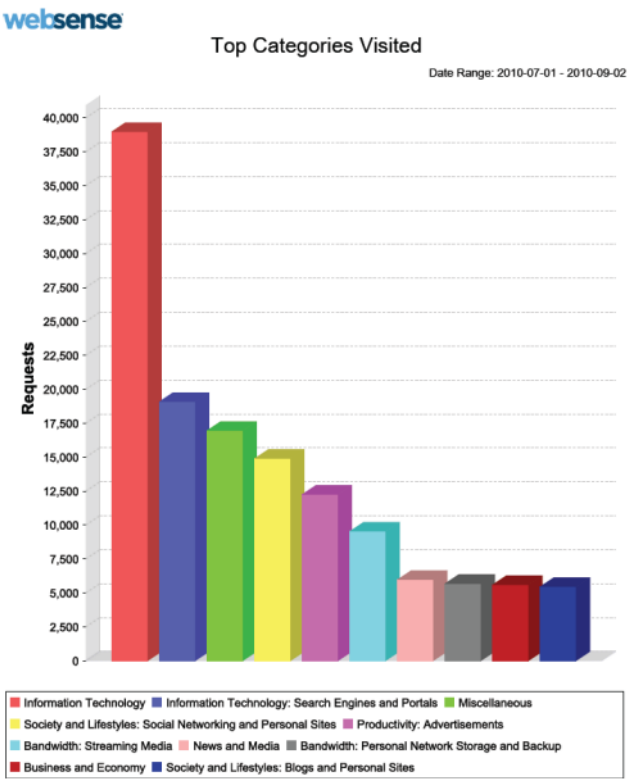
Une nouvelle session commence lorsque l'utilisateur demande d'autres sites après plus de trois minutes. En général, le temps de navigation d'un utilisateur comprend plusieurs sessions quotidiennes.

Rapports de présentation

Rubriques connexes :

- *Création d'un nouveau rapport de présentation*, page 133
- *Fonctionnement des favoris*, page 141
- *Exécution d'un rapport de présentation*, page 142
- *Planification des rapports de présentation*, page 143
- *Affichage de la liste des tâches planifiées*, page 149

La page **Génération de rapports** > **Rapports de présentation** permet de générer des rapports sous forme de graphiques à barres, de graphiques de tendance et de tableaux au format HTML, PDF ou Microsoft Excel (XLS).



Les rapports et les modèles sont disponibles dans le Catalogue de rapports, qui les classe dans les **catégories de rapports** associées. Les catégories de rapports et les rapports prédéfinis présents dans ce catalogue dépendent de votre abonnement. Un abonnement Websense Web Security Gateway ou Gateway Anywhere est par exemple nécessaire pour les rapports de catégories tels que Risques de sécurité en temps réel et Activité d'analyse.

- Pour afficher les rapports ou les modèles inclus dans une catégorie, développez cette dernière.
- Cliquez sur le titre d'un rapport pour obtenir une brève description de son contenu.

Pour générer un rapport de présentation :

1. Sélectionnez le rapport dans le catalogue, puis cliquez sur **Exécuter**. La page Run Report (Exécuter le rapport) s'affiche.
2. Définissez les détails du rapport selon les instructions de la section *Exécution d'un rapport de présentation*, page 142.
   - Si vous exécutez le rapport au premier plan (sans planifier son exécution), il n'est pas automatiquement enregistré lorsque vous fermez l'application utilisée pour l'afficher (navigateur Web, Adobe Reader ou Microsoft Excel, par exemple). Vous devez enregistrer le rapport manuellement.
   - Si vous exécutez le rapport en arrière-plan (planification d'une exécution immédiate), une copie est enregistrée dès que le rapport est terminé et un lien permettant d'accéder à ce rapport s'affiche dans la page Review Reports (Examiner les rapports).

Pour utiliser l'un des modèles, des rapports prédéfinis ou des rapports personnalisés du catalogue de rapports comme base du nouveau rapport :

1. Sélectionnez un nom de rapport ou de modèle dans le catalogue.

   Si vous sélectionnez un modèle de rapport :
   - Un **Nouveau rapport de tendances** présente les tendances de l'activité Internet dans le temps.
   - Un **Nouveau rapport N premiers** affiche les principaux niveaux de l'activité Internet présentant les caractéristiques que vous avez définies.
2. Cliquez sur **Enregistrer sous**.
3. Saisissez le nom, le titre et la catégorie de rapport du nouveau fichier.

   Si vous utilisez un modèle de rapport, définissez également les dimensions de ce dernier (par exemple, ce qui est mesuré et l'unité de mesure).

   Pour plus d'informations, consultez la section *Création d'un nouveau rapport de présentation*, page 133.
4. Pour affiner votre rapport, modifiez son filtre. Ce filtre contrôle les éléments tels que les utilisateurs, les catégories, les protocoles et les actions à inclure dans votre rapport.

   Pour plus d'informations, consultez la section *Définition du filtre du rapport*, page 135.

Pour modifier le filtre d'un rapport personnalisé, sélectionnez ce rapport, puis cliquez sur **Modifier**. Vous ne pouvez pas modifier ni supprimer les rapports prédéfinis et les modèles de rapport.

Pour supprimer un rapport personnalisé, sélectionnez-le, puis cliquez sur **Supprimer**. Si les rapports supprimés apparaissent dans des tâches planifiées, ils continuent à être générés avec ces tâches. Pour plus d'informations sur la modification et la suppression des tâches planifiées, consultez la section *Affichage de la liste des tâches planifiées*, page 149.

Les rapports fréquemment utilisés sont marqués comme Favoris pour vous aider à les retrouver plus rapidement. Sélectionnez simplement le rapport, puis cliquez sur **Favoris** (voir *Fonctionnement des favoris*, page 141). Cochez la case **Afficher uniquement les favoris** pour afficher uniquement les modèles que vous avez désignés comme favoris dans le Catalogue de rapports.

Servez-vous des boutons présents en haut de la page pour planifier l'exécution ultérieure des rapports, afficher les tâches de rapport planifiées, et afficher et gérer les rapports créés par le planificateur.

- Cliquez sur **Planificateur** pour définir une tâche contenant un ou plusieurs rapports à exécuter à un moment spécifique ou de façon périodique. Voir *Planification des rapports de présentation*, page 143.
- Cliquez sur **File d'attente de tâches** pour afficher et gérer la liste des tâches planifiées existantes, ainsi que l'état de chaque tâche. Voir *Affichage de la liste des tâches planifiées*, page 149.
- Cliquez sur **Review Reports (Examiner les rapports)** pour afficher et gérer la liste des rapports qui ont déjà été planifiés et exécutés. Voir *Examen des rapports de présentation planifiés*, page 151.

Création d'un nouveau rapport de présentation

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Définition du filtre du rapport*, page 135
- *Exécution d'un rapport de présentation*, page 142

La page **Save As New Report (Enregistrer sous forme de nouveau rapport)** vous permet de créer :

- Une version modifiable d'un rapport prédéfini
- Une copie d'un rapport personnalisé existant, afin d'y appliquer d'autres filtres
- Un nouveau rapport à partir d'un modèle

Les options disponibles dans cette page varient selon l'option sélectionnée.

Si vous créez une copie d'un rapport prédéfini ou personnalisé :

1. Remplacez le **Nom du rapport** par un nom simplifiant son identification. (Le nom par défaut correspond au nom du modèle de rapport d'origine, auquel est ajouté un nombre indiquant qu'il s'agit d'une copie.)

   Le nom doit comprendre 1 à 85 caractères et ne doit pas correspondre au nom d'un rapport déjà existant.
2. Entrez un **Titre de rapport**. Ce titre s'affichera en haut de la page lors de la génération du rapport.
3. Sélectionnez une **Catégorie de rapport**. Ce paramètre définit le mode de classement du rapport dans le Catalogue de rapports. L'option Rapports définis par l'utilisateur est la valeur par défaut.
4. Procédez de l'une des manières suivantes :
   - Cliquez sur **Enregistrer** pour enregistrer la nouvelle version du rapport et revenir au Catalogue de rapports.
   - Cliquez sur **Enregistrer et modifier** pour modifier le filtre du nouveau rapport (voir *Définition du filtre du rapport*, page 135).
   - Cliquez sur **Annuler** pour abandonner vos modifications et revenir au Catalogue de rapports.

Si vous utilisez un modèle de rapport pour en créer un nouveau :

1. Entrez un **Nom de rapport** unique. Ce nom apparaîtra dans le Catalogue de rapports.

   Le nom doit comprendre 1 à 85 caractères et ne doit pas correspondre au nom d'un rapport déjà existant.
2. Entrez un **Titre de rapport**. Ce titre s'affichera en haut de la page lors de la génération du rapport.
3. Sélectionnez une **Catégorie de rapport**. Ce paramètre définit le mode de classement du rapport dans le Catalogue de rapports. L'option Rapports définis par l'utilisateur est la valeur par défaut.
4. Si vous créez un rapport N premiers, passez à l'étape 5.

   Si vous créez un rapport de tendance, définissez l'**unité de temps** de l'axe des X du graphique. Vous pouvez créer un rapport présentant les tendances par jour (par défaut), semaine, mois ou année.

   - Pour être certain que les données désirées s'affichent dans le rapport de tendance, assurez-vous que le **premier jour** de la première semaine, du premier mois ou de la première année à inclure soit défini en tant que première date de la plage. (Par défaut, le premier jour de la semaine est le dimanche, mais cela peut dépendre de votre configuration Microsoft SQL Server et de vos paramètres régionaux.)
   - Lorsque les informations des utilisateurs sont mises à jour dans le service d'annuaire, les informations relatives aux groupes d'utilisateurs peuvent également changer. Les rapports de tendance de groupes hebdomadaires, mensuels et annuels peuvent donc être affectés puisque, pour être inclus dans un rapport de groupe, l'utilisateur doit être membre de ce groupe un jour avant le début de la période sélectionnée au moins.

     Par exemple, pour que l'activité d'un utilisateur soit incluse dans un rapport de tendance de groupe d'Août 2012, cet utilisateur doit être membre du groupe dès le 31 juillet 2012. Un utilisateur rejoignant le groupe le 23 août 2012 (un mercredi) sera inclus dans les rapports de tendance quotidienne qui commencent le jour suivant, dans les rapports de tendance hebdomadaire qui commencent le samedi, le dimanche ou le lundi suivant (selon la configuration de SQL Server) et dans les rapports de tendance mensuelle qui commencent le 1er septembre 2012.
5. Servez-vous de la liste déroulante **Activité Internet par** pour sélectionner les éléments visés par le rapport. Vous pouvez afficher l'activité Internet par catégorie (par défaut), protocole, classe de risques, action (par exemple autorisée ou bloquée), utilisateur ou groupe.
6. Servez-vous de la liste déroulante **Measure by (Mesurer par)** pour indiquer comment mesurer l'élément visé par le rapport. Vous pouvez effectuer des mesures par requête (par défaut), bande passante ou temps de navigation.
7. Procédez de l'une des manières suivantes :
   - Cliquez sur **Enregistrer** pour enregistrer le rapport et revenir au Catalogue de rapports. Le nouveau rapport s'affiche alors dans la catégorie de rapports que vous avez sélectionnée à l'étape 5.
   - Cliquez sur **Enregistrer et modifier** pour modifier le filtre du nouveau rapport. La procédure de modification du filtre de rapport est la même que pour tout rapport personnalisé (voir *Définition du filtre du rapport*, page 135).
   - Cliquez sur **Annuler** pour abandonner vos modifications et revenir au Catalogue de rapports.

Définition du filtre du rapport

Rubriques connexes :

- *Création d'un nouveau rapport de présentation*, page 133
- *Exécution d'un rapport de présentation*, page 142

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

> **Remarque**
>
> L'utilisation d'un logo personnalisé requiert une certaine préparation avant la définition du filtre de rapport. Vous devez en effet créer l'image dans un format pris en charge et placer ce fichier dans l'emplacement approprié. Voir *Personnalisation du logo des rapports*, page 140.

Les options disponibles dans le filtre varient :

- Si vous modifiez un rapport prédéfini ou un rapport personnalisé basé sur un rapport prédéfini, les options disponibles dans le filtre dépendent du rapport sélectionné.

  Par exemple, si vous avez sélectionné un rapport d'informations de groupe, tel que Principaux groupes bloqués par requête, vous pouvez contrôler les groupes s'affichant dans le rapport mais pas choisir les utilisateurs individuels.

- Si vous modifiez un rapport créé à l'aide du modèle Nouveau rapport N premiers ou Nouveau rapport de tendances, **toutes** les options s'affichent dans le filtre, y compris lorsqu'elles ne sont pas applicables dans ce rapport personnalisé.

  Prenez soin de ne sélectionner que les options pertinentes pour votre rapport.

Le filtre des rapports prédéfinis ne peut pas être modifié. Vous pouvez modifier le filtre d'un rapport personnalisé lors de sa création en sélectionnant **Enregistrer et modifier** dans la page Save As New Report (Enregistrer sous forme de nouveau rapport), ou sélectionner à tout moment le rapport dans le Catalogue de rapports et cliquer sur **Modifier**.

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

- *Sélection des clients pour un rapport*, page 136
- *Sélection des catégories pour un rapport*, page 137
- *Sélection des protocoles pour un rapport*, page 138
- *Sélection des actions pour un rapport*, page 138
- *Définition des options du rapport*, page 139

Dans l'onglet **Confirmer**, choisissez d'exécuter ou de planifier le rapport, et enregistrez son filtre. Voir *Confirmation de la définition du filtre de rapport*, page 140.

Sélection des clients pour un rapport

Rubriques connexes :

- *Sélection des catégories pour un rapport*, page 137
- *Sélection des protocoles pour un rapport*, page 138
- *Sélection des actions pour un rapport*, page 138
- *Définition des options du rapport*, page 139
- *Confirmation de la définition du filtre de rapport*, page 140

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

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

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

1. Sélectionnez un type de clients dans la liste déroulante.
2. Définissez le nombre maximal de résultats de la recherche dans la liste **Limiter la recherche**.

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

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

   Définissez soigneusement votre chaîne de recherche pour être certain que tous les résultats désirés soient inclus dans le nombre de résultats limitant la recherche.
4. Mettez en surbrillance une ou plusieurs entrées dans la liste des résultats, puis cliquez sur la flèche droite (>) pour les déplacer vers la liste **Sélectionné**.
5. Répétez les étapes 2 à 4 autant de fois que nécessaire pour effectuer d'autres recherches et ajouter d'autres clients dans la liste Sélectionné.
6. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Catégories. Voir *Sélection des catégories pour un rapport*, page 137.

Sélection des catégories pour un rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 136
- *Sélection des protocoles pour un rapport*, page 138
- *Sélection des actions pour un rapport*, page 138
- *Définition des options du rapport*, page 139
- *Confirmation de la définition du filtre de rapport*, page 140

L'onglet **Catégories** de la page Rapports de présentation > Modifier le filtre du rapport permet de contrôler les informations incluses dans votre rapport en fonction des catégories ou des classes de risques. Voir *Classes de risque*, page 54.

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

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

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

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

   Remarque

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

2. Cochez la case de chaque catégorie ou classe de risques à inclure dans votre rapport.

   Utilisez les boutons **Sélectionner tout** et **Effacer tout** situés sous la liste pour réduire le nombre de sélections individuelles requises.

3. Cliquez sur la flèche droite (>) pour déplacer vos sélections vers la liste **Sélectionné**.

   Lorsque vous cochez une classe de risques, un clic sur la flèche droite place toutes ses catégories associées dans la liste Sélectionné.

4. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Protocoles. Voir *Sélection des protocoles pour un rapport*, page 138.

Sélection des protocoles pour un rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 136
- *Sélection des catégories pour un rapport*, page 137
- *Sélection des actions pour un rapport*, page 138
- *Définition des options du rapport*, page 139
- *Confirmation de la définition du filtre de rapport*, page 140

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

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

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

   Utilisez les boutons **Sélectionner tout** et **Effacer tout** situés sous la liste pour réduire le nombre de sélections individuelles requises.
3. Cliquez sur la flèche droite (>) pour déplacer vos sélections vers la liste **Sélectionné**.
4. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Actions. Voir *Sélection des actions pour un rapport*, page 138.

Sélection des actions pour un rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 136
- *Sélection des catégories pour un rapport*, page 137
- *Sélection des protocoles pour un rapport*, page 138
- *Définition des options du rapport*, page 139
- *Confirmation de la définition du filtre de rapport*, page 140

L'onglet **Actions** de la page Rapports de présentation > Modifier le filtre du rapport permet de contrôler avec précision les actions de filtrage (par exemple, autorisées par filtre d'accès limité ou bloquées par temps contingenté) incluses dans votre rapport. Si votre rapport indique qu'il ne s'applique qu'aux requêtes bloquées, vous ne pouvez sélectionner que les actions liées au blocage (bloquées par type de fichier, par mots-clés, etc.).

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

1. Cliquez sur l'icône placée à côté du nom du groupe pour développer et réduire les groupes d'actions.

2. Cochez la case de chaque action à inclure dans votre rapport.

   Utilisez les boutons **Sélectionner tout** et **Effacer tout** situés sous la liste pour réduire le nombre de sélections individuelles requises.

3. Cliquez sur la flèche droite (>) pour déplacer vos sélections vers la liste **Sélectionné**.
4. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Options. Voir *Définition des options du rapport*, page 139.

Définition des options du rapport

Rubriques connexes :

- *Personnalisation du logo des rapports*, page 140
- *Sélection des clients pour un rapport*, page 136
- *Sélection des catégories pour un rapport*, page 137
- *Sélection des protocoles pour un rapport*, page 138
- *Sélection des actions pour un rapport*, page 138
- *Définition des options du rapport*, page 139
- *Confirmation de la définition du filtre de rapport*, page 140

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

1. Au besoin, modifiez le **Nom du Catalogue de rapports**. Ce nom doit inclure 1 à 85 caractères.

   Ce nom n'apparaît pas dans le rapport lui-même mais permet seulement d'identifier une combinaison unique de format et de filtre dans le Catalogue de rapports.

2. Modifiez le **Titre du rapport** affiché dans le rapport. Ce titre peut comprendre jusqu'à 85 caractères.
3. Modifiez la **Description** affichée dans le Catalogue de rapports. Cette description peut comprendre jusqu'à 336 caractères.

   La description doit permettre d'identifier cette combinaison unique de format et de filtre dans le Catalogue de rapports.

4. Sélectionnez le logo à afficher dans votre rapport.

   Tous les fichiers image pris en charge dans le répertoire approprié sont énumérés. Voir *Personnalisation du logo des rapports*, page 140.

5. Cochez la case **Enregistrer comme favori** pour que ce rapport apparaisse dans les Favoris.

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

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

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

7. Lorsque vos sélections sont terminées, cliquez sur **Suivant** pour ouvrir l'onglet Confirmer. Voir *Confirmation de la définition du filtre de rapport*, page 140.

Personnalisation du logo des rapports

Par défaut, les rapports de présentation affichent le logo Websense dans le coin supérieur gauche. Lorsque vous créez un rapport personnalisé et que vous modifiez son filtre, vous pouvez choisir un autre logo.

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

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

2. Le nom du fichier image ne doit pas dépasser 25 caractères, extension comprise.
3. Copiez ce fichier image dans le répertoire **ReportTemplates\images**. Le chemin par défaut est :

   ```
   C:\Program Files (x86)\Websense\Web Security\Manager\
      ReportTemplates\images
   ```

Tous les fichiers image pris en charge dans ce répertoire apparaissent automatiquement dans la liste déroulante de l'onglet Options dans la page Modifier le filtre du rapport. L'image est automatiquement mise à l'échelle en fonction de l'espace affecté au logo. (Voir *Définition des options du rapport*, page 139.)

> **Remarque**
>
> Ne supprimez pas et ne modifiez pas les images actives dans les filtres de rapport. En l'absence du fichier de logo, le rapport ne peut pas être généré.

Confirmation de la définition du filtre de rapport

Rubriques connexes :

- *Sélection des clients pour un rapport*, page 136
- *Sélection des catégories pour un rapport*, page 137
- *Sélection des protocoles pour un rapport*, page 138
- *Sélection des actions pour un rapport*, page 138
- *Définition des options du rapport*, page 139

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

1. Vérifiez le **Nom** et la **Description** de votre rapport.

   Si des modifications sont nécessaires, cliquez sur **Précédent** pour revenir à l'onglet Options et apporter les modifications désirées. (Voir *Définition des options du rapport*, page 139.)

2. Indiquez ensuite ce que vous souhaitez faire :

Option	Description
Enregistrer	Enregistre le filtre du rapport et rouvre le Catalogue de rapports. Voir *Rapports de présentation*, page 131.
Enregistrer et exécuter	Enregistre le filtre du rapport et ouvre la page Exécuter le rapport. Voir *Exécution d'un rapport de présentation*, page 142.
Enregistrer et planifier	Enregistre le filtre du rapport et ouvre la page Planifier le rapport. Voir *Planification des rapports de présentation*, page 143.

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

Fonctionnement des favoris

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Exécution d'un rapport de présentation*, page 142
- *Planification des rapports de présentation*, page 143

Vous pouvez désigner tout rapport de présentation, personnalisé ou modèle, en tant que Favori. Utilisez cette option pour identifier les rapports que vous générez le plus souvent et que vous souhaitez pouvoir localiser rapidement dans le Catalogue de rapports.

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

   Un symbole en forme d'étoile s'affiche dans la liste à côté du nom des rapports favoris, ce qui vous permet de les identifier rapidement lorsque tous les rapports sont affichés.

3. Cochez la case **Afficher uniquement les favoris**, située au-dessus du Catalogue de rapports, pour limiter la liste aux rapports désignés comme Favoris. Désactivez cette option pour restaurer la liste complète des rapports.

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

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

2. Cliquez sur **Favori**.

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

Exécution d'un rapport de présentation

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Planification des rapports de présentation*, page 143

La page **Rapports de présentation > Run Report (Exécuter le rapport)** permet de générer un seul rapport immédiatement. Vous pouvez également créer les tâches associées à un ou plusieurs rapports et planifier leur exécution unique ou récurrente (voir *Planification des rapports de présentation*, page 143).

Remarque

Avant de générer un rapport au format PDF, assurez-vous qu'Adobe Reader v7.0 ou une version ultérieure est installé dans votre ordinateur local.

Avant de générer un rapport au format XLS, assurez-vous que Microsoft Excel 2003 ou une version ultérieure est installé dans votre ordinateur local.

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

Pour exécuter un rapport :

1. Sélectionnez la **Date de début** et la **Date de fin** pour définir la période couverte par votre rapport.
2. Sélectionnez le **Format de sortie** du rapport.

Format	Description
PDF	Portable Document Format. Les fichiers PDF sont mis en forme pour l'affichage et peuvent être ouverts dans Adobe Reader.
HTML	HyperText Markup Language. Les fichiers HTML sont mis en forme pour l'affichage et peuvent être ouverts dans un navigateur.
XLS	Feuille de calcul Excel. Les fichiers XLS sont mis en forme en vue d'une réutilisation et peuvent être ouverts dans Microsoft Excel.

3. Si vous sélectionnez un rapport **N premiers**, choisissez le nombre d'éléments devant apparaître dans votre rapport.
4. Définissez le mode de génération désiré pour votre rapport :

- Sélectionnez l'option **Schedule the report to run in the background (Planifier l'exécution du rapport en arrière-plan)** (activée par défaut) pour que le rapport s'exécute immédiatement sous forme de tâche planifiée. Vous pouvez éventuellement définir l'adresse électronique à avertir lorsque le rapport est terminé. Vous pouvez également définir l'adresse électronique à avertir lorsque le rapport ne peut pas être généré. (Vous pouvez aussi surveiller la file d'attente des tâches pour vérifier l'état de votre rapport.)
- Désactivez l'option **Schedule the report to run in the background (Planifier l'exécution du rapport en arrière-plan)** pour que votre report s'exécute au premier plan. Dans ce cas, le rapport n'est pas planifié et n'apparaît pas dans la page Review Reports (Examiner les rapports).

> **Remarque**
>
> Si vous envisagez d'exécuter plusieurs rapports au premier plan, veillez à utiliser le bouton **Fermer** pour fermer la fenêtre contextuelle qui présente les messages de génération de rapports et de rapport terminé. Si vous utilisez le bouton de fermeture (X) du navigateur, il est possible que les prochaines tentatives d'exécution des rapports au premier plan échouent jusqu'à ce que vous quittiez la page Rapports de présentation avant de la rouvrir et de réexécuter le rapport.

5. Cliquez sur **Exécuter**.
   - Si vous planifiez le rapport pour une exécution immédiate, le rapport terminé est automatiquement enregistré et ajouté dans la liste Review Reports (Examiner les rapports). Pour afficher, enregistrer ou supprimer le rapport, cliquez sur **Review Reports (Examiner les rapports)** en haut de la page Rapports de présentation.
   - Si vous avez choisi d'exécuter le rapport au premier plan, une nouvelle fenêtre de navigateur s'affiche et présente la progression de l'opération. Dès qu'ils sont terminés, les rapports HTML s'affichent dans la fenêtre du navigateur. Dans le cas des formats PDF et XLS, vous avez la possibilité d'ouvrir le rapport ou de l'enregistrer sur le disque.

     Avec cette option, les rapports de présentation ne stockent pas automatiquement une copie du rapport. Pour enregistrer une copie à consulter ultérieurement, servez-vous de la fonction intégrée à l'application utilisée pour ouvrir le rapport.
6. Pour imprimer un rapport, utilisez la commande Imprimer de l'application utilisée pour afficher le rapport.

   Pour de meilleurs résultats lors de l'impression, générez une sortie au format PDF. Servez-vous ensuite des options d'impression d'Adobe Reader.

Planification des rapports de présentation

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Exécution d'un rapport de présentation*, page 142
- *Affichage de la liste des tâches planifiées*, page 149

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

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

Les rapports terminés sont également répertoriés dans la page Rapports de présentation > Review Reports (Examiner les rapports) (voir *Examen des rapports de présentation planifiés*, page 151).

Pour accéder au Planificateur :

- Cliquez sur le bouton **Planificateur** situé en haut de la page Rapports de présentation (au-dessus du Catalogue de rapports).
- Si vous modifiez un filtre du rapport, choisissez **Enregistrer et planifier** dans l'onglet Confirmer, puis cliquez sur **Terminer** (voir *Définition du filtre du rapport*, page 135).
- Cliquez sur le lien du nom de la tâche dans la page File d'attente des tâches pour modifier une tâche.
- Cliquez sur **Ajouter** dans la page File d'attente des tâches pour créer une nouvelle tâche.

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

- *Définition du planning*, page 145
- *Sélection des rapports à planifier*, page 147
- *Définition de la plage de dates*, page 147
- *Sélection des options de sortie*, page 148

Après avoir créé des tâches, servez-vous de la File d'attente des tâches pour afficher leur état et d'autres informations utiles (voir *Affichage de la liste des tâches planifiées*, page 149).

Après l'exécution d'un rapport de présentation planifié, son fichier terminé est envoyé aux destinataires sous forme de pièce jointe de messagerie électronique appelée **presentationreport_0**. Ce nombre est incrémenté en fonction du nombre de rapports joints.

Les rapports planifiés sont automatiquement enregistrés dans le répertoire **ReportingOutput** de l'ordinateur TRITON - Web Security (C:\Program Files (x86)\Websense\Web Security\ReportingOutput, par défaut). Notez que le nom de la pièce jointe envoyée par courrier électronique ne correspond pas à celui du fichier stocké dans le répertoire ReportingOutput. Le meilleur moyen de localiser un rapport spécifique consiste à utiliser la page Review Reports (Examiner les rapports), dans laquelle vous pouvez effectuer des recherches par date ou nom de tâche, ou encore par nom de rapport.

Les rapports sont automatiquement supprimés de la page Review Reports (Examiner les rapports) et du répertoire ReportingOutput lorsque la période définie dans la page Paramètres > Génération de rapports > Préférences (5 jours, par défaut) s'est écoulée. Si vous souhaitez conserver certains de vos rapports plus longtemps, incluez-les dans votre routine de sauvegarde ou enregistrez leurs fichiers dans un emplacement autorisant le stockage à long terme.

Une alerte s'affiche dans la page Review Reports (Examiner les rapports) quelques jours avant que le rapport ne soit supprimé (3 jours, par défaut). Pour modifier ce délai d'avertissement, utilisez la page Paramètres > Génération de rapports > Préférences.

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

Websense génère le rapport au format choisi : PDF (Adobe Reader), XLS (Microsoft Excel) ou HTML. Si vous choisissez le format HTML, il est possible que votre rapport s'affiche dans le panneau de contenu de TRITON - Web Security. Les rapports affichés dans ce panneau de contenu ne peuvent pas être imprimés ni enregistrés dans un fichier. Pour imprimer un rapport ou l'enregistrer dans un fichier, choisissez le format PDF ou XLS.

Important

Pour pouvoir afficher les rapports de présentation au format PDF, Adobe Reader v7.0 ou une version ultérieure doit être installé dans votre ordinateur local.

Pour pouvoir afficher les rapports de présentation au format XLS, Microsoft Excel 2003 ou une version ultérieure doit être installé dans votre ordinateur local.

Définition du planning

Rubriques connexes :

- *Planification des rapports de présentation*, page 143
- *Sélection des rapports à planifier*, page 147
- *Sélection des options de sortie*, page 148
- *Définition de la plage de dates*, page 147

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

Remarque

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

1. Entrez un **nom de tâche** identifiant de façon unique cette tâche planifiée.

2. Sélectionnez le **Modèle de récurrence** et les **Options de récurrence** de la tâche. Les différentes options disponibles dépendent du modèle sélectionné.

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

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

   La tâche démarre en fonction de l'heure définie sur l'ordinateur dans lequel s'exécute TRITON - Web Security.

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

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

Option	Description
Aucune date de fin	La tâche poursuit indéfiniment son exécution selon le planning établi. Pour l'interrompre par la suite, modifiez-la ou supprimez-la. Voir *Affichage de la liste des tâches planifiées*, page 149.
Finir après	Sélectionnez le nombre de fois où la tâche doit s'exécuter. Après ce nombre d'occurrences, la tâche ne s'exécute plus, mais demeure dans la file d'attente jusqu'à ce que vous la supprimiez. Voir *Affichage de la liste des tâches planifiées*, page 149.
Finir le	Définissez la date à laquelle l'exécution de la tâche doit s'arrêter. Après cette date, elle ne s'exécute plus.

5. Cliquez sur **Suivant** pour ouvrir l'onglet Rapports. Voir *Sélection des rapports à planifier*, page 147.

Sélection des rapports à planifier

Rubriques connexes :

- *Planification des rapports de présentation*, page 143
- *Définition du planning*, page 145
- *Sélection des options de sortie*, page 148
- *Définition de la plage de dates*, page 147

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

1. Sélectionnez un rapport pour cette tâche dans le Catalogue de rapports.
2. Cliquez sur la flèche droite (>) pour déplacer ce rapport vers la liste **Sélectionné**.
3. Répétez les étapes 1 et 2 jusqu'à ce que tous les rapports de cette tâche s'affichent dans la liste **Sélectionné**.
4. Cliquez sur **Suivant** pour ouvrir l'onglet Intervalle de dates. Voir *Définition de la plage de dates*, page 147.

Définition de la plage de dates

Rubriques connexes :

- *Planification des rapports de présentation*, page 143
- *Définition du planning*, page 145
- *Sélection des rapports à planifier*, page 147
- *Sélection des options de sortie*, page 148

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

Intervalle de dates	Description
Toutes les dates	Les rapports comprennent toutes les dates disponibles dans la Base de données d'activité. Aucune entrée supplémentaire n'est nécessaire. Lorsque cette option est utilisée pour des tâches récurrentes, les mêmes informations peuvent apparaître en double dans des rapports exécutés séparément.
Dates spécifiques	Sélectionnez les heures exactes de début (**Du**) et de fin (**Au**) des rapports de cette tâche. Cette option est idéale pour les tâches qui ne s'exécutent qu'une seule fois. Choisir cette option pour un planning récurrent entraîne des rapports en double.

Intervalle de dates	Description
Dates relatives	Utilisez les listes déroulantes pour choisir le nombre de périodes devant faire l'objet des rapports (Ce/cette, Dernier(ère), Deux dernier(ère)s, etc.), et le type de période (Jours, Semaines ou Mois). Par exemple, la tâche peut couvrir les deux dernières semaines ou le mois en cours. Une semaine représente une semaine de calendrier, du dimanche au samedi. Un mois représente un mois du calendrier. Par exemple, Cette semaine produit un rapport allant du dimanche à la date du jour ; Le mois en cours produit un rapport allant du premier jour du mois à la date du jour ; La semaine dernière produit un rapport allant du dimanche au samedi précédent, etc. Cette option est idéale pour les tâches qui s'exécutent de manière récurrente. Il vous permet de choisir la quantité de données apparaissant dans chaque rapport et de réduire le nombre de données en double dans les rapports exécutés séparément.

Après avoir défini la plage de dates de votre tâche, cliquez sur **Suivant** pour afficher l'onglet Sortie. Voir *Sélection des options de sortie*, page 148.

Sélection des options de sortie

Rubriques connexes :

- *Planification des rapports de présentation*, page 143
- *Définition du planning*, page 145
- *Sélection des rapports à planifier*, page 147
- *Définition de la plage de dates*, page 147

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

1. Sélectionnez le format de fichier du rapport final.

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

2. Entrez les adresses électroniques qui doivent recevoir le rapport.

   Chaque adresse doit être placée sur une ligne distincte.

3. Au besoin, cochez la case **Personnaliser le sujet et le corps du courrier électronique**. Dans ce cas, entrez le texte personnalisé **Objet** et **Corps** du courrier électronique de cette tâche.

4. Cliquez sur **Enregistrer une tâche** pour enregistrer et implémenter la définition de votre tâche et afficher la page File d'attente des tâches.
5. Vérifiez cette tâche et les autres tâches planifiées. Voir *Affichage de la liste des tâches planifiées*, page 149.

Affichage de la liste des tâches planifiées

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Planification des rapports de présentation*, page 143
- *Sélection des options de sortie*, page 148
- *Planification des rapports d'investigation*, page 172

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

(Pour revoir les tâches planifiées pour les rapports d'investigation, consultez la section *Gestion des tâches planifiées de rapports d'investigation*, page 174.)

La liste fournit les informations suivantes pour chaque tâche.

Colonne	Description
Nom de tâche	Nom donné à la tâche lors de sa création
État	Indique si la tâche est • en exécution • planifiée (en attente de la prochaine exécution planifiée) • terminée avec succès • en échec • n'a pas été déclenchée (ne s'est pas exécutée à la dernière exécution planifiée, à cause d'un problème de mémoire faible ou de fermeture du serveur, par exemple)
État	L'état peut être : • ACTIVÉ, indique que la tâche s'exécute en fonction du modèle de récurrence établi • DÉSACTIVÉ, indique que la tâche est inactive et ne s'exécute pas
Récurrence	Modèle de récurrence (Une fois, Quotidien, Hebdomadaire, Mensuel) défini pour cette tâche
Historique	Cliquez sur le lien **Détails** pour ouvrir la page Historique de tâches pour la tâche sélectionnée. Voir *Affichage de l'historique d'une tâche*, page 150.
Prochaine planification	Date et heure de la prochaine exécution
Propriétaire	Nom d'utilisateur de l'administrateur qui a planifié cette tâche

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

Option	Description
Lien nom de la tâche	Ouvre la page Planificateur, qui vous permet de modifier la définition de la tâche. Voir *Planification des rapports de présentation*, page 143.
Ajouter une tâche	Ouvre la page Planificateur, qui vous permet de définir une nouvelle tâche. Voir *Planification des rapports de présentation*, page 143.
Supprimer	Supprime de la file d'attente toutes les tâches cochées dans la liste. Après avoir été supprimée, une tâche ne peut pas être restaurée. Pour interrompre temporairement l'exécution d'une tâche spécifique, utilisez le bouton **Désactiver**.
Exécuter maintenant	Lance immédiatement l'exécution des tâches cochées dans la liste. Il s'agit là d'un ajout aux exécutions planifiées régulièrement.
Activer	Réactive immédiatement les tâches désactivées qui ont été cochées dans la liste. La tâche commence son exécution selon le planning établi.
Désactiver	Désactive l'exécution des tâches activées et cochées dans la liste. Servez-vous de cette option pour interrompre temporairement une tâche que vous souhaiterez peut-être restaurer ultérieurement.

Affichage de l'historique d'une tâche

Rubriques connexes :

- *Planification des rapports de présentation*, page 143
- *Affichage de la liste des tâches planifiées*, page 149

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

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

Examen des rapports de présentation planifiés

Rubriques connexes :

- *Rapports de présentation*, page 131
- *Exécution d'un rapport de présentation*, page 142
- *Planification des rapports de présentation*, page 143

La page **Rapports de présentation > Review Reports (Examiner les rapports)** permet de localiser les rapports planifiés et de les supprimer. Par défaut, les rapports s'affichent dans la liste du plus ancien au plus récent.

Pour afficher l'un des rapports de la liste, cliquez sur son nom.

- Si le rapport est un unique fichier PDF ou XLS, il est possible que vous puissiez l'enregistrer ou l'ouvrir. Cela dépend des paramètres de sécurité de votre navigateur et des plug-ins installés dans votre ordinateur.
- Si le rapport est très volumineux, il peut être enregistré sous forme de plusieurs fichiers PDF ou XLS et stocké dans un fichier ZIP. Le fichier est alors compressé au format ZIP, que le rapport ait été créé dans un ordinateur Windows ou Linux. Enregistrez ce fichier ZIP, puis extrayez les fichiers PDF ou XLS pour afficher le contenu du rapport.
- Pour voir si votre rapport contient un ou plusieurs fichiers, survolez l'icône accolée à son nom avec votre souris.

Pour limiter la liste aux rapports devant bientôt être supprimés, cochez la case **Show only reports due to be purged (Afficher uniquement les rapports devant être purgés)**. La durée de stockage des rapports est configurée dans la page Paramètres > Génération de rapports > Préférences (voir *Configuration des préférences de génération de rapports*, page 397).

Pour lancer une recherche dans la liste des rapports, sélectionnez d'abord une entrée dans la liste déroulante **Filtrer par**, puis saisissez un nom ou une date en tout ou partie. Vous pouvez lancer une recherche par :

- Nom de rapport ou de tâche
- Nom de l'administrateur qui a planifié le rapport (demandeur)
- Date de création du rapport (Date de création)
- Date de suppression prévue du rapport (Date de purge)

Saisissez votre terme de recherche, puis cliquez sur **Aller**. La recherche respecte la casse.

Cliquez sur **Effacer** pour supprimer le terme de recherche en cours, puis lancez une autre recherche ou cliquez sur **Actualiser** pour afficher la liste complète des rapports.

Lorsqu'un rapport récemment terminé ne s'affiche pas dans la page Review Reports (Examiner les rapports), vous pouvez également cliquer sur **Actualiser** pour que la page présente les données les plus récentes.

Pour supprimer un rapport, cliquez sur le X situé à droite de la taille de son fichier.

Pour afficher l'état d'une tâche de rapport planifiée, cliquez sur **File d'attente des tâches** en haut de la page. Pour plus d'informations sur le fonctionnement de la file d'attente des tâches, consultez la section *Affichage de la liste des tâches planifiées*, page 149.

Pour planifier une nouvelle tâche de rapport, cliquez sur **Scheduler (Planificateur)** (voir *Planification des rapports de présentation*, page 143).

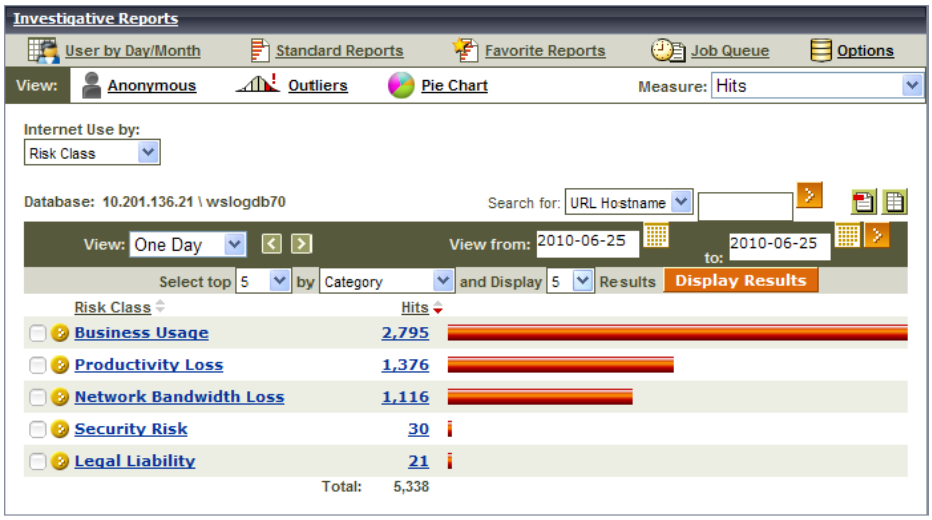
Rapports d'investigation

Rubriques connexes :

- *Rapports récapitulatifs*, page 154
- *Rapports récapitulatifs multi-niveaux*, page 158
- *Rapports détaillés flexibles*, page 159
- *Rapports Détails de l'activité utilisateur*, page 163
- *Rapports standard*, page 168
- *Rapports d'investigation favoris*, page 169
- *Planification des rapports d'investigation*, page 172
- *Rapports Cas particuliers*, page 175
- *Sortie dans un fichier*, page 176
- *Connexion à la base de données et paramètres par défaut des rapports*, page 421

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

Au départ, la page Rapports d'investigation principale affiche un résumé de l'activité par classe de risques (voir *Classes de risque*, page 54).



Dans le rapport récapitulatif, cliquez sur les liens et les éléments disponibles qui vous intéressent et examinez l'aperçu global de l'utilisation d'Internet dans votre organisation (voir *Rapports récapitulatifs*, page 154).

Les rapports récapitulatifs multi-niveaux (voir *Rapports récapitulatifs multi-niveaux*, page 158) et les rapports détaillés flexibles (voir *Rapports détaillés flexibles*, page 159) vous permettent d'analyser les informations sous différentes perspectives.

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

Option	Action
Utilisateur par jour/mois	Affiche une boîte de dialogue qui vous permet de définir un rapport sur une activité spécifique de l'utilisateur, pour une journée ou un mois. Pour plus d'informations, consultez la section *Rapports Détails de l'activité utilisateur*, page 163.
Rapports standard	Affiche la liste des rapports prédéfinis qui vous permettent de consulter rapidement une combinaison spécifique de données. Voir *Rapports standard*, page 168.
Rapports favoris	Permet d'enregistrer le rapport en cours en tant que Favori et d'afficher la liste des Favoris que vous pouvez générer ou planifier. Voir *Rapports d'investigation favoris*, page 169.
File d'attente des tâches	Affiche la liste des tâches des rapports d'investigation planifiés. Voir *Planification des rapports d'investigation*, page 172.
Cas particuliers	Affiche les rapports d'utilisation Internet qui s'éloignent significativement de la moyenne. Voir *Rapports Cas particuliers*, page 175.
Options	Affiche la page qui permet de sélectionner une autre Base de données d'activité pour la génération de rapports. La page Options vous permet également de personnaliser certaines fonctions de génération de rapports, par exemple la période initialement affichée dans les rapports récapitulatifs et les colonnes par défaut des rapports détaillés. Voir *Connexion à la base de données et paramètres par défaut des rapports*, page 421.
	Cliquez sur ce bouton, à droite des champs Rechercher, pour exporter le rapport actif dans une feuille de calcul compatible Microsoft Excel. Le système vous invite à ouvrir ou à enregistrer le fichier. Pour pouvoir ouvrir ce fichier, Microsoft Excel 2003 ou une version ultérieure doit être installé. Voir *Sortie dans un fichier*, page 176.
	Cliquez sur ce bouton, à droite des champs Rechercher, pour exporter le rapport actif dans un fichier PDF compatible avec Adobe Reader. Le système vous invite à ouvrir ou à enregistrer le fichier. Pour pouvoir ouvrir ce fichier, Adobe Reader version 7.0 ou ultérieure doit être installé. Voir *Sortie dans un fichier*, page 176.

N'oubliez pas que la génération de rapports est limitée aux informations enregistrées dans la Base de données d'activité (Log Database).

- Si vous désactivez la journalisation des noms des utilisateurs, des adresses IP ou des catégories sélectionnées (voir *Configuration du mode de journalisation des requêtes filtrées*, page 398), ces informations ne pourront pas être incluses dans les rapports.
- De même, si vous désactivez la journalisation de certains protocoles (voir *Modification d'un filtre de protocoles*, page 64), les requêtes ne seront pas disponibles pour ces protocoles.

- Si vous voulez que le rapport présente à la fois le nom de domaine (www.domaine.com) et le chemin d'une page particulière dans le domaine (/produits/produitA), vous devez journaliser les adresses URL complètes (voir *Configuration de la journalisation des URL*, page 413).
- Si votre service d'annuaire n'inclut pas le nom et le prénom de l'utilisateur, les rapports ne peuvent pas afficher ces informations.

Les rapports d'investigation de Websense sont limités par le processeur et la mémoire disponible dans l'ordinateur sur lequel s'exécute TRITON - Web Security, de même que certaines ressources réseau. L'exécution de certains rapports de grande taille peut se révéler très longue. Une option du message de progression permet d'enregistrer le rapport en tant que Favori de manière à pouvoir planifier son exécution à un autre moment. Voir *Planification des rapports d'investigation*, page 172.

Rapports récapitulatifs

Rubriques connexes :

- *Rapports récapitulatifs multi-niveaux*, page 158
- *Rapports détaillés flexibles*, page 159
- *Rapports Détails de l'activité utilisateur*, page 163
- *Rapports standard*, page 168
- *Rapports d'investigation favoris*, page 169
- *Planification des rapports d'investigation*, page 172
- *Rapports Cas particuliers*, page 175
- *Sortie dans un fichier*, page 176

Au départ, la page Rapports d'investigation affiche le rapport récapitulatif de l'activité Internet de tous les utilisateurs par classe de risques, présentant l'activité de la Base de données d'activité pour la journée. La mesure du graphique à barres initial est Accès (nombre de fois où le site a été demandé). Pour configurer la période que doit couvrir ce rapport récapitulatif initial, consultez la section *Connexion à la base de données et paramètres par défaut des rapports*, page 421.

Servez-vous des liens et des options de cette page pour modifier rapidement le contenu du rapport ou pour explorer les détails du rapport.

1. Pour personnaliser la quantification des résultats, sélectionnez l'une des options suivantes dans la liste **Mesurer**.

Option	Description
Accès	Nombre de fois où l'URL a été demandée Selon la configuration de Log Server, il peut s'agir de véritables accès, qui conservent un enregistrement distinct pour chaque élément du site demandé, ou de visites, qui combinent les différents éléments du site dans un même enregistrement du journal.

Option	Description
Bande passante [ko]	Quantité de données, en kilo-octets, contenues dans la requête initiale de l'utilisateur et dans la réponse du site Web. Il s'agit du total combiné des valeurs Envoyés et Reçus. N'oubliez pas que certains produits d'intégration n'envoient pas ces informations à Websense. Les pare-feu Check Point FireWall-1 et Cisco PIX Firewall en sont deux exemples. Si votre intégration n'envoie pas ces informations et si Network Agent est installé, activez l'option **Journaliser les demandes HTTP** pour activer la génération des informations de bande passante dans les rapports. Voir *Configuration des paramètres des cartes réseau*, page 431.
Envoyés [ko]	Nombre de kilo-octets envoyés dans la requête Internet. Cela représente la quantité de données transmises, pouvant correspondre à une simple demande d'URL, ou à une soumission plus importante (par exemple si l'utilisateur s'enregistre auprès d'un site Web).
Reçus [ko]	Nombre de kilo-octets reçus en réponse à la requête, ensemble des textes, graphiques et scripts de la page compris. Dans le cas des sites bloqués, le nombre de kilo-octets dépend du logiciel qui crée l'enregistrement du journal. Lorsque Websense Network Agent journalise les enregistrements, le nombre d'octets reçus pour un site bloqué correspond à la taille de la page de blocage de Websense. Si l'enregistrement de journal est créé par Websense Security Gateway en résultat d'une analyse, les kilo-octets reçus représentent la taille de la page analysée. Pour plus d'informations sur l'analyse, consultez la section *Options d'analyse et contournement du décryptage SSL*, page 181. Lorsqu'un autre produit d'intégration crée les enregistrements du journal, les kilo-octets reçus pour un site bloqué peuvent correspondre à zéro (0), à la taille de la page bloquée ou à la valeur obtenue du site demandé.
Temps de navigation	Évaluation du temps passé à naviguer sur le site. Voir *Qu'est-ce que le temps de navigation sur Internet ?*, page 130.

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

   Les options dépendent du contenu de la Base de données d'activité et de certaines caractéristiques du réseau. Par exemple, si la Base de données d'activité ne comprend qu'un seul groupe ou domaine, Groupes et Domaines n'apparaissent pas dans la liste. De même, lorsqu'il y a trop d'utilisateurs (plus de 5 000) ou de groupes (plus de 3 000), ces options ne s'affichent pas. (Certaines de ces limites peuvent être configurées. Voir *Options d'affichage et de sortie*, page 423.)

3. Cliquez sur un nom dans la colonne de gauche (ou sur la flèche accolée au nom) pour afficher la liste des options, par exemple par utilisateur, par domaine ou par action.

   Les options de la liste sont les mêmes que celles qui apparaissent sous Utilisation d'Internet par, personnalisées par rapport au contenu affiché.

> **Remarque**
>
> Certaines options, telles qu'Utilisateur ou Groupe, s'affichent parfois en lettres rouges. Dans ce cas, la sélection de cette option peut entraîner la production d'un rapport très volumineux dont l'exécution sera très longue. Avant de sélectionner cette option, tentez de préciser davantage de détails.

4. Sélectionnez l'une de ces options pour générer un nouveau rapport récapitulatif présentant les informations sélectionnées pour l'entrée associée.

   Par exemple, dans un rapport récapitulatif Classe de risques, un clic sur Par utilisateur, sous la classe de risque Responsabilité légale, génère un rapport sur l'activité de chaque utilisateur dans cette classe de risques.
5. Cliquez sur une nouvelle entrée dans la colonne de gauche, puis sélectionnez une option pour afficher davantage de détails sur cet élément particulier.
6. Pour modifier l'ordre de tri du rapport, servez-vous des flèches placées à côté des en-têtes de colonne.
7. Contrôlez le rapport récapitulatif à l'aide des options suivantes, placées au-dessus du graphique. Ensuite, explorez les détails associés en cliquant sur les éléments du nouveau rapport.

Option	Action
Chemin du rapport (Utilisateur > Jour)	À côté de la liste **Utilisation d'Internet par**, un chemin présente les sélections à l'origine du rapport actuel. Cliquez sur l'un des liens du chemin pour revenir à cette vue des données.
Afficher	Sélectionnez une période pour le rapport : Un jour, Une semaine, Un mois ou Tous. Le rapport s'actualise pour afficher les données de la période sélectionnée. Servez-vous des flèches adjacentes pour parcourir les données disponibles, une période (jour, semaine, mois) à la fois. Lorsque vous modifiez cette sélection, les champs **Afficher de** sont mis à jour pour refléter la période consultée. Si vous choisissez une date spécifique dans les champs Afficher de ou via la boîte de dialogue Favoris, le champ **Afficher** indique Personnalisé, à la place d'une période.
Afficher du... au...	Les dates de ces champs s'actualisent automatiquement pour refléter la période consultée lorsque vous modifiez le champ **Afficher**. Vous pouvez également entrer les dates exactes de début et de fin des rapports, ou cliquer sur l'icône du calendrier pour sélectionner les dates désirées. Cliquez sur la flèche droite adjacente pour actualiser le rapport après avoir sélectionné des dates.
Graphique en secteurs / Graphique à barres	Lorsque le graphique à barres est actif, cliquez sur **Graphique en secteurs** pour afficher le rapport récapitulatif actuel sous forme de graphique en secteurs. Cliquez sur l'étiquette d'un secteur pour afficher les mêmes options que celles qui sont disponibles lorsque vous cliquez sur une entrée de la colonne gauche du graphique à barres. Lorsque le graphique en secteurs est actif, cliquez sur **Graphique à barres** pour afficher le rapport récapitulatif actuel sous forme de graphique à barres.

Option	Action
Plein écran	Sélectionnez cette option pour afficher le rapport d'investigation actif dans une fenêtre distincte, sans les panneaux de navigation gauche et droit.
Anonyme / Noms	• Cliquez sur **Anonyme** pour que les rapports présentent un numéro d'identification d'utilisateur attribué en interne chaque fois que le nom de l'utilisateur devrait s'afficher. • Si les noms sont masqués, cliquez sur **Noms** pour afficher de nouveau les noms d'utilisateur. Dans certains cas, les noms d'utilisateur ne peuvent pas s'afficher. Pour plus d'informations, consultez la section *Configuration du mode de journalisation des requêtes filtrées*, page 398. Pour plus d'informations sur le masquage des informations qui permettent d'identifier les utilisateurs, consultez la section *Anonymat des rapports d'investigation*, page 157.
Rechercher	Sélectionnez un élément de rapport dans la liste, puis entrez une partie ou la totalité de la valeur de la recherche dans la zone de texte adjacente. Cliquez sur la flèche adjacente pour lancer la recherche et afficher les résultats. La saisie d'une adresse IP partielle, telle que 10.5, lance une recherche sur tous les sous-réseaux, de 10.5.0.0 à 10.5.255.255 dans cet exemple.

8. Ajoutez un sous-ensemble d'informations pour toutes les entrées ou pour les entrées sélectionnées dans la colonne de gauche en créant un rapport récapitulatif multi-niveaux. Voir *Rapports récapitulatifs multi-niveaux*, page 158.
9. Créez un rapport tabulaire pour un élément spécifique de la colonne de gauche en cliquant sur le nombre adjacent ou dans la barre de mesure. Ce rapport détaillé peut être modifié en fonction de vos besoins spécifiques. Voir *Rapports détaillés flexibles*, page 159.

Anonymat des rapports d'investigation

Plusieurs options vous permettent de ne pas afficher les informations d'identification dans les rapports d'investigation.

- La méthode la plus sûre consiste à interdire la journalisation des noms d'utilisateur et des adresses IP sources. Dans ce cas, aucune information d'identification des utilisateurs n'est enregistrée dans la Base de données d'activité, et les rapports d'investigation et de présentation ne peuvent pas inclure ces informations. Pour obtenir des instructions, consultez la section *Configuration du mode de journalisation des requêtes filtrées*, page 398.
- Lorsque certains administrateurs doivent pouvoir accéder à des rapports contenant des informations sur les utilisateurs, alors que d'autres ne doivent jamais pouvoir voir ces informations, servez-vous des rôles d'administration déléguée pour contrôler l'accès aux rapports. Vous pouvez configurer des rôles autorisés à accéder aux rapports d'investigation, mais masquer les noms d'utilisateur dans ces rapports. Pour plus d'informations, consultez la section *Administration déléguée et génération de rapports*, page 323.
- Si vous devez parfois générer des rapports contenant des informations sur les utilisateurs et parfois des rapports anonymes, servez-vous de l'option **Anonyme** située en haut de la page Rapports d'investigation pour masquer temporairement les noms d'utilisateur et, éventuellement, les adresses IP sources. Pour plus d'informations, consultez la section *Option Anonyme*, page 158.

Option Anonyme

Par défaut, cliquer sur **Anonyme** masque les noms d'utilisateur uniquement, les adresses IP sources s'affichant toujours dans les rapports. Vous pouvez configurer Websense de sorte qu'il masque les noms d'utilisateur et les adresses IP sources lorsque l'option Anonyme est sélectionnée :

1. Dans l'ordinateur TRITON - Web Security, ouvrez le fichier **wse.ini** dans un éditeur de texte. (Par défaut, ce fichier est situé dans le répertoire C:\Program Files\Websense\webroot\Explorer.)
2. Ajoutez la ligne suivante sous la section **[explorer]** :

   ```
   encryptIP=1
   ```

3. Enregistrez et fermez le fichier.

À présent, dès que vous cliquerez sur Anonyme, toutes les informations d'identification des utilisateurs seront masquées.

Si vous cliquez sur **Anonyme** et que vous passez ensuite à une autre vue des données, par exemple à une vue détaillée ou à des cas particuliers, les noms d'utilisateur demeurent masqués dans le nouveau rapport. Pour revenir à la vue résumée avec les noms masqués, utilisez les liens placés en haut du rapport et non ceux de la bannière (fil d'Ariane).

Rapports récapitulatifs multi-niveaux

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports récapitulatifs*, page 154
- *Rapports détaillés flexibles*, page 159
- *Rapports Détails de l'activité utilisateur*, page 163
- *Rapports standard*, page 168
- *Rapports d'investigation favoris*, page 169
- *Planification des rapports d'investigation*, page 172
- *Rapports Cas particuliers*, page 175
- *Sortie dans un fichier*, page 176

Les rapports récapitulatifs multi-niveaux présentent un second niveau d'informations qui complète les informations principales affichées. Par exemple, si l'affichage principal présente les classes de risques, vous pouvez définir un second niveau pour identifier les catégories les plus demandées dans chaque classe de risques. Dans un autre exemple, si le rapport principal présente les requêtes pour chaque catégorie, vous pouvez afficher les cinq premières catégories et les dix utilisateurs à l'origine de la plupart des requêtes dans chaque catégorie.

Pour créer un rapport récapitulatif multi-niveaux, servez-vous des paramètres situés immédiatement au-dessus du rapport récapitulatif.

1. Dans la liste **Relever les**, choisissez un chiffre indiquant le nombre d'entrées principales (colonne de gauche) à utiliser dans le rapport. Le rapport résultant inclut les entrées principales avec les plus grandes valeurs. (Les dates les plus récentes s'affichent si l'entrée principale est Jour.)

   Vous pouvez également cocher la case accolée aux entrées individuelles désirées dans la colonne de gauche pour ne créer des rapports que pour ces entrées. Le champ **Relever les** affiche **Personnalisé**.
2. Dans la liste **par**, choisissez les informations secondaires à utiliser dans le rapport.
3. Dans le champ **Afficher**, choisissez le nombre de résultats secondaires à utiliser dans le rapport pour chaque entrée principale.
4. Cliquez sur **Afficher les résultats** pour générer le rapport récapitulatif multi-niveaux.

   Le rapport récapitulatif est mis à jour de manière à n'afficher que le nombre sélectionné d'entrées principales. La liste des entrées secondaires apparaît sous la barre de chaque entrée principale.
5. Pour modifier l'ordre de tri du rapport, servez-vous des flèches placées à côté des en-têtes de colonne.

Pour revenir à un rapport récapitulatif sur un seul niveau, sélectionnez une autre option dans **Utilisation d'Internet par**. Vous pouvez également cliquer sur l'une des entrées principales ou secondaires et sélectionner une option pour générer un nouveau rapport d'investigation avec ces informations.

Rapports détaillés flexibles

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports récapitulatifs*, page 154
- *Rapports récapitulatifs multi-niveaux*, page 158
- *Rapports d'investigation favoris*, page 169
- *Planification des rapports d'investigation*, page 172
- *Rapports Cas particuliers*, page 175
- *Sortie dans un fichier*, page 176
- *Connexion à la base de données et paramètres par défaut des rapports*, page 421
- *Colonnes des rapports détaillés flexibles*, page 161

Les rapports détaillés donnent une vue tabulaire des informations de la Base de données d'activité. Accédez à un rapport en vue détaillée à partir de la page principale après avoir consulté un rapport récapitulatif pour lequel vous souhaitez davantage de détails.

Vous pouvez demander une vue détaillée à partir de n'importe quelle ligne. Toutefois, lorsque vous demandez un rapport détaillé basé sur les accès, il est préférable de commencer par une ligne présentant moins de 100 000 accès. Lorsqu'une ligne contient plus de 100 000 accès, la valeur des accès s'affiche en rouge pour vous avertir que l'exécution du rapport détaillé peut être très lente.

Le rapport en vue détaillée est considéré comme *flexible*, car il vous permet de concevoir votre propre rapport. Vous pouvez en effet ajouter ou supprimer des colonnes d'informations et modifier l'ordre des colonnes affichées. Les informations sont triées en fonction de l'ordre des colonnes. Vous pouvez même inverser l'ordre de tri de n'importe quelle colonne, croissant à décroissant ou vice versa.

Les rapports d'investigation de Websense sont limités par le processeur et la mémoire disponible dans l'ordinateur sur lequel s'exécute TRITON - Web Security, de même que certaines ressources réseau. Les demandes de rapports très volumineux peuvent provoquer une expiration du délai de connexion. Lorsque vous demandez un rapport volumineux, vous avez la possibilité de générer le rapport sans délai.

Important

Dans les listes déroulantes ou de valeurs, certaines options peuvent s'afficher en rouge. Cette couleur rouge signale que cette option peut entraîner un rapport très volumineux. Il est généralement plus efficace de tenter de préciser davantage de détails avant de sélectionner cette option.

1. Générez le rapport récapitulatif ou multi-niveaux sur la page principale des rapports d'investigation. (Voir *Rapports récapitulatifs*, page 154, ou *Rapports récapitulatifs multi-niveaux*, page 158.)
2. Explorez les résultats afin de vous concentrer sur les informations qui vous intéressent directement.

   Lorsque vous générez un rapport sur les accès, il est préférable de naviguer jusqu'à une entrée présentant moins de 100 000 accès avant d'ouvrir ce rapport en vue détaillée.
3. Cliquez sur le nombre ou la barre de la ligne que vous souhaitez explorer plus en détails. Pour inclure plusieurs lignes dans votre rapport, cochez la case accolée à chaque ligne avant de cliquer sur le nombre ou sur la barre d'une ligne.

   Un message contextuel montre la progression du chargement du rapport détaillé.

Remarque

Si la création du rapport prend du temps, vous pouvez l'enregistrer sous forme de Favori en cliquant sur le lien du message de chargement et planifier une exécution ultérieure. Voir *Rapports d'investigation favoris*, page 169.

4. Vérifiez les informations du rapport initial.

   Les colonnes par défaut varient, selon si vous créez un rapport sur les accès, la bande passante ou le temps de navigation, et selon vos sélections dans la page Options. (Voir *Connexion à la base de données et paramètres par défaut des rapports*, page 421.)
5. Cliquez sur **Modifier le rapport** en haut de la page.

   La liste **Rapport en cours** de la boîte de dialogue Modifier le rapport présente les colonnes affichées dans le rapport détaillé en cours.
6. Sélectionnez un nom de colonne dans la liste **Colonnes disponibles** ou **Rapport en cours**, puis cliquez sur la flèche droite (>) ou gauche (<) pour déplacer cette colonne vers l'autre liste.

   Choisissez un maximum de 7 colonnes pour le rapport. La colonne présentant la mesure (accès, bande passante, temps de navigation), issue du rapport récapitulatif initial, s'affiche toujours le plus à droite. Sa position n'est pas modifiable.

Consultez la section *Colonnes des rapports détaillés flexibles*, page 161, pour obtenir la liste des colonnes disponibles et leur description.

7. Sélectionnez un nom de colonne dans la liste **Rapport en cours** et utilisez les flèches vers le haut et vers le bas pour modifier l'ordre des colonnes.

   La première colonne de la liste Rapport en cours devient la colonne gauche du rapport.

8. Cliquez sur le lien **Récapitulatif** ou **Détail**, situé au-dessus du rapport, pour passer d'un affichage à l'autre.

Option	Description
Récapitulatif	Pour afficher un rapport récapitulatif, vous devez supprimer la colonne Temps. Les rapports récapitulatifs regroupent en une seule entrée tous les enregistrements qui partagent un élément commun. L'élément spécifique varie en fonction des informations utilisées dans le rapport. En général, la colonne située immédiatement à droite avant la mesure présente l'élément récapitulatif.
Détails	L'option Détail présente chaque enregistrement sur une ligne distincte. La colonne Temps peut être affichée.

9. Cliquez sur **Appliquer** pour générer le rapport défini.
10. Servez-vous des options suivantes pour modifier le rapport affiché.
    - Utilisez les options **Afficher** situées au-dessus du rapport pour modifier la période utilisée dans le rapport.
    - Cliquez sur les flèches dirigées vers le haut ou vers le bas d'un en-tête de colonne pour inverser l'ordre de tri de cette colonne et ses données associées.
    - Servez-vous des liens **Suivant** et **Précédent**, situés au-dessus et au-dessous du rapport, pour éventuellement afficher les autres pages du rapport. Par défaut, chaque page contient 100 lignes, que vous pouvez ajuster en fonction de vos besoins. Voir *Options d'affichage et de sortie*, page 423.
    - Cliquez sur l'URL pour ouvrir le site Web demandé dans une nouvelle fenêtre.
11. Cliquez sur **Rapports favoris** si vous souhaitez enregistrer le rapport de manière à pouvoir le générer de nouveau rapidement ou de façon périodique (voir *Enregistrement d'un rapport en tant que Favori*, page 170).

Colonnes des rapports détaillés flexibles

Rubriques connexes :

- *Rapports détaillés flexibles*, page 159
- *Rapports d'investigation favoris*, page 169
- *Planification des rapports d'investigation*, page 172

Le tableau ci-dessous présente les colonnes disponibles dans les rapports détaillés (voir *Rapports détaillés flexibles*, page 159).

Certaines colonnes ne sont pas toujours disponibles. Par exemple, si la colonne Utilisateur est affichée, la colonne Groupe n'est pas disponible. Si la colonne Catégorie est affichée, Classe de risques n'est pas disponible.

Nom de la colonne	Description
Utilisateur	Nom de l'utilisateur à l'origine de la requête. Les informations relatives à l'utilisateur doivent être disponibles dans la Base de données d'activité pour être incluses dans les rapports. Les informations relatives aux groupes ne sont pas disponibles dans les rapports basés sur les utilisateurs.
Jour	Date de la requête Internet
Nom hôte URL	Nom de domaine (également appelé nom d'hôte) du site demandé
Domaine	Domaine du service d'annuaire du client (utilisateur ou groupe, domaine ou unité d'organisation) à l'origine de la requête
Groupe	Nom du groupe auquel le demandeur appartient. Les noms des utilisateurs individuels ne sont pas fournis dans les rapports basés sur les groupes. Si l'utilisateur qui a demandé le site appartient à plusieurs groupes dans le service d'annuaire, le rapport affiche plusieurs groupes dans cette colonne.
Classe de risques	Classe de risques associée à la catégorie à laquelle le site demandé appartient. Si la catégorie appartient à plusieurs classes de risques, toutes les classes de risques concernées apparaissent dans la liste. Voir *Attribution de catégories aux classes de risque*, page 396.
Objet d'annuaire	Chemin d'accès à l'annuaire de l'utilisateur à l'origine de la requête, sans le nom d'utilisateur. Cela donne généralement plusieurs lignes pour le même trafic, car chaque utilisateur appartient à plusieurs chemins d'accès. Si vous utilisez un service d'annuaire non LDAP, cette colonne n'est pas disponible.
Disposition	Action exécutée par Websense en résultat de la requête (par exemple, catégorie autorisée ou catégorie bloquée)
Serveur source	Adresse IP de l'ordinateur qui envoie les requêtes à Filtering Service. Dans les déploiements autonomes, il s'agit de l'adresse IP de Network Agent. Dans les déploiements intégrés, il s'agit de l'adresse IP de la passerelle, du pare-feu ou du cache. Avec Websense Web Security Gateway Anywhere, cette option vous permet d'identifier les requêtes des utilisateurs sur site (emplacement filtré) et hors site, filtrées par le service hybride.
Protocole	Protocole de la demande (par exemple, HTTP ou FTP)
Groupe de protocoles	Groupe de la Base de données principale dans lequel se situe le protocole demandé (par exemple, Accès à distance ou Médias en temps-réel)
IP source	Adresse IP de l'ordinateur à partir duquel la demande a été effectuée Avec Websense Web Security Gateway Anywhere, cette option vous permet d'examiner les requêtes provenant d'un emplacement hybride et filtré spécifique. Voir *Définition des emplacements filtrés*, page 205.
IP de destination	Adresse IP du site demandé
URL complète	Nom de domaine et chemin complet du site demandé (exemple : http://www.mondomaine.com/produits/elementun/). Si vous ne journalisez pas les URL complètes, cette colonne sera vide. Voir *Configuration de la journalisation des URL*, page 413.

Nom de la colonne	Description
Mois	Mois du calendrier au cours duquel la demande a été effectuée
Port	Port TCP/IP par lequel l'utilisateur a communiqué avec le site
Largeur de bande	Quantité de données, en kilo-octets, contenues dans la requête initiale de l'utilisateur et dans la réponse du site Web. Il s'agit du total combiné des valeurs Envoyés et Reçus. N'oubliez pas que certains produits d'intégration n'envoient pas ces informations à Websense. Les pare-feu Check Point FireWall-1 et Cisco PIX Firewall en sont deux exemples. Si votre intégration n'envoie pas ces informations et que Websense Network Agent est installé, activez l'option **Journaliser les demandes HTTP** de la carte d'interface réseau appropriée pour activer la génération de rapports sur les informations de bande passante. Voir *Configuration des paramètres des cartes réseau*, page 431.
Octets envoyés	Nombre d'octets envoyés dans la requête Internet. Cela représente la quantité de données transmises, pouvant correspondre à une simple demande d'URL, ou d'une soumission plus importante, par exemple si l'utilisateur s'enregistre auprès d'un site Web.
Octets reçus	Nombre d'octets reçus d'Internet en réponse à la requête. Cela comprend l'ensemble du texte, des graphiques et des scripts qui composent le site. Dans le cas des sites bloqués, le nombre d'octets dépend du logiciel qui crée l'enregistrement du journal. Lorsque Websense Network Agent journalise les enregistrements, le nombre d'octets reçus pour un site bloqué correspond à la taille de la page de blocage. Si l'enregistrement de journal est créé par Websense Security Gateway en résultat d'une analyse, les octets reçus représentent la taille de la page analysée. Pour plus d'informations sur l'analyse, consultez la section *Options d'analyse et contournement du décryptage SSL*, page 181. Lorsqu'un autre produit d'intégration crée les enregistrements du journal, les octets reçus pour un site bloqué peuvent correspondre à zéro (0), à la taille de la page bloquée ou à la valeur obtenue du site demandé.
Heure	Heure à laquelle le site a été demandé, au format HH:MM:SS, sur 24 heures
Catégorie	Catégorie à laquelle la requête a été affectée. Il peut s'agir d'une catégorie de la Base de données principale ou d'une catégorie personnalisée.

Rapports Détails de l'activité utilisateur

Rubriques connexes :

- *Rapports d'investigation*, page 152

Cliquez sur le lien **Utilisateur par jour/mois** pour générer un rapport Détails de l'activité d'un utilisateur. Ce rapport illustre de manière graphique l'activité Internet de l'utilisateur pour une seule journée ou un mois complet.

Commencez par générer un rapport pour l'utilisateur spécifique pour un jour sélectionné. À partir de ce rapport, vous pouvez générer un rapport sur l'activité du même utilisateur pour un mois complet. Pour plus d'informations, consultez les sections suivantes :

- *Détail de l'activité utilisateur par jour*, page 164
- *Activité utilisateur par mois*, page 165

Détail de l'activité utilisateur par jour

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports Détails de l'activité utilisateur*, page 163
- *Activité utilisateur par mois*, page 165

Le rapport Détail de l'activité utilisateur par jour présente une vue exhaustive de l'activité d'un utilisateur spécifique dans une journée.

1. Sélectionnez **Utilisateur par jour/mois** en haut de la page principale. La boîte de dialogue Activité utilisateur par jour apparaît.
2. Entrez une partie ou la totalité du nom d'un utilisateur dans le champ **Rechercher un utilisateur**, puis cliquez sur **Rechercher**.

   La recherche présente une liste contenant jusqu'à 100 noms d'utilisateur correspondants issus de la Base de données d'activité.
3. Faites votre sélection dans la liste **Sélectionner un utilisateur**.
4. Dans le champ **Sélectionner le jour**, acceptez la dernière date d'activité affichée par défaut ou choisissez une autre date.

   Vous pouvez saisir la nouvelle date ou cliquer sur l'icône du calendrier pour en sélectionner une. La zone de sélection du calendrier indique la plage de dates couverte par la Base de données d'activité active.
5. Cliquez sur **Afficher l'activité quotidienne de l'utilisateur** pour obtenir un rapport détaillé de l'activité de cet utilisateur pour la date demandée.

   Le rapport initial présente la chronologie de l'activité de l'utilisateur par incréments de 5 minutes. Chaque requête est affichée sous forme d'icône, correspondant à une catégorie de la base de données principale Websense. Toutes les catégories personnalisées sont représentées par une seule icône. (La couleur des icônes correspond au regroupement des risques présentés dans les rapports Activité utilisateur par mois. Voir *Activité utilisateur par mois*, page 165.)

   Survolez une icône avec votre souris pour afficher l'heure exacte, la catégorie et l'action de la requête associée.

Servez-vous des contrôles énumérés ci-dessous pour modifier l'affichage du rapport ou afficher sa légende.

Option	Description
Jour précédent / Jour suivant	Affiche l'activité Internet de cet utilisateur pour le jour suivant ou précédent
Vue tableau	Affiche la liste de chaque URL demandée, en précisant la date et l'heure de la requête, la catégorie et l'action effectuée (bloquée, autorisée ou autre)
Vue détaillée	Affiche la vue graphique initiale du rapport
Regrouper les accès similaires / Afficher tous les accès	Combine sur une seule ligne toutes les requêtes survenues à moins de 10 secondes les unes des autres et présentant les mêmes domaine, catégorie et action. La vue résumée des informations est ainsi plus courte. Le seuil de temps standard est de 10 secondes. Pour modifier cette valeur, consultez la section *Options d'affichage et de sortie*, page 423. Lorsque vous cliquez sur le lien, ce dernier devient Afficher tous les accès, qui permet de restaurer la liste d'origine de chaque requête.
Afficher les catégories	Affiche la liste de toutes les catégories présentes dans le rapport en cours, en indiquant à la fois le nom de la catégorie et l'icône qui la représente. Pour contrôler les catégories affichées dans le rapport, cochez les cases des catégories à inclure. Cliquez ensuite sur **Ok** pour actualiser le rapport avec vos sélections.

6. Cliquez sur **Activité utilisateur par mois**, au-dessus du rapport, pour afficher l'activité du même utilisateur pour le mois complet. Pour plus d'informations, consultez *Activité utilisateur par mois*, page 165.

Activité utilisateur par mois

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports Détails de l'activité utilisateur*, page 163
- *Détail de l'activité utilisateur par jour*, page 164
- *Correspondance des catégories*, page 166

Lorsque le rapport Détail de l'activité utilisateur par jour est ouvert, vous pouvez choisir de consulter l'activité mensuelle de cet utilisateur.

1. Ouvrez un rapport Détail de l'activité utilisateur par jour. Voir *Détail de l'activité utilisateur par jour*, page 164.
2. Cliquez sur **Activité utilisateur par mois** en haut.

   Le nouveau rapport affiche une image de calendrier, chaque jour étant représenté par un petit bloc coloré correspondant à l'activité Internet de l'utilisateur pour cette journée. Les requêtes de sites appartenant aux catégories personnalisées sont indiquées par des blocs gris.

3. Cliquez sur **Légende des catégories de la base de données** en haut et à gauche pour découvrir les correspondances entre les couleurs et les risques potentiels faibles ou élevés pour le site demandé.

   Les affectations de catégories sont fixes et ne peuvent pas être modifiées. Voir *Correspondance des catégories*, page 166.

4. Cliquez sur **Précédent** ou **Suivant** pour afficher l'activité Internet de cet utilisateur pour le mois suivant ou précédent.

Correspondance des catégories

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports Détails de l'activité utilisateur*, page 163
- *Activité utilisateur par mois*, page 165

La liste suivante identifie les catégories représentées par chacune des couleurs dans les rapports Activité utilisateur par jour et Activité utilisateur par mois.

N'oubliez pas que les noms des catégories peuvent changer dans la base de données principale. De plus, des catégories peuvent être ajoutées et supprimées à tout moment.

Couleur	Catégories
Gris	Catégories personnalisées Trafic non HTTP
Bleu foncé	**Commerce et économie** et toutes ses sous-catégories **Enseignement** et toutes ses sous-catégories **Santé** **Technologies de l'information**, y compris les sous-catégories Moteurs de recherche et portails, et Hébergement de sites Web **Divers** sous-catégories Réseaux de diffusion de contenu, Contenu dynamique, Images (Médias), Serveurs d'images et Adresses IP privées **Productivité**/Publicités
Bleu clair	**Drogues**/Médicaments sur ordonnance **Gouvernement** et sa sous-catégorie Armée **Technologies de l'information**/Sites de traduction automatique de pages Web **Divers**, catégorie parente uniquement **Actualités et médias**, catégorie parente uniquement **Événements spéciaux**

Couleur	Catégories
Vert jaune	**Avortement** et toutes ses sous-catégories **Section pour adultes**/Éducation sexuelle **Bande passante**, y compris les sous-catégories Radio et TV Internet, Sauvegarde et stockage réseau personnels, et Médias en temps réel **Divertissement** et sa sous-catégorie MP3 **Jeux** **Gouvernement**/Organisations politiques **Technologies de l'information**/Sécurité informatique **Communication Internet**/Consultation en ligne de courrier électronique **Divers**/Serveurs de téléchargement de fichiers **Divers**/Erreurs réseau **Actualités et médias**/Journaux alternatifs **Productivité**, y compris les sous-catégories Messagerie instantanée, Tableaux d'affichage et forums électroniques, Courtage et commerce en ligne **Religion** et les sous-catégories Religions non traditionnelles, occultes et folklore et Religions traditionnelles **Sécurité**, catégorie parente uniquement **Shopping** et toutes ses sous-catégories **Organisations sociales** et toutes ses sous-catégories **Société et styles de vie**, y compris les sous-catégories Homosexuels, lesbiennes et bisexuels, Hobbies, Sites Web personnels et Restaurants **Sports** et toutes ses sous-catégories **Voyage** **Définie par l'utilisateur** **Véhicules**

Couleur	Catégories
Orange	**Section pour adultes**/Nudité **Groupes activistes/Associations** **Bande passante**/Téléphonie Internet **Drogues** et les sous-catégories Abus de drogues, Marijuana et Compléments/Substances non réglementées **Technologies de l'information**/Antiblocage par proxy **Communication Internet** et la sous-catégorie Conversations en ligne **Recherche d'emploi** **Divers**/Non catégorisés **Productivité** sous-catégories Téléchargement de logiciels et de freewares et Sites rémunérateurs **Religion** **Société et style de vie** sous-catégories Alcool et tabac, et Petites annonces personnelles/Rendez-vous amoureux **Mauvais goût** **Armes**
Rouge	**Section pour adultes** et ses sous-catégories : Contenu pour adultes, Lingerie et maillots de bain, et Sexe **Largeur de bande**/Partage de fichiers en P2P **Jeux de hasard** **Illégal ou douteux** **Technologies de l'information**/Piratage **Militantisme, extrémisme** **Racisme, haine** **Sécurité** sous-catégories Enregistreurs de frappe, Sites Web dangereux, Phishing et Logiciels espion **Violence**

Rapports standard

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports d'investigation favoris*, page 169
- *Planification des rapports d'investigation*, page 172

Les rapports standard vous permettent d'afficher rapidement un ensemble particulier d'informations sans qu'il soit nécessaire d'investiguer plus avant.

1. Cliquez sur le lien **Rapports standard** dans la page Rapports d'investigation principale.

2. Choisissez le rapport contenant les informations désirées. Les rapports suivants sont disponibles.

Niveaux d'activité les plus élevés
• Quels utilisateurs ont le plus d'accès ? • 10 principaux utilisateurs pour les 10 URL les plus visitées • 5 principaux utilisateurs dans les catégories Shopping, Divertissement et Sports • 5 principales URL pour les 5 catégories les plus visitées
Consommation la plus élevée de bande passante
• Groupes consommant le plus de bande passante • Groupes consommant le plus de bande passante pour la sous-catégorie Médias en temps réel • Rapport détaillé des URL sur les utilisateurs par perte de bande passante réseau • 10 principaux groupes pour les catégories de bande passante
Temps le plus long en ligne
• Utilisateurs ayant passé le plus de temps en ligne • Utilisateurs ayant passé le plus de temps sur les sites pour les catégories Productivité
Les plus bloqués
• Utilisateurs les plus bloqués • Sites les plus bloqués • Rapport détaillé des URL des utilisateurs bloqués • 10 principales catégories bloquées
Risque de sécurité le plus élevé
• Catégories principales supposant un risque de sécurité • Principaux utilisateurs du protocole P2P • Principaux utilisateurs des sites pour les catégories Sécurité • URL pour les 10 principaux ordinateurs avec logiciels espion
Responsabilité légale
• Risque de responsabilité légale par catégorie • Principaux utilisateurs pour les catégories Section pour adultes

3. Consultez le rapport qui s'affiche.
4. Enregistrez-le sous forme de Rapport favori pour le réexécuter régulièrement. Voir *Rapports d'investigation favoris*, page 169.

Rapports d'investigation favoris

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Planification des rapports d'investigation*, page 172

Vous pouvez enregistrer la plupart des rapports d'investigation en tant que **Favoris**. Cela comprend les rapports que vous générez en naviguant jusqu'à des informations spécifiques, les rapports standard et les rapports détaillés que vous avez modifiés en fonction de vos besoins. Exécutez ensuite le rapport favori à tout moment, ou planifiez son exécution à des jours et des heures spécifiques.

Dans les organisations qui utilisent l'administration déléguée, l'autorisation d'enregistrer et de planifier des Favoris est définie par le Super administrateur. Les administrateurs qui disposent de cette autorisation peuvent uniquement exécuter et planifier les favoris qu'ils ont enregistrés ; ils n'ont pas accès aux favoris enregistrés par les autres administrateurs.

Pour plus d'informations sur le fonctionnement des rapports favoris, consultez les sections suivantes :

- *Enregistrement d'un rapport en tant que Favori*, page 170
- *Création ou suppression d'un rapport Favori*, page 170
- *Modification d'un rapport favori*, page 171

Enregistrement d'un rapport en tant que Favori

Rubriques connexes :

- *Rapports d'investigation favoris*, page 169
- *Modification d'un rapport favori*, page 171

Utilisez la procédure suivante pour enregistrer un rapport en tant que Favori.

1. Créez un rapport d'investigation avec le format et les informations désirés.
2. Cliquez sur **Rapports favoris**.
3. Acceptez ou modifiez le nom proposé par TRITON - Web Security.

   Ce nom peut contenir des lettres, des chiffres et des caractères de soulignement (_). Les espaces et les autres caractères spéciaux ne peuvent pas être utilisés.
4. Cliquez sur **Ajouter**.

   Le nom du rapport est ajouté dans la liste des favoris.
5. Sélectionnez un rapport dans cette liste, puis une option de gestion du rapport. Selon l'option choisie, consultez :
   - *Création ou suppression d'un rapport Favori*, page 170
   - *Planification des rapports d'investigation*, page 172

Création ou suppression d'un rapport Favori

Rubriques connexes :

- *Rapports d'investigation favoris*, page 169
- *Modification d'un rapport favori*, page 171

Vous pouvez à tout moment générer un rapport favori ou supprimer ceux qui sont devenus inutiles.

1. Cliquez sur **Rapports favoris** pour afficher la liste des rapports enregistrés comme favoris.

   > **Remarque**
   > Si votre organisation utilise l'administration déléguée, cette liste ne comprend pas les rapports favoris enregistrés par les autres administrateurs.

2. Sélectionnez un rapport dans la liste.
3. Procédez de l'une des manières suivantes :
   - Cliquez sur **Exécuter maintenant** pour générer et afficher le rapport sélectionné immédiatement.
   - Cliquez sur **Planification** pour planifier une exécution ultérieure ou périodique du rapport. Pour plus d'informations, consultez *Planification des rapports d'investigation*, page 172.
   - Cliquez sur **Supprimer** pour retirer ce rapport de la liste des favoris.

Modification d'un rapport favori

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports d'investigation favoris*, page 169

Vous pouvez aisément créer un rapport Favori similaire à un autre rapport favori existant, comme suit.

1. Cliquez sur **Rapports favoris** pour afficher la liste des rapports enregistrés comme favoris.

   > **Remarque**
   > Si votre organisation utilise l'administration déléguée, cette liste ne comprend pas les rapports favoris enregistrés par les autres administrateurs.

2. Sélectionnez et exécutez le rapport favori ressemblant le plus au nouveau rapport que vous souhaitez créer. (Voir *Création ou suppression d'un rapport Favori*, page 170.)
3. Modifiez le rapport affiché selon vos besoins.
4. Cliquez sur **Rapports favoris** pour enregistrer le rapport modifié en tant que favori sous un nouveau nom. (Voir *Enregistrement d'un rapport en tant que Favori*, page 170.)

Planification des rapports d'investigation

Rubriques connexes :

- *Rapports d'investigation favoris*, page 169
- *Enregistrement d'un rapport en tant que Favori*, page 170
- *Gestion des tâches planifiées de rapports d'investigation*, page 174

Vous devez enregistrer le rapport d'investigation en tant que favori pour qu'il puisse être planifié pour une exécution ultérieure ou régulière. Lorsque la tâche du rapport planifié s'exécute, les rapports résultants sont envoyés par message électronique aux destinataires désignés. Lorsque vous créez des tâches planifiées, tenez compte de la taille et de la quantité de fichiers joints que peut gérer votre serveur de messagerie.

Les fichiers des rapports planifiés sont automatiquement enregistrés dans le répertoire suivant :

```
<chemin_installation>\webroot\Explorer\<nom>\
```

Le chemin d'installation par défaut est C:\Program Files\Websense\Web Security. Si la tâche planifiée n'a qu'un seul destinataire, <*nom*> correspond à la première partie de son adresse électronique (située avant le caractère @). Lorsqu'il existe plusieurs destinataires, les rapports sont enregistrés dans un répertoire appelé Other.

> **Remarque**
>
> Les rapports enregistrés à partir d'une tâche récurrente utilisent chaque fois le même nom de fichier. Si vous souhaitez enregistrer les fichiers pour une période plus longue, assurez-vous de modifier le nom du fichier ou de copier ce dernier dans un autre emplacement.
>
> Selon la taille et le nombre de rapports planifiés, ce répertoire peut devenir très volumineux. Assurez-vous de le vider régulièrement, en supprimant tous les fichiers inutiles.

1. Enregistrez un ou plusieurs rapports en tant que Favoris. (Voir *Enregistrement d'un rapport en tant que Favori*, page 170.)
2. Cliquez sur **Rapports favoris** pour afficher la liste des rapports enregistrés comme favoris.

> **Remarque**
>
> Si votre organisation utilise des rôles d'administration déléguée, cette liste ne comprend pas les rapports favoris enregistrés par les autres administrateurs.

3. Mettez en surbrillance jusqu'à 5 rapports à exécuter dans le cadre de la tâche planifiée.
4. Cliquez sur **Planification** pour créer une tâche de rapport planifiée, puis saisissez les informations demandées dans la page Planifier le rapport.

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

Champ	Description
Récurrence	Sélectionnez la fréquence (Une fois, Quotidien, Hebdomadaire, Mensuel) d'exécution de la tâche de rapport.
Date de début	Choisissez le jour de la semaine ou la date à laquelle cette tâche doit s'exécuter pour la première fois (ou pour la seule fois).
Heure d'exécution	Définissez l'heure d'exécution de cette tâche.
Envoyer par e-mail à	Utilisez le champ **Adresses de courrier électronique supplémentaires** pour ajouter les adresses appropriées dans cette liste. Mettez une ou plusieurs adresses électroniques en surbrillance pour recevoir les rapports de cette tâche. (N'oubliez pas de désélectionner les adresses qui ne doivent pas recevoir ces rapports.)
Adresses de courrier électronique supplémentaires	Entrez une adresse électronique, puis cliquez sur **Ajouter** pour la placer dans la liste **Envoyer par e-mail à**. La nouvelle adresse électronique est automatiquement surlignée avec les autres adresses électroniques sélectionnées.
Personnaliser l'objet et le corps du texte du courrier électronique	Cochez cette case pour personnaliser la ligne d'objet de votre notification électronique et le corps du message. Si cette case n'est pas activée, l'objet et le texte par défaut seront utilisés.
Objet du courrier électronique	Entrez le texte devant apparaître dans la ligne d'objet du message électronique lors de l'envoi des rapports planifiés. L'objet par défaut du message électronique est : Tâche de planification des rapports d'investigation
Texte du courrier électronique	Entrez le texte à ajouter dans le message électronique des rapports planifiés envoyés. Le message est identique à celui présenté ci-dessous, votre texte remplaçant le <TEXTE PERSONNALISÉ>. Le planificateur de rapports a généré le ou les fichiers joints le <*date/heure*>. <TEXTE PERSONNALISÉ> Pour afficher le ou les rapports générés, cliquez sur le ou les liens suivants. Remarque : ce lien ne fonctionne pas si le destinataire n'a pas accès au serveur Web d'où provient la tâche.
Planifier le nom de la tâche	Attribuez un nom unique à la tâche planifiée. Ce nom identifie la tâche dans la file d'attente des tâches. Voir *Gestion des tâches planifiées de rapports d'investigation*, page 174.

Champ	Description
Format de sortie	Choisissez le format du fichier des rapports planifiés : **PDF** : les fichiers PDF s'affichent dans Adobe Reader. **Excel** : les fichiers XLS s'affichent dans Microsoft Excel.
Intervalle de dates	Définissez la plage de dates couverte par les rapports de cette tâche. **Toutes les dates** : toutes les dates disponibles dans la Base de données d'activité. **Relatif** : choisissez une période (Jours, Semaines ou Mois) et la période spécifique à inclure (Ce(tte), Dernier(ère)(s), Deux dernier(ère)s, etc.). **Spécifique** : définissez les dates ou une plage de dates spécifiques pour les rapports de cette tâche.

5. Cliquez sur **Suivant** pour ouvrir la page Confirmation de planification.
6. Cliquez sur **Enregistrer** pour enregistrer vos sélections et ouvrir la page File d'attente des tâches (voir *Gestion des tâches planifiées de rapports d'investigation*, page 174).

Gestion des tâches planifiées de rapports d'investigation

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Planification des rapports de présentation*, page 143

Lorsque vous créez une tâche planifiée pour des rapports d'investigation, la page **File d'attente des tâches** s'affiche et présente la nouvelle tâche et la liste des tâches planifiées existantes. Vous pouvez également accéder à cette page en cliquant sur le lien **File d'attente des tâches** de la page principale des rapports d'investigation.

Remarque

Si votre organisation utilise l'administration déléguée, cette page ne présentent pas les tâches planifiées par les autres administrateurs.

La section **Planifier le rapport détaillé** présente la liste des tâches planifiées dans l'ordre de leur création en indiquant le planning défini et l'état de chaque tâche. Les options suivantes sont également disponibles.

Option	Description
Modifier	Présente le planning défini pour cette tâche et vous permet de le modifier si nécessaire
Supprimer	Supprime la tâche et ajoute l'entrée dans la section Journal d'état en désignant cette tâche comme Supprimée

La section **Journal d'état** présente la liste des tâches qui ont été modifiées, en indiquant l'heure de début planifiée, l'heure de fin réelle et l'état.

Cliquez sur **Effacer le journal d'état** pour supprimer toutes les entrées de la section Journal d'état.

Rapports Cas particuliers

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Rapports récapitulatifs*, page 154

Un rapport Cas particuliers présente les utilisateurs dont l'activité Internet est la plus hors norme dans la base de données. Websense calcule l'activité moyenne de tous les utilisateurs par catégorie, par jour, par action (disposition) et par protocole. Il affiche ensuite l'activité des utilisateurs qui s'écartent le plus de cette moyenne statistique. L'écart est calculé en tant qu'écart standard par rapport à la moyenne.

1. Dans la page principale des rapports d'investigation, créez un rapport récapitulatif contenant les informations pour lesquelles vous souhaitez connaître les cas particuliers. Les sélections soulignées et présentées en bleu à côté du champ « Utilisation d'Internet par » se reflètent dans le rapport Cas particuliers.

   Par exemple, pour afficher les cas particuliers par accès pour une catégorie spécifique, sélectionnez **Catégorie** dans la liste **Utilisation d'Internet par** et **Accès** en tant que **Mesure**.

   > **Remarque**
   > Les rapports de cas particuliers ne sont pas générés pour le temps de navigation. Si vous partez d'un rapport récapitulatif présentant le temps de navigation, le rapport Cas particuliers est basé sur les accès.

2. Cliquez sur **Cas particuliers**.

   Les lignes sont triées par ordre décroissant, l'écart le plus important étant affichant en premier. Chaque ligne indique :

   - Le Total (accès ou bande passante) pour l'utilisateur, la catégorie, le protocole, le jour et l'action
   - La Moyenne (accès ou bande passante) pour tous les utilisateurs, cette catégorie, ce protocole, ce jour et cette action
   - L'écart de l'utilisateur par rapport à la moyenne

3. Pour afficher l'activité dans le temps d'un utilisateur individuel dans cette catégorie, cliquez sur le nom de cet utilisateur.

   Par exemple, si l'activité d'un utilisateur est sensiblement élevée un certain jour, cliquez sur son nom pour afficher un rapport permettant de mieux comprendre son activité générale.

Sortie dans un fichier

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Impression des rapports d'investigation*, page 176

Après la création d'un rapport d'investigation, vous pouvez utiliser les boutons situés au-dessus du rapport pour l'enregistrer dans un fichier. Le bouton sur lequel vous cliquez détermine le format du fichier.

Option	Description
	Enregistre le rapport au format XLS Si Microsoft Excel 2003 ou une version ultérieure est installée dans l'ordinateur à partir duquel vous accédez à TRITON - Web Security, vous êtes invité(e) à afficher ou à enregistrer le rapport. Autrement, vous êtes invité(e) à sélectionner un répertoire et le nom de fichier du rapport enregistré. Servez-vous des options de Microsoft Excel pour imprimer, enregistrer ou envoyer le rapport par courrier électronique.
	Crée un rapport au format PDF Si Adobe Reader v7.0 ou une version ultérieure est installée dans l'ordinateur à partir duquel vous accédez à TRITON - Web Security, vous êtes invité(e) à afficher ou à enregistrer le rapport. Autrement, vous êtes invité(e) à sélectionner un répertoire et le nom de fichier du rapport enregistré. Servez-vous des options d'Adobe Reader pour imprimer, enregistrer ou envoyer le rapport par courrier électronique.

Impression des rapports d'investigation

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Sortie dans un fichier*, page 176

Pour imprimer des rapports d'investigation :

- Utilisez la fonction d'impression de votre navigateur Web lorsque le rapport est affiché.
- Créez un fichier PDF ou XLS, puis utilisez la fonction d'impression d'Adobe Reader ou de Microsoft Excel (voir *Sortie dans un fichier*, page 176).

Bien que les rapports aient été configurés pour s'imprimer depuis le navigateur, vous pouvez tester l'impression pour vérifier le résultat.

Les rapports Activité utilisateur par mois sont configurés pour une impression au format paysage. Tous les autres rapports sont configurés pour une impression en mode portrait.

Lorsque vous créez votre propre rapport (voir *Rapports détaillés flexibles*, page 159), la largeur des colonnes diffère selon les informations incluses. L'orientation de la page passe en mode paysage lorsque le rapport dépasse le format A4 (21,59 x 27,49 cm).

La largeur du contenu de la page est de 184 mm ou de 254 mm. Dans le cas du format A4, les marges sont légèrement plus étroites mais restent dans la zone imprimable. (La taille du papier par défaut est Lettre, ou 21,59 x 27,49 cm. Si vous utilisez du papier A4, assurez-vous de modifier ce paramètre dans le fichier de configuration wse.ini. Voir *Options d'affichage et de sortie*, page 423.)

Rapports sur activité propre

Rubriques connexes :

- *Rapports d'investigation*, page 152
- *Configuration des préférences de génération de rapports*, page 397
- *Rapports sur activité propre*, page 425

Les rapports sur activité propre de Websense vous permettent d'évaluer vos propres activités Internet et de les ajuster, si nécessaire, pour vous rapprocher des directives de votre organisation. Ils respectent également la législation qui exige que les organisations autorisent les utilisateurs à savoir quels types d'informations les concernant sont collectées.

Si les rapports sur activité propre sont activés dans votre organisation, vous pouvez y accéder depuis votre navigateur :

1. Entrez l'URL fournie par votre administrateur Websense ou cliquez sur le lien Rapports sur activité propre dans la page de connexion principale de TRITON - Web Security pour accéder à la page de connexion des rapports sur activité propre.
2. Si le serveur **Policy Server** présente une liste déroulante, choisissez l'adresse IP de celui qui journalise les informations de votre activité Internet.

   Au besoin, demandez l'aide de votre administrateur Websense.
3. Entrez le **Nom d'utilisateur** et le **Mot de passe** que vous utilisez pour vous connecter au réseau.
4. Cliquez sur **Se connecter**.

TRITON - Web Security affiche un rapport d'investigation présentant votre activité Internet par classe de risques. Cliquez sur les différents liens et éléments de la page pour accéder aux différentes options d'affichage des informations stockées sur votre activité. Servez-vous du système d'**Aide** pour obtenir de l'assistance lorsque vous travaillez avec les rapports.

Real-Time Monitor

Rubriques connexes :

- *Exploitation des rapports pour évaluer l'efficacité du filtrage*, page 129
- *Real-Time Monitor dans les déploiements à plusieurs serveurs Policy Server*, page 180

Servez-vous de la page **Génération de rapports > Real-Time Monitor** pour afficher l'activité du filtrage Internet en cours dans votre réseau.

Important

L'Affichage de compatibilité Internet Explorer 8 n'est **pas** pris en charge avec la console TRITON. Si Real-Time Monitor ne s'affiche pas correctement dans Internet Explorer 8, vérifiez que le bouton Affichage de compatibilité (situé entre l'URL et le bouton Actualiser de la barre d'adresse du navigateur) n'est pas activé.

Cliquez sur **Démarrer** pour renseigner la page. La page présente alors les requêtes Internet récentes, dont :

- L'adresse IP ou le nom de l'**utilisateur** à l'origine de la demande
  - Si vous utilisez le filtrage par utilisateur dans votre réseau et que le nom d'utilisateur s'affiche, survolez une entrée avec votre souris pour voir l'adresse IP.
  - Lorsque le nom d'utilisateur comprend plus de 30 caractères, un tiret (« - ») et les derniers 30 caractères du nom s'affichent. Si vous cliquez du bouton droit pour ajouter un long nom d'utilisateur dans le filtre de recherche, supprimez le tiret dans le champ du filtre, puis cliquez sur **Show Results (Afficher les résultats)** pour afficher les entrées correspondantes.
- L'**URL** demandée

  Par défaut, lorsque l'URL est trop longue pour pouvoir s'afficher dans l'espace fourni, le champ présente ses 30 premiers caractères, un espace, un tiret (« - ») et un espace, puis ses 20 derniers caractères. Cliquez du bouton droit sur l'URL tronquée pour afficher la chaîne dans son intégralité.

  Cliquez sur **Personnaliser** dans la barre d'outils située en haut de la page, puis sélectionnez **Show the full URL (Afficher l'URL complète)** pour modifier ce comportement.
- Si le site demandé a été ou non classé dans une catégorie après une analyse de Content Gateway
  - La présence d'une icône signale que le site a été recatégorisé dynamiquement sur la base des résultats de l'analyse. Survolez l'icône avec votre souris pour identifier la catégorie d'origine.
  - L'absence d'icône indique que la catégorie Base de données principale ou une catégorie d'URL personnalisée a été utilisée. (Cela inclut les sites que Content Gateway a analysés, mais n'a pas recatégorisés.)

- La **Catégorie** affectée au site

  La véritable catégorie utilisée pour filtrer la requête est indiquée, qu'il s'agisse de la catégorie Base de données principale, de la catégorie des URL personnalisées ou d'une catégorie affectée dynamiquement suite à une analyse.

- L'**Action** (autorisée ou bloquée) appliquée à la requête

  Survolez une entrée avec votre souris pour afficher la ou les stratégies utilisées pour déterminer l'action à appliquer. Plusieurs stratégies peuvent être répertoriées si, par exemple :

  - Plusieurs stratégies de groupe pouvaient s'appliquer au même utilisateur
  - Une stratégie a été affectée à la fois à l'adresse IP et à l'utilisateur ou au groupe

  Lorsque plusieurs stratégies sont répertoriées, vous pouvez utiliser l'outil Tester le filtrage (de la boîte à outils de TRITON - Web Security) pour identifier la stratégie prioritaire pour une requête de l'utilisateur ou l'adresse IP affiché(e) dans Real-Time Monitor.

- L'**Heure** à laquelle la requête a été envoyée à Real-Time Monitor

  Real-Time Monitor récupérant les informations sur les requêtes auprès d'Usage Monitor en temps réel (sans lire dans la Base de données d'activité), l'heure de la requête indiquée ici peut ne pas correspondre à celle indiquée dans les rapports d'investigation ou de présentation.

Pour examiner les données actuelles, cliquez sur **Pause** pour interrompre l'actualisation continuelle de la page. Lorsque vous êtes prêt à surveiller de nouvelles informations, cliquez de nouveau sur **Démarrer**.

- Par défaut, les données sont actualisées toutes les 15 secondes. Pour modifier cette fréquence d'actualisation, cliquez sur **Personnaliser** dans la barre d'outils située en haut de la page, puis sélectionnez une nouvelle valeur **Data refresh rate (Fréquence d'actualisation des données)**.

Selon vos paramètres actuels, Real-Time Monitor stocke un nombre défini d'enregistrements (250, 500 ou 1 000) et affiche systématiquement le jeu d'enregistrements le plus récent à sa disposition. Lorsque vous interrompez l'affichage des nouveaux enregistrements pour examiner les données en cours, les centaines, voire les milliers de requêtes pouvant survenir entre-temps ne sont pas disponibles pour l'affichage. (Ces requêtes sont toutefois stockées dans la Base de données d'activité et apparaîtront dans les rapports d'investigation et de présentation.)

Pour modifier le nombre d'enregistrements affichés, cliquez sur **Personnaliser** dans la barre d'outils située en haut de la page, puis sélectionnez une nouvelle valeur pour **Number of records shown (Nombre d'enregistrements affichés)**.

Filtrage des données de rapport

Pour filtrer les données affichées à l'écran :

1. Entrez tout ou partie d'un nom d'utilisateur ou d'une adresse IP, d'une URL, d'une catégorie ou d'une action dans les champs **Filter results by (Filtrer les résultats par)**. Vous pouvez également sélectionner un filtre temporel pour afficher les 5, 10 ou 15 dernières minutes de résultats applicables.
2. Cliquez sur **Show Results (Afficher les résultats)**.
3. Pour réafficher tous les résultats, cliquez sur **Clear Search Filters (Effacer les filtres de recherche)**.

Vous pouvez également cliquer du bouton droit sur une entrée des champs Utilisateur, URL, Catégorie ou Action et sélectionner l'option **Filtrer par** ou **Add...to search filter (Ajouter... au filtre de recherche)** pour filtrer aussitôt les résultats en fonction de la chaîne sélectionnée.

Fonctionnement du comportement de l'expiration

Par défaut, les sessions TRITON Unified Security Center expirent au bout de 30 minutes. Pour exécuter Real-Time Monitor sans expiration, cliquez sur **Plein écran** pour l'ouvrir dans une nouvelle fenêtre. L'adresse IP du serveur Policy Server surveillé est affichée dans la barre de titre de Real-Time Monitor. Pour surveiller plusieurs instances de Policy Server, consultez la section *Real-Time Monitor dans les déploiements à plusieurs serveurs Policy Server*, page 180, pour découvrir les considérations et les instructions associées.

Real-Time Monitor dans les déploiements à plusieurs serveurs Policy Server

Lorsque vous ouvrez la page Génération de rapports > Real-Time Monitor dans TRITON - Web Security, Real-Time Monitor présente des informations sur l'instance de Policy Server à laquelle la console de gestion est actuellement connectée. Cela signifie que si vous utilisez plusieurs instances de Policy Server, lorsque vous connectez la console de gestion à une nouvelle instance de Policy Server, Real-Time Monitor commence à afficher des informations pour un autre jeu de clients du filtrage.

Pour que Real-Time Monitor continue à surveiller le trafic d'une instance de Policy Server spécifique, quelle que soit celle à laquelle TRITON - Web Security est connecté, cliquez sur **Plein écran** pour ouvrir Real-Time Monitor dans une nouvelle fenêtre. L'adresse IP de l'instance de Policy Server surveillée est indiquée en haut de l'écran.

- Real-Time Monitor reçoit les informations sur l'activité Internet envoyées par Usage Monitor. Chaque instance de Policy Server doit être associée à une instance d'Usage Monitor pour que Real-Time Monitor puisse afficher son activité de filtrage.
- Vous pouvez exécuter plusieurs instances de Real-Time Monitor en mode plein écran, montrant chacune les données d'une instance de Policy Server différente :
  1. Ouvrez TRITON - Web Security. Ce dernier se connectera à l'instance centrale (par défaut) de Policy Server.
  2. Ouvrez la page Génération de rapports > Real-Time Monitor, puis cliquez sur Plein écran.

     L'adresse IP de l'instance centrale de Policy Server s'affiche dans la barre de titre.
  3. Revenez dans TRITON - Web Security et servez-vous du bouton Policy Server Connection (Connexion à Policy Server) de la barre d'outils de TRITON pour vous connecter à une autre instance de Policy Server.
  4. Reprenez l'étape 2.
  5. Répétez cette procédure pour chaque instance de Policy Server supplémentaire de votre réseau.
- En mode plein écran, Real-Time Monitor n'expire jamais.

9 Options d’analyse et contournement du décryptage SSL

Rubriques connexes :

- *Options d’analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Détection des protocoles mis en tunnel*, page 186
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Options avancées*, page 191
- *Exceptions d’analyse*, page 193
- *Fichiers de données utilisés avec l’analyse*, page 195
- *Génération de rapports sur l’activité d’analyse*, page 196
- *Contournement du décryptage SSL*, page 198

Des options d’analyse (avancée) et des fonctions de contournement du décryptage SSL sont disponibles avec Websense Web Security Gateway et Websense Web Security Gateway Anywhere.

Les **options d’analyse** autorise l’analyse avancée du trafic Web lorsqu’il passe par le module Content Gateway (proxy Websense sur site). Seuls les sites qui ne sont pas encore bloqués, sur la base de la stratégie active, sont analysés.

- *Catégorisation du contenu*, page 184, catégorise le contenu des URL non présentes dans la Base de données principale de Websense et des sites qui renferment du contenu dynamique, identifiés comme tels par les laboratoires Websense Security Labs. L’analyse renvoie une catégorie à utiliser pour le filtrage.
- *Détection des protocoles mis en tunnel*, page 186, analyse le trafic pour identifier les protocoles mis en tunnel sur **HTTP** et **HTTPS**. Ce type de trafic est signalé au filtrage Web de Websense de sorte que les stratégies de protocoles soient imposées. L’analyse porte à la fois sur le trafic entrant et sortant.
- *Risques de sécurité : Sécurité du contenu*, page 187, analyse le contenu entrant afin d’identifier les menaces de sécurité, telles que le phishing, les programmes malveillants, les virus, les redirections d’URL, les exploits Web et l’antiblocage par proxy, entre autres.

- *Risques de sécurité : Analyse des fichiers*, page 188, applique deux méthodes d'inspection pour détecter les menaces pesant sur la sécurité.
  - La **Détection avancée de Websense** pour identifier le contenu malveillant tel que les virus, les chevaux de Troie et les vers, en renvoyant une catégorie de menaces pour imposer la stratégie
  - Les **Fichiers de définition antivirus (AV) classiques** pour identifier les fichiers infectés par des virus

  Lorsque l'option Advanced Detection (Détection avancée) ou Antivirus File Scanning (Analyse antivirus des fichiers) est activée, vous pouvez éventuellement analyser :
  - **Les applications Internet multimédia**, par exemple les fichiers Flash, pour détecter et bloquer le contenu malveillant
  - **Les fichiers FTP** pour détecter et bloquer le contenu malveillant

  Les options d'analyse des types de fichiers (**File Type Scanning Options**) déterminent sur quels types de fichiers porte l'analyse du contenu malveillant, y compris sur les fichiers exécutables et non reconnus. Des extensions de fichiers individuelles peuvent également être définies.
- *Sécurité sortante*, page 190, propose deux types d'analyse du contenu sortant. La première effectue une analyse du contenu sortant qui reflète votre configuration de l'analyse du contenu des menaces entrantes pour la sécurité et l'analyse des fichiers. La seconde analyse les vols de données, en examinant et en bloquant les fichiers cryptés personnalisés sortants, les fichiers de mots de passe et autres données sensibles.
- Le contrôle de la **sensibilité de la catégorisation du contenu et de l'analyse** vous permet d'ajuster les seuils de sensibilité de la Catégorisation du contenu et de l'Analyse du contenu (voir *Options avancées*, page 191).
- Dans le cas des vastes transactions en temps réel ou des transactions lentes, l'option **Content Delay Handling (Gestion du délai du contenu)** vous donne un certain contrôle sur le délai devant s'écouler avant que la partie du contenu mis en mémoire tampon soit envoyée au client (voir *Options avancées*, page 191).
- Les options avancées **Scanning Timeout (Expiration de l'analyse), Limite de taille des fichiers** et **Découpage du contenu** s'appliquent à l'ensemble du trafic transitant par le proxy (voir *Options avancées*, page 191).

Plusieurs rapports de présentation peuvent fournir des détails sur le mode de protection appliqué par les fonctions d'analyse avancées pour protéger votre réseau contre les tentatives d'accès aux sites contenant des menaces. Voir *Génération de rapports sur l'activité d'analyse*, page 196.

Les options de **contournement du décryptage SSL** permettent de définir les clients, les sites Web et les catégories de sites Web **non** soumis au décryptage et à l'analyse lorsqu'ils passent par le proxy. Ces options s'appliquent uniquement si SSL Manager est activé dans Content Gateway. Voir *Contournement du décryptage SSL*, page 198.

Les **exceptions d'analyse** sont des listes de noms d'hôte ou d'URL systématiquement analysées ou jamais analysées. Le type d'analyse à effectuer ou à ignorer systématiquement est spécifié par nom d'hôte/URL ou groupe de noms d'hôte/URL. Une liste d'adresses IP des clients dont le contenu n'est jamais analysé doit également être définie. Voir *Exceptions d'analyse*, page 193.

Activation de l’analyse et des fonctions de contournement du décryptage SSL

Pour activer les fonctions d’analyse avancées et de contournement du décryptage SSL disponibles avec Websense Web Security Gateway et Gateway Anywhere, vous devez saisir une clé d’abonnement appropriée dans TRITON - Web Security. Vous pouvez saisir cette clé :

- Lorsque vous y êtes invité(e) après la connexion
- Dans la page **Paramètres > Général > Policy Servers (Serveurs Policy Server)**

Vérifiez les informations actuelles de la clé dans la page Paramètres > Général > Compte. La clé est automatiquement transmise à toutes les instances de Content Gateway associées à l’instance de Policy Server en cours. Pour plus d’informations, consultez *Vérification des connexions à Policy Server*, page 361, et *Gestion des connexions à Content Gateway*, page 372.

Pour plus d’informations sur la configuration des options d’analyse avancées, consultez la section *Options d’analyse*, page 183. Pour plus d’informations sur les options de contournement du décryptage SSL, consultez la section *Contournement du décryptage SSL*, page 198.

Options d’analyse

Rubriques connexes :

- *Catégorisation du contenu*, page 184
- *Détection des protocoles mis en tunnel*, page 186
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Options avancées*, page 191
- *Exceptions d’analyse*, page 193
- *Génération de rapports sur l’activité d’analyse*, page 196

Les options d’analyse sont disponibles avec Websense Web Security Gateway et Websense Web Security Gateway Anywhere. Ces options contrôlent le type d’analyse avancée pouvant être effectuée sur le trafic Web lorsqu’il transite par le module Content Gateway (proxy Websense sur site).

Pour obtenir une présentation des options d’analyse avancées et des autres options liées à Content Gateway, consultez la section *Options d’analyse et contournement du décryptage SSL*, page 181.

La page **Paramètres > Scanning (Analyse) > Scanning Options (Options d’analyse)** vous permet de configurer les éléments suivants :

- *Catégorisation du contenu*, page 184
- *Détection des protocoles mis en tunnel*, page 186
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190

- La sensibilité de l'analyse, l'expiration de l'analyse, la limite de taille de l'analyse, la gestion du délai du contenu et le découpage du contenu (voir *Options avancées*, page 191)

Les paramètres de base sont les suivants :

- **Off (Désactivé)** : pas d'analyse
- **On (Activé)** (par défaut) : analyse du contenu ou des fichiers présentant des profils de risque élevés, identifiés comme tel par les laboratoires Websense Security Labs
- **Aggressive analysis (Analyse agressive)** : analyse du contenu et des fichiers présentant des profils de risque élevés et faibles. L'analyse agressive consomme davantage de ressources. Pour de meilleurs résultats, surveillez les performances du système et faites évoluer ses ressources en fonction de la demande.

En plus des paramètres d'analyse On/Off/Aggressive, l'analyse est effectuée ou non en fonction des listes d'exceptions Toujours analyser, Ne jamais analyser et de listes d'exceptions d'adresses IP de client. Ces listes sont gérées dans la page **Paramètres** > **Scanning (Analyse)** > **Scanning Exceptions (Exceptions d'analyse)**. Voir *Exceptions d'analyse*, page 193.

Avertissement

Les sites présents dans la liste Ne jamais analyser ne sont analysés en aucune circonstance. Lorsque l'un des sites de la liste Ne jamais analyser est compromis, les options d'analyse n'analysent pas et ne détectent pas le code malveillant.

Lorsque la configuration est terminée dans la page en cours, 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)**.

Catégorisation du contenu

Rubriques connexes :

- *Options d'analyse*, page 183
- *Détection des protocoles mis en tunnel*, page 186
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Options avancées*, page 191
- *Exceptions d'analyse*, page 193
- *Génération de rapports sur l'activité d'analyse*, page 196

Lorsqu'une page Web est demandée, la catégorisation du contenu intervient dans les cas suivants :

- L'URL n'est pas déjà bloquée par la stratégie active.
- L'URL n'est pas répertoriée dans la Base de données principale de Websense.
- L'URL présente un profil de risque élevé, identifié comme tel par les laboratoires Websense Security Labs.

La catégorie identifiée par la catégorisation du contenu est transmise au logiciel de filtrage de Websense pour imposer la stratégie.

La catégorisation du contenu peut éventuellement inclure une **analyse des liens d'URL intégrés au contenu**. Cette analyse affine la classification de certains types de contenus. Par exemple, une page qui ne contient que peu, voire aucun contenu indésirable, mais qui comprend des liens vers des sites connus pour leur contenu indésirable peut elle-même être catégorisée de façon plus précise. L'analyse des liens se révèle particulièrement efficace pour 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. Pour plus d'informations sur l'optimisation de la couverture grâce à l'analyse du voisinage des liens, lisez le billet de blog de Websense Security Labs In Bad Company (En mauvaise compagnie).

L'efficacité de la catégorisation du contenu et de l'analyse des liens est mesurée dans plusieurs rapports de présentation. Pour plus d'informations, consultez la section *Rapports de présentation*, page 131.

Important

Si vous envisagez de générer des rapports sur l'activité de l'analyse avancée, activez la journalisation des URL complètes (voir *Configuration de la journalisation des URL*, page 413). Sinon, les enregistrements du journal ne contiendront que le domaine (www.domaine.com) des sites catégorisés, et les pages individuelles d'un site peuvent appartenir à des catégories différentes.

Si votre site utilise WebCatcher pour signaler les URL non catégorisées à Websense, Inc. (voir *Qu'est-ce que WebCatcher ?*, page 30), les URL catégorisées via la catégorisation du contenu sont transmises pour être ajoutées dans la base de données principale.

Pour configurer la catégorisation du contenu :

1. Sélectionnez **Paramètres > Scanning (Analyse) > Scanning Options (Options d'analyse)**.
2. Sélectionnez **Off (Désactivé)** pour désactiver la catégorisation du contenu.
3. Sélectionnez **On (Activé)** (par défaut) pour activer la catégorisation du contenu.
4. Pour inclure l'analyse des liens intégrés, sélectionnez **Analyse des liens intégrés au contenu Web**. Les requêtes bloquées par l'analyse des liens sont enregistrées et peuvent être affichées dans les rapports de présentation de l'Activité d'analyse.
5. Lorsque vous avez terminé, 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 algorithmes utilisés pour effectuer la catégorisation du contenu sont mis au point par Websense Security Labs afin de garantir les meilleurs résultats possibles à la plupart des organisations. Toutefois, si le paramètre optimisé n'a pas les effets escomptés, vous pouvez ajuster le niveau de sensibilité pour obtenir des résultats plus restrictifs ou plus permissifs. Reportez-vous à la section *Options avancées* de cet écran.

Détection des protocoles mis en tunnel

Rubriques connexes :

- *Options d’analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Options avancées*, page 191
- *Exceptions d’analyse*, page 193
- *Génération de rapports sur l’activité d’analyse*, page 196

La détection des protocoles mis en tunnel analyse le trafic pour identifier les protocoles mis en tunnel sur HTTP et HTTPS. Le trafic dont la mise en tunnel est autorisée sur certains ports est également analysé. Ce type de trafic est signalé au filtrage Web de Websense de sorte que les stratégies de protocoles soient imposées. Lorsque la détection des protocoles mis en tunnel est activée, l’analyse porte à la fois sur le trafic entrant et sortant, quels que soient les autres paramètres de l’analyse.

Une mise en tunnel HTTP se produit lorsque des applications utilisant des protocoles de communication personnalisés sont encapsulées dans du trafic HTTP (c’est-à-dire qu’une mise en forme de requête/réponse HTTP standard est présente) pour utiliser les ports désignés pour le trafic HTTP/HTTPS. Ces ports sont ouverts pour autoriser le trafic destiné à et provenant d’Internet. La mise en tunnel HTTP permet à ces applications de contourner les pare-feu et les proxy, ouvrant une faille dans le système.

La fonction de détection des protocoles mis en tunnel analyse le trafic HTTP et HTTPS et, lorsqu’elle détecte un protocole, le transmet au filtrage Web de Websense pour imposer les stratégies. À ce stade, le protocole en question est bloqué ou autorisé en fonction des stratégies définies. Cette fonction permet de bloquer les protocoles utilisés pour la messagerie instantanée, les applications P2P et le contournement du proxy. Notez que certaines applications s’exécutant sur HTTP (par exemple, Google Video) peuvent ne pas afficher la page de blocage des protocoles. Pour plus d’informations sur le filtrage des protocoles, consultez la section *Filtrage des catégories et des protocoles*, page 50.

Remarque

La détection des protocoles mis en tunnel intervient avant la catégorisation du contenu. En conséquence, lorsqu’un protocole mis en tunnel est identifié, la stratégie du protocole est imposée et le contenu n’est pas catégorisé.

La page **Paramètres > Scanning (Analyse) > Scanning Options (Options d’analyse)** vous permet d’activer et de configurer la détection des protocoles mis en tunnel :

1. Sélectionnez **Off (Désactivé)** pour désactiver la détection des protocoles mis en tunnel.

2. Sélectionnez **On (Activé)** (par défaut) pour analyser l'ensemble du trafic et détecter les protocoles mis en tunnel sur HTTP ou HTTPS. Ce type de trafic est signalé au filtrage Web pour imposer les stratégies.
3. 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)**.

La page **Paramètres > Scanning (Analyse) > Scanning Exceptions (Exceptions d'analyse)** vous permet de définir les sites approuvés qui ne doivent jamais être analysés (voir *Exceptions d'analyse*, page 193).

Risques de sécurité : Sécurité du contenu

Rubriques connexes :

- *Options d'analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Détection des protocoles mis en tunnel*, page 186
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Options avancées*, page 191
- *Exceptions d'analyse*, page 193
- *Génération de rapports sur l'activité d'analyse*, page 196

La sécurité du contenu effectue une analyse du contenu des pages Web afin de détecter les risques de sécurité et le code malveillant présents dans le contenu HTTP et HTTPS (HTTPS lorsque Content Gateway SSL Manager est activé).

La page **Paramètres > Scanning (Analyse) > Scanning Options (Options d'analyse)** vous permet d'activer et de configurer la sécurité du contenu.

1. Sélectionnez **Off (Désactivé)** pour désactiver l'analyse du contenu.
2. Sélectionnez **On (Activé)** (par défaut) pour activer l'analyse du contenu des sites non catégorisés et des sites présentant des profils de risque élevés, identifiés comme tels par les laboratoires Websense Security Labs.
3. Sélectionnez **Aggressive analysis (Analyse agressive)** pour analyser le contenu des sites présentant des profils de risque élevés et faibles. Cette option consomme davantage de ressources système.
4. Lorsque vous avez terminé, 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)**.

La page **Paramètres > Scanning (Analyse) > Scanning Exceptions (Exceptions d'analyse)** vous permet de définir les sites approuvés ou non qui ne doivent jamais être analysés ou systématiquement analysés (voir *Exceptions d'analyse*, page 193).

La sensibilité de l'analyse du contenu est réglée par Websense Security Labs pour garantir les meilleurs résultats possibles à la plupart des organisations. Toutefois, si le paramètre d'optimisation n'a pas les effets escomptés, vous pouvez ajuster le niveau de sensibilité via la section *Options avancées*.

Risques de sécurité : Analyse des fichiers

Rubriques connexes :

- *Options d’analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Sécurité sortante*, page 190
- *Options avancées*, page 191
- *Exceptions d’analyse*, page 193
- *Génération de rapports sur l’activité d’analyse*, page 196

L’analyse des fichiers recherche la présence de virus et autres contenus malveillants dans les fichiers que les utilisateurs tentent de télécharger ou d’ouvrir à distance. L’analyse des fichiers renvoie une catégorie au filtrage Websense pour imposer les stratégies définies.

Il existe 4 types d’analyse de fichiers. Ces quatre types peuvent être combinés.

- **La détection avancée** applique les techniques développées par Websense pour identifier les menaces connues ou émergentes, y compris les virus, les chevaux de Troie, les vers et autres contenus malveillants.
- **L’analyse antivirale** utilise les fichiers de définition des virus pour identifier les fichiers infectés par des virus.
- **L’analyse des applications Internet multimédia** recherche du contenu malveillant dans les fichiers Flash.
- **L’analyse des fichiers FTP** recherche du contenu malveillant dans les fichiers FTP.

Pour configurer les différents types de fichiers à analyser, cliquez sur **File Type Options (Options de types de fichier)**.

Remarque

Si l’analyse des fichiers est configurée de manière à inclure les fichiers multimédia, lorsque le contenu en streaming est mis en mémoire tampon et analysé, la connexion au serveur peut arriver à expiration. Dans ce cas, la meilleure solution consiste à créer une exception pour ce site. Voir *Exceptions d’analyse*.

La page **Paramètres > Scanning (Analyse) > Scanning Exceptions (Exceptions d’analyse)** vous permet de définir les sites approuvés ou non qui ne doivent jamais être analysés ou systématiquement analysés (voir *Exceptions d’analyse*, page 193).

La page **Paramètres > Scanning (Analyse) > Scanning Options (Options d’analyse)** vous permet d’activer et de configurer l’analyse des fichiers.

Détection avancée

1. Sélectionnez **Off (Désactivé)** pour désactiver l'analyse des fichiers.
2. Sélectionnez **On (Activé)** (par défaut) pour activer l'analyse des fichiers provenant de sites non catégorisés et de sites présentant des profils de risque élevés, identifiés comme tels par les laboratoires Websense Security Labs.
3. Sélectionnez **Aggressive analysis (Analyse agressive)** pour analyser les fichiers entrants provenant de sites présentant des profils de risque élevés et faibles. Cette option consomme davantage de ressources système.

Analyse antivirus

1. Sélectionnez **Off (Désactivé)** pour désactiver l'analyse antivirus.
2. Sélectionnez **On (Activé)** (par défaut) pour activer l'analyse antivirus des fichiers provenant de sites non catégorisés et de sites présentant des profils de risque élevés, identifiés comme tels par les laboratoires Websense Security Labs.
3. Sélectionnez **Aggressive analysis (Analyse agressive)** pour appliquer l'analyse antivirus aux fichiers entrants qui proviennent de sites présentant des profils de risque élevés et faibles. Cette option consomme davantage de ressources système.

Analyse des applications Internet multimédia

Sélectionnez **Analyse des applications Internet multimédia** pour détecter le contenu malveillant dans les fichiers Flash.

Analyse des fichiers FTP

Sélectionnez **Scan FTP files (Analyse des fichiers FTP)** pour analyser les fichiers téléchargés via le protocole FTP. (Les téléchargements de fichiers FTP sur HTTP sont soumis aux paramètres d'analyse des fichiers HTTP/HTTPS.) Pour avoir un sens, cette option implique que Content Gateway soit configuré de sorte que le trafic FTP passe par un proxy. Consultez l'Aide de Content Gateway Manager.

> **Remarque**
>
> Les options **Analyse des applications Internet multimédia** et **Scan FTP files (Analyse des fichiers FTP)** ne sont disponibles que si la Détection avancée est activée. Lorsque la fonction d'analyse de fichiers Détection avancée est désactivée, la fonction d'analyse des applications Internet multimédia est désactivée, de même que sa case à cocher.

Options de types de fichiers

1. Pour définir les types de fichiers à analyser, cliquez sur **File Type Options (Options de types de fichiers)**. Il est recommandé d'analyser tous les fichiers suspects identifiés comme tels par les laboratoires Websense Security Labs, de même que tous les fichiers exécutables et non reconnus.
2. Pour systématiquement analyser les fichiers qui présentent une extension spécifique, sélectionnez **Files with the following extensions (Fichiers présentant les extensions suivantes)**, entrez une extension dans le champ de saisie, puis cliquez sur **Ajouter**.

   Pour retirer une extension de la liste, cliquez sur celle-ci pour la sélectionner, puis sur **Supprimer**.

Lorsque la configuration des options d'analyse de fichiers est terminée, 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)**.

Plusieurs rapports de présentation fournissent des détails sur les tentatives de téléchargement de fichiers contenant des menaces. Ces rapports ne sont répertoriés dans le Catalogue de rapports que si l'analyse a détecté des sites dont l'activité a changé depuis leur affectation à une catégorie de la Base de données principale. Pour plus d'informations, consultez la section *Rapports de présentation*, page 131.

Pour plus d'informations sur le blocage des fichiers en fonction du type et de la catégorie d'URL, consultez la section *Gestion du trafic en fonction du type de fichiers*, page 273.

Sécurité sortante

Rubriques connexes :

- *Options d'analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Exceptions d'analyse*, page 193
- *Génération de rapports sur l'activité d'analyse*, page 196
- *Options avancées*, page 191

La sécurité sortante :

- Effectue une analyse du contenu sortant qui reflète votre configuration des menaces de sécurité entrantes. Cette option prend également en charge les contrôles du Web social de TRITON - Web Security.
- Assure une protection particulière contre les vols de données grâce à l'examen et au blocage des fichiers cryptés personnalisés sortants, des fichiers de mots de passe et d'autres données sensibles.

1. Activez l'option **Analyze for and block outbound security threats (Analyser et bloquer les risques de sécurité sortants)** (par défaut) pour analyser le contenu sortant et rechercher le trafic « zombie » ou « d'appel automatique ». Cette option effectue une analyse du contenu sortant qui reflète votre configuration des menaces de sécurité entrantes.

   Important

   Cette option doit être activée pour prendre en charge les contrôles du Web social de TRITON - Web Security.

2. Activez l'option **Data theft protection (Protection contre les vols de données)** (par défaut) pour analyser et bloquer les fichiers cryptés personnalisés sortants, les fichiers de mots de passe et les fichiers contenant des données sensibles ou suspectes. Les résultats de cette analyse s'affichent dans le tableau de bord Threats (Menaces) et dans les rapports et les journaux de transactions.

Options avancées

Rubriques connexes :

- *Options d’analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Exceptions d’analyse*, page 193
- *Génération de rapports sur l’activité d’analyse*, page 196

Utilisez ces options pour :

- Définir le niveau de sensibilité de l’analyse de la catégorisation et de la sécurité du contenu
- Définir la limite temporelle de l’analyse*
- Définir la limite de taille de l’analyse*
- Activer le découpage de types de code spécifiques du contenu HTML*

*Ces paramètres s’appliquent au trafic entrant dans son intégralité.

Niveau de sensibilité de la catégorisation du contenu et de l’analyse

Les algorithmes utilisés pour la catégorisation du contenu et l’analyse du contenu sont mis au point par les laboratoires Websense Security Labs afin de garantir des résultats optimaux à la plupart des organisations. Toutefois, si le paramètre optimisé n’a pas les effets escomptés, vous pouvez ajuster le niveau de sensibilité pour obtenir des résultats plus restrictifs ou plus permissifs.

Il existe 5 niveaux de sensibilité.

- **Optimized (Optimisé)** est le niveau de sensibilité mis au point par les laboratoires Websense Security Labs.
- **More Stringent (Plus strict)** et **Most Stringent (Le plus strict)** augmentent la sensibilité de l’analyse.
- **Less Stringent (Moins strict)** et **Least Stringent (Le moins strict)** réduisent la sensibilité de l’analyse.

Lorsque vous avez terminé, 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)**.

Expiration de l’analyse

Chaque analyse de contenu et de fichiers prend un certain temps, qu’il n’est pas possible de déterminer avant le début de l’analyse. Par défaut, pour optimiser le confort d’utilisation, l’analyse est limitée à 1,5 seconde (1 500 millisecondes). Pour ajuster le délai d’expiration, sélectionnez **Personnaliser** et saisissez une valeur comprise entre 500 et 10 000 (millisecondes).

Limite de taille de l'analyse

La limite de taille de l'analyse représente le seuil que l'analyse ne doit pas dépasser. Dès que ce seuil est atteint, l'analyse cesse. La valeur par défaut est 10 Mo. Pour modifier cette valeur, sélectionnez **Personnaliser** et saisissez une taille en méga-octets.

Gestion du délai du contenu

Selon la configuration de Content Gateway et la charge de travail, les fichiers très volumineux, les transactions en temps réel et les serveurs d'origine lents peuvent laisser des clients en attente de contenu.

Les options de cette section permettent d'envoyer une partie du contenu mis en mémoire tampon au client **avant que l'analyse n'intervienne**. L'analyse commence lorsque toutes les données ont été reçues ou lorsque la limite de taille de l'analyse est dépassée.

Servez-vous de l'option **Begin returning data to the client after (Commencer à envoyer les données au client après)** pour définir le délai devant s'écouler avant qu'un certain pourcentage de données mises en mémoire tampon soit envoyé au client. La valeur par défaut est 30 secondes. Pour entrer une autre valeur, sélectionnez **Personnaliser**.

Servez-vous de l'option **Specify how much data to return to the client (Définir le volume de données à renvoyer au client)** pour définir le pourcentage de données mises en mémoire tampon à envoyer au client. La valeur par défaut est 80 %. Pour saisir une autre valeur (jusqu'à 90 %), sélectionnez **Personnaliser**.

Découpage du contenu

Les menaces pesant sur votre système peuvent être dissimulées dans le **contenu actif** envoyé par l'intermédiaire de pages Web. Le contenu actif est le contenu intégré dans la page HTML qui exécute des actions, par exemple qui exécute une animation ou un programme.

Les options de découpage du contenu de Websense permettent de spécifier que le contenu rédigé en certains langages de programmation (ActiveX, JavaScript ou VB Script) soit retiré des pages Web entrantes. Lorsque le découpage du contenu est activé, l'ensemble du contenu écrit dans les langages de programmation spécifiés sont supprimés des sites désignés comme comprenant du contenu dynamique ou apparaissant dans la liste Toujours analyser (voir *Options d'analyse*, page 183).

Le découpage du contenu intervient seulement après la catégorisation du site par les options d'analyse avancée et l'identification par Websense des stratégies devant s'appliquer.

> **Avertissement**
> Les pages Web qui dépendent du contenu actif supprimé ne fonctionneront pas comme prévu. Pour autoriser un accès total aux sites comprenant du contenu actif, désactivez le découpage du contenu ou ajoutez ces sites dans la liste Ne jamais analyser.

L'utilisateur qui demande une page de contenu actif ne reçoit pas de notification de retrait du contenu.

La section **Paramètres > Scanning (Analyse) > Scanning Options (Options d’analyse) > Advanced Options (Options avancées)** vous permet de définir les options de découpage du contenu.

1. Dans la section **Advanced Options (Options avancées) > Content Stripping (Découpage du contenu)**, sélectionnez les différents types de langage de programmation à retirer des pages Web entrantes.

   Pour désactiver le découpage du contenu de l’un des langages sélectionnés, désactivez la case à cocher associée.

2. Lorsque vous avez terminé, 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)**.

Avertissement

Le découpage du contenu peut générer un contenu altéré et inintelligible. Vous pouvez réduire le nombre de telles occurrences en modifiant légèrement la configuration de Content Gateway.

1) Ouvrez Content Gateway Manager, puis l’onglet **Configurer > Protocoles > HTTP > Confidentialité**.

2) Dans le champ **Remove Headers (Retirer des en-têtes) > Remove Others (Autres retraits)**, ajoutez : Accept-Encoding

3) Cliquez sur **Appliquer**, puis redémarrez Content Gateway.

Exceptions d’analyse

Rubriques connexes :

- *Options d’analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Risques de sécurité : Sécurité du contenu*, page 187
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Sécurité sortante*, page 190
- *Options avancées*, page 191

Les exceptions d’analyse sont des listes de sites approuvés ou non (noms d’hôte et URL) qui ne sont **jamais analysés** ou **toujours analysés**. Le type d’analyse à effectuer ou à ignorer systématiquement est spécifié par nom d’hôte ou URL, ou par groupe de noms d’hôte et d’URL.

Vous pouvez également créer une liste d’adresses IP de clients approuvés dont le contenu ne doit jamais être analysé.

Pour obtenir une présentation des options d’analyse, consultez la section *Options d’analyse et contournement du décryptage SSL*, page 181.

Servez-vous des listes **Toujours analyser** et **Ne jamais analyser** pour ajuster le comportement de la catégorisation du contenu, la détection des protocoles mis en tunnel, les risques de sécurité (analyse du contenu et analyse des fichiers) et le découpage du contenu.

- Lorsque les options de catégorisation du contenu, de sécurité du contenu ou d'analyse des fichiers sont **activées**, les sites de la liste **Toujours analyser** sont systématiquement analysés et ceux de la liste **Ne jamais analyser** ne le sont jamais (voir *Options d'analyse*, page 183).
- Lorsque l'option Tunneled Protocol Detection (Détection des protocoles mis en tunnel) ou **l'analyse agressive** est **activée**, les sites de la liste **Ne jamais analyser** ne sont jamais analysés.

Utilisez la liste Ne jamais analyser avec précaution. Lorsqu'un site de cette liste est compromis, Websense Web Security Gateway ne l'analyse pas et ne peut pas détecter les éventuels problèmes de sécurité.

Exceptions de nom d'hôte/URL

Pour ajouter des sites dans les listes Toujours analyser ou Ne jamais analyser :

1. Cliquez sur le bouton **Add Hostname/URL (Ajouter un nom d'hôte/URL)**.

   Vous pouvez définir un site de différentes manières et spécifier simultanément plusieurs noms d'hôte ou URL.

   - Vous pouvez saisir un simple nom d'hôte, par exemple, **cesite.com**. Veillez à entrer à la fois le domaine et l'extension (**cesite.com** et **cesite.net** sont des hôtes distincts).
   - Les sites comprenant plusieurs intitulés sont pris en charge. Par exemple : **www.bbc.co.uk**
   - Vous pouvez utiliser le caractère générique « * » pour établir une correspondance avec les premiers sous-domaines uniquement.

     Par exemple : ***.yahoo.com**.
   - Vous pouvez saisir une URL ou un nom d'hôte complet ou partiel. Le schéma de début « HTTPS:// » n'est pas nécessaire. Une correspondance exacte est établie avec la chaîne spécifiée.

     Par exemple : **www.exemple.com/media/**

     Ou : **www.youtube.com/watch?v=**
2. Après avoir saisi un nom d'hôte/URL unique ou un groupe de noms d'hôte/URL, sélectionnez les options d'analyse s'appliquant à l'ensemble des sites saisis. Vous pouvez sélectionner une ou plusieurs options.

   Pour appliquer différentes options selon les sites, entrez leurs noms séparément.

   Un même site ne peut apparaître que dans l'une des deux listes. Par exemple, vous ne pouvez pas définir un même site de sorte que les protocoles mis en tunnel ne soient jamais analysés et que la catégorisation du contenu soit systématiquement effectuée.

   Cliquez sur **OK** pour ajouter l'entrée.
3. Pour retirer un site d'une liste, sélectionnez-le, puis cliquez sur **Supprimer**.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Pour modifier les options d'analyse associées à un site :

1. Sélectionnez le site dans la liste et ajustez les options.
2. Lorsque vous avez terminé, 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)**.

Exceptions de clients

La liste Exceptions de clients permet d'identifier des utilisateurs approuvés (adresses IP de client) dont le contenu ne doit jamais être analysé.

Pour ajouter une adresse IP dans cette liste :

Cliquez dans le champ **Enter clients (Entrer des clients)** et saisissez l'adresse IP ou une plage d'adresses IP. Par exemple, 10.201.67.245 ou 10.201.67.245 - 10.201.67.250.

Cliquez sur la flèche droite (>) pour envoyer l'adresse dans la liste.

Pour modifier une entrée :

Sélectionnez l'entrée dans la liste, puis cliquez sur **Modifier**.

Apportez les modifications nécessaires, puis cliquez sur **OK**.

Pour supprimer une entrée :

Sélectionnez l'entrée dans la liste, puis cliquez sur **Supprimer**.

Lorsque vous avez terminé, 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)**.

Fichiers de données utilisés avec l'analyse

Pour fonctionner, l'analyse utilise un jeu de fichiers de données. Ces fichiers sont régulièrement mis à jour par les laboratoires Websense Security Labs et mis à disposition sur le serveur de téléchargement de Websense. De son côté, Websense Content Gateway vérifie régulièrement la présence de fichiers de données d'analyse. Le nom et la version de chaque fichier sont indiqués dans Content Gateway Manager **Monitor (Surveiller) > Mon proxy > Résumé**.

Les mises à jour des fichiers de données et de la Base de données principale Websense (y compris des mises à jour de bases de données et de sécurité en temps réel) sont indépendantes.

Chaque exécution de la commande **./WCGAdmin start** entraîne la vérification de la présence de fichiers de données et leur téléchargement. Si le téléchargement échoue, une nouvelle tentative intervient toutes les 15 minutes jusqu'à la réussite de l'opération.

L'intervalle par défaut de vérification de la présence de mises à jour des bases de données est de 15 minutes. Il s'agit là du paramètre recommandé. Augmenter cet intervalle allonge la fenêtre de vulnérabilité aux exploits émergents non encore signalés (*zero-day*).

Pour modifier l'intervalle d'interrogation, modifiez la valeur **PollInterval** du fichier **/opt/bin/downloadservice.ini** dans l'ordinateur Content Gateway. Après avoir modifié le fichier **downloadservice.ini**, arrêtez et redémarrez Content Gateway depuis la ligne de commande :

```
/opt/WCG/WCGAdmin restart
```

Génération de rapports sur l’activité d’analyse

Rubriques connexes :

- *Options d’analyse*, page 183
- *Catégorisation du contenu*, page 184
- *Risques de sécurité : Analyse des fichiers*, page 188
- *Découpage du contenu*, page 192

Après avoir installé Websense Content Gateway et saisi une clé autorisant les fonctions d’analyse avancée, vous pouvez voir et analyser les effets de ces fonctions dans le tableau de bord et dans les rapports de présentation et d’investigation.

Deux graphiques du tableau de bord Usage tiennent, par défaut, le compte des requêtes destinées aux sites Web 2.0 effectuées au cours des 30 derniers jours :

- Catégories Web 2.0
- Web 2.0 URL Bandwidth (Bande passante : URL Web 2.0)

Pour plus d’informations sur la personnalisation des graphiques ou leur déplacement vers un autre onglet du tableau de bord, consultez la section *Tableau de bord de Web Security*, page 33.

Dans la page **Rapports de présentation**, le groupe **Activité d’analyse** contient les rapports liés à l’activité d’analyse et à la navigation Web 2.0, et notamment à la recatégorisation des résultats issus de la catégorisation du contenu. Un autre rapport surveille également les blocages de page qui résultent de l’analyse des liens.

Important

Pour être sûr que les rapports sur l’activité d’analyse soient significatifs, activez la journalisation des URL complètes (voir *Configuration de la journalisation des URL*, page 413). Sinon, les rapports ne pourront afficher que le domaine (www.domaine.com) du site catégorisé, y compris lorsque les pages individuelles d’un site appartiennent à des catégories différentes ou ont été recatégorisées pour d’autres raisons.

Pour créer un rapport personnalisé, vous pouvez copier un modèle de rapport de sécurité ou d’analyse. Vous pouvez ensuite modifier le filtre du rapport pour ajuster les informations incluses lors de la génération de ce rapport personnalisé.

Certains rapports sur les menaces de sécurité comprennent une colonne **ID de la menace**. Vous pouvez cliquer sur l’identifiant de la menace pour ouvrir une page Web des laboratoires Websense Security Labs décrivant le type de menace identifié.

Les autres rapports de présentation peuvent contenir des informations sur les activités d’analyse et sur les activités du filtrage standard. Par exemple, le rapport Détails des URL complètes par catégorie, situé dans le groupe Activité Internet du Catalogue des rapports,

fournit la liste détaillée de chaque URL consultée dans chaque catégorie. Pour créer un rapport spécifique à l'analyse avancée, copiez le rapport Détails des URL complètes par catégorie et modifiez son filtre. Dans l'onglet Actions, sélectionnez uniquement les actions autorisées et bloquées liées à l'analyse avancée. Dans l'onglet Options, modifiez le nom du catalogue de rapports et le titre du rapport de manière à l'identifier comme rapport d'analyse avancée. Vous pouvez par exemple remplacer le nom et le titre par Analyse avancée : Détails des URL complètes par catégorie.

Les rapports d'investigation permettent également d'obtenir un aperçu des activités de l'analyse avancée.

1. Dans la liste déroulante **Utilisation d'Internet par**, sélectionnez **Action**.
2. Dans le rapport résultant, cliquez sur une action, par exemple sur **Catégorie bloquée en temps réel**, pour afficher la liste des options d'exploration.
3. Cliquez sur l'option d'exploration désirée, par exemple **Catégorie** ou **Utilisateur**.
4. Cliquez sur la valeur **Accès** ou sur la barre de l'une des lignes pour voir les détails associés.
5. Cliquez sur **Modifier le rapport**, en haut de la page, pour ajouter la colonne **URL complète** dans le rapport.

Pour plus d'informations sur l'utilisation des fonctions des rapports d'investigation, consultez la section *Rapports d'investigation*, page 152.

Journalisation de l'analyse

La journalisation de l'activité du filtrage Web standard et de l'analyse avancée présente d'importantes différences.

Dans le cas du filtrage Web standard, plusieurs options permettent de réduire la taille de la base de données d'activité.

- Activez **visites** pour ne journaliser qu'un enregistrement pour chaque site Web demandé. Voir *Configuration de Log Server*, page 400.
- Activez **consolidation** pour combiner dans un seul enregistrement de journal plusieurs requêtes comportant des éléments communs. Voir *Configuration de Log Server*, page 400.
- Désactivez **Enregistrement des URL complètes** pour ne journaliser que le nom de domaine (www.domaine.com) de chaque requête, et non le chemin d'accès conduisant à une page spécifique du domaine (/produits/produitA). Voir *Configuration de la journalisation des URL*, page 413.

> **Remarque**
>
> Si votre organisation doit générer des rapports incluant l'URL complète de chaque site visité, il est préférable de ne pas désactiver la journalisation des URL complètes. Sinon, les rapports ne pourront afficher que le domaine (www.domaine.com) du site catégorisé, y compris lorsque les pages individuelles d'un site appartiennent à des catégories différentes ou ont été recatégorisées pour d'autres raisons.

- Configurez la **Journalisation de catégories spécifiques** de manière à limiter la journalisation aux catégories essentielles pour votre organisation. Voir *Configuration du mode de journalisation des requêtes filtrées*, page 398.

> **Remarque**
> L'activation des **visites**, de la **consolidation** ou de la **journalisation sélective des catégories** affecte la précision du temps de navigation sur Internet.

De leur côté, les fonctions d'analyse avancée ne sont liées que partiellement à ces paramètres. Lorsqu'un site est analysé, deux enregistrements de journal distincts sont créés.

- Les **enregistrements de filtres Web** tirent parti des paramètres de réduction de taille éventuellement implémentés et sont disponibles pour tous les rapports sur le filtrage Web.
- Les **enregistrements d'analyse** ignorent la plupart des paramètres de réduction de taille. Chaque accès distinct est journalisé, les requêtes de toutes les catégories sont journalisées et aucun enregistrement n'est consolidé. Un enregistrement d'analyse est généré, que le site soit bloqué ou autorisé par l'analyse. Seul le paramètre de journalisation des URL complètes est respecté pour les enregistrements de l'analyse avancée.

Si vous avez activé des options de réduction de taille pour la base de données d'activité, il est possible que les chiffres présentés dans les rapports d'analyse ne correspondent **pas** aux chiffres présentés dans les rapports de filtrage standard, même si ces rapports sont configurés pour les mêmes utilisateurs, périodes et catégories. Par exemple, si vous avez choisi de journaliser les visites et qu'un utilisateur demande un site analysé par les fonctions d'analyse, cette requête prend la forme d'une seule visite dans les rapports du filtrage standard, mais peut se traduire par plusieurs accès dans les rapports de l'analyse avancée.

Pour obtenir des données comparables pour le filtrage standard et l'analyse avancée, **désactivez** les paramètres de réduction de taille de la base de données d'activité. Comme il peut en résulter une base de données très volumineuse, assurez-vous que l'ordinateur de la base de données d'activité dispose de suffisamment d'espace disque, de capacité de traitement et de mémoire.

Pour plus d'informations sur la configuration des paramètres de réduction de taille, consultez la section *Administration de la génération de rapports*, page 395. Pour plus d'informations sur la création des rapports, consultez les sections *Rapports de présentation*, page 131, et *Rapports d'investigation*, page 152.

Contournement du décryptage SSL

Lorsque Content Gateway est configuré avec SSL Manager pour gérer le trafic crypté :

- Les paramètres de catégorie permettent de définir les catégories de sites Web pour lesquelles le décryptage et l'examen sont ignorés.
- Il est possible de créer une liste d'adresses IP et de plages d'adresses IP de clients approuvés pour lesquels le décryptage et l'examen sont ignorés.
- Il est également possible de créer une liste de noms d'hôte, d'adresses IP et de plages d'adresses IP définissant les serveurs de destination approuvés pour lesquels le décryptage et l'examen sont ignorés.

Paramètres de catégories

Dans le cas des paramètres de catégorie, un groupe **Privacy Category (Catégories confidentielles)** prédéfini regroupe les catégories susceptibles d’être soumises à des exigences réglementaires.

Les catégories confidentielles par défaut incluent :

- Enseignement
- Services Financiers
- Gouvernement
- Santé
- Courtage en ligne
- Médicaments sur ordonnance

Le trafic lié aux sites Web de ces catégories peut inclure des informations d’identification personnelles qui ne doivent pas être décryptées. Pour éviter d’examiner ce type d’informations, vous pouvez définir un contournement du décryptage pour certaines catégories ou toutes ces catégories. Les utilisateurs peuvent savoir que le site Web consulté n’est pas décrypté en vérifiant que le certificat est bien l’original pour ce site.

Utilisez **Paramètres > Contournement du décryptage SSL** pour sélectionner les catégories confidentielles par défaut contournant le décryptage SSL :

1. Cliquez sur le bouton **Select Privacy Categories (Sélectionner les catégories confidentielles)**. Les cases à cocher des catégories de sites Web constituant le groupe par défaut sont sélectionnées dans la section Category Bypass (Contournement de catégorie).
2. Cliquez sur la flèche située à droite de l’arborescence des catégories pour ajouter des catégories confidentielles dans la section **Categories selected for SSL decryption bypass (Catégories sélectionnées pour le contournement du décryptage SSL)**.

Vous pouvez créer votre propre jeu de catégories contournant le décryptage SSL. Dans la page **Contournement du décryptage SSL**, définissez les catégories individuelles de sites Web pour lesquelles le décryptage n’est pas effectué :

1. Pour sélectionner une catégorie ou une sous-catégorie pour le contournement, cochez sa case.
2. Cliquez sur la flèche située à droite de l’arborescence des catégories pour ajouter la catégorie sélectionnée dans la section **Categories selected for SSL decryption bypass (Catégories sélectionnées pour le contournement du décryptage SSL)**.

Pour annuler vos sélections dans l’arborescence des catégories, cliquez sur le bouton **Effacer tout**.

Pour retirer une catégorie ou une sous-catégorie de la liste, sélectionnez-la, puis cliquez sur le bouton **Supprimer**.

Liste des clients

Pour identifier une adresse IP ou une plage d'adresses IP de clients contournant le décryptage SSL :

1. Cliquez sur **Ajouter**, puis saisissez l'adresse IP ou la plage d'adresses IP des clients dans la section **Add Client Entry (Ajouter une entrée de client)**, une entrée par ligne.

   Lorsque vous définissez une plage d'adresses IP, servez-vous du caractère « - » (tiret) pour séparer la première adresse de la dernière.

   Les adresses IPv6 sont uniquement valides avec le trafic de proxy explicite.
2. Pour simplifier la gestion de la liste, ajoutez une description identifiant votre entrée.
3. Cliquez sur **OK** pour ajouter les entrées dans la liste.

Pour modifier une entrée, cliquez sur l'adresse IP et modifiez l'entrée dans la section **Edit Client Entry (Modifier une entrée de client)**. Cliquez sur **OK** pour enregistrer vos modifications ou sur **Annuler** pour fermer la boîte de dialogue sans les enregistrer.

Pour retirer une entrée de la liste, cochez la case qui lui est accolée, puis cliquez sur **Supprimer**. Confirmez l'opération.

Lorsque vous avez terminé, 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)**.

Liste de destinations

Pour définir un nom d'hôte, une adresse IP ou une plage d'adresses IP de destination contournant le décryptage SSL :

1. Cliquez sur **Ajouter**, puis saisissez le nom d'hôte, l'adresse IP ou la plage d'adresses IP de destination dans la section **Add Destination Entry (Ajouter une entrée de destination)**, une entrée par ligne.
   - Vous pouvez saisir un simple nom d'hôte.

     Par exemple : **cesite.com**.

     Veillez à entrer à la fois le domaine et l'extension (**cesite.com** et **cesite.net** sont des hôtes distincts).
   - Les sites comprenant plusieurs intitulés sont pris en charge.

     Par exemple, **www.bbc.co.uk**.
   - Vous pouvez utiliser le caractère générique « * » pour établir une correspondance avec les premiers sous-domaines uniquement.

     Par exemple : ***.yahoo.com**.

- Vous pouvez saisir une URL ou un nom d’hôte complet ou partiel. Le schéma de début « HTTPS:// » n’est pas nécessaire. Une correspondance exacte est établie avec la chaîne spécifiée.

  Par exemple : **www.exemple.com/media/**

  Ou : **www.youtube.com/watch?v=**
- Servez-vous du caractère « - » (tiret) pour séparer la première adresse de la dernière d’une plage.
- Les adresses IPv6 sont uniquement valides avec le trafic de proxy explicite.

2. Pour simplifier la gestion de la liste, ajoutez une description identifiant clairement votre entrée.
3. Cliquez sur **OK** pour ajouter les entrées dans la liste.

Pour modifier une entrée, cliquez sur le nom d’hôte ou l’adresse IP et modifiez l’entrée dans la boîte de dialogue **Edit Destination Entry (Modifier une entrée de destination)**. Cliquez sur **OK** pour enregistrer vos modifications ou sur **Annuler** pour fermer la boîte de dialogue sans les enregistrer.

Pour retirer une entrée de la liste, cochez la case qui lui est accolée, puis cliquez sur **Supprimer**. Confirmez l’opération.

Lorsque vous avez terminé, 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)**.

10 Configuration du filtrage hybride

Websense Web Security Gateway Anywhere fournit une solution de sécurité Web flexible et exhaustive qui vous permet de combiner les filtrages sur site et hybride (dans le cloud) pour gérer l'activité Internet de votre organisation en fonction de vos besoins. Vous choisissez vous-même quelle méthode utiliser avec tel ou tel client.

Une même organisation peut exploiter une solide solution de sécurité Web sur site pour son siège social ou son campus central, tandis que ses bureaux régionaux ou emplacements satellites, plus petits, envoient leurs requêtes Internet via le service hybride. Le filtrage hybride se révèle également utile pour les utilisateurs non connectés au réseau, par exemple les télétravailleurs, les employés en déplacement professionnel, etc. (voir *Filtrage hybride des utilisateurs hors site*, page 242).

Web Security Gateway Anywhere vous permet de définir les clients et de créer des stratégies pour le filtrage sur site et hybride via la même interface utilisateur (TRITON - Web Security), la configuration, la génération de rapports et la gestion étant centralisées.

Pour utiliser le filtrage hybride :

1. *Activation de votre compte de filtrage hybride*, page 204
2. *Définition des emplacements filtrés*, page 205
3. *Définition des sites non filtrés par le service hybride*, page 211, (le cas échéant)
4. *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214
5. *Identification des utilisateurs du filtrage hybride*, page 311
6. *Envoi de données d'utilisateur et de groupe au service hybride*, page 220

Pour s'assurer que le service hybride dispose des informations de stratégie, d'utilisateur et de groupe les plus récentes et que le logiciel de génération de rapports sur site exploite les données de rapports issues des utilisateurs filtrés par le service hybride, consultez la section *Planification de la communication avec le filtrage hybride*, page 227.

Activation de votre compte de filtrage hybride

Rubriques connexes :

- *Définition des emplacements filtrés*, page 205
- *Définition des sites non filtrés par le service hybride*, page 211
- *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214
- *Envoi de données d'utilisateur et de groupe au service hybride*, page 220
- *Planification de la communication avec le filtrage hybride*, page 227

Avant de pouvoir configurer le service hybride et commencer à filtrer les requêtes Internet pour votre organisation, vous devez activer votre compte hybride en envoyant une adresse électronique de contact. Cette opération crée alors une connexion entre les parties sur site et hybride de Websense Web Security Gateway Anywhere.

Utilisez la section Filtrage hybride de la page **Paramètres > Général > Compte** pour définir l'adresse électronique de contact et le pays des administrateurs de votre filtrage Websense (voir *Configuration des informations de votre compte*, page 24).

L'adresse électronique est généralement un alias surveillé par le groupe chargé de la gestion de votre logiciel Websense. Il est essentiel que le courrier reçu par ce compte soit rapidement examiné et que les mesures nécessaires soient prises aussitôt.

- Le Support technique de Websense utilise cette adresse pour envoyer les notifications relatives aux problèmes urgents qui affectent le filtrage hybride.
- En cas de problème de configuration de votre compte, le fait de ne pas répondre en temps voulu au message du support technique peut entraîner une interruption du service.
- En cas de certains problèmes peu fréquents, cette adresse électronique est utilisée pour envoyer les informations nécessaires afin que le service de synchronisation reprenne contact avec le service hybride.
- Cette adresse électronique n'est **pas** utilisée pour envoyer des communications à caractère marketing, commercial, général ou autre.

Le pays que vous indiquez définit le fuseau horaire pour le système.

Après avoir activé le filtrage hybride pour votre compte, vous pouvez définir les emplacements (identifiés par adresse IP, plage d'adresses IP ou sous-réseau) que le service hybride doit filtrer, le mode d'échange des informations entre les parties sur site et hybride de votre logiciel Web Security, le mode d'authentification des utilisateurs filtrés par le service hybride, etc.

Définition des emplacements filtrés

Rubriques connexes :

- *Définition des sites non filtrés par le service hybride*, page 211
- *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214
- *Planification de la communication avec le filtrage hybride*, page 227

La page **Paramètres > Hybrid Configuration (Configuration hybride) > Filtered Locations (Emplacements filtrés)** vous permet de vérifier, d'ajouter et de modifier les informations relatives aux emplacements dont les utilisateurs peuvent être filtrés par le service hybride.

Un **emplacement filtré** est une adresse IP, une plage d'adresses IP ou un sous-réseau d'où semblent provenir les navigateurs qui se connectent au filtrage Web. Dans les déploiements Web Security Gateway Anywhere, le filtrage hybride peut s'appliquer aux utilisateurs hors site, quel que soit le mode de filtrage dont ils font l'objet lorsqu'ils sont connectés au réseau.

- Pour les utilisateurs filtrés par le filtrage hybride au sein et à l'extérieur du réseau, saisissez les détails de leur emplacement au sein du réseau en précisant que cet emplacement est filtré par le service hybride. Lorsqu'ils envoient une requête Internet, les utilisateurs hors site sont invités à se connecter au filtrage hybride de sorte que la stratégie d'utilisateur ou de groupe appropriée puisse être appliquée.

  Le service hybride étant hébergé à l'extérieur de votre réseau, tous les emplacements qu'il filtre doivent être des adresses externes, visibles depuis Internet. Les emplacements filtrés par le service hybride :

  - Sont les adresses IP publiques des bureaux filtrés par Web Security Gateway Anywhere
  - Correspondent généralement à l'adresse externe de votre pare-feu NAT (Network Address Translation)
  - Peuvent inclure des filiales, des sites distants ou des campus affiliés

  Ces emplacements ne sont PAS :

  - Des adresses IP d'ordinateurs clients individuels
  - L'adresse IP d'un ordinateur Content Gateway utilisé par les composants sur site de Websense Web Security Gateway Anywhere
- Pour les utilisateurs filtrés par les composants sur site (Filtering Service) lorsqu'ils sont à l'intérieur du réseau, vous pouvez configurer le fichier PAC du navigateur de sorte qu'il détermine si l'utilisateur est au sein du réseau ou hors site avant d'envoyer une demande Internet au filtrage.

  Si vous utilisez le fichier PAC généré par le service hybride, cette configuration intervient automatiquement conformément aux paramètres définis dans la page Filtered Locations (Emplacements filtrés). Indiquez si ces utilisateurs sont filtrés par le logiciel Websense local et si leur filtrage sur site est effectué par un proxy transparent ou intégré au pare-feu (par exemple, Content Gateway en mode transparent) ou par un proxy explicite. Lorsque des requêtes Internet issues d'ordinateurs réseau situés dans un emplacement défini passent par un proxy explicite, vous devez fournir l'emplacement (nom d'hôte ou adresse IP) et le port du proxy pour garantir que les requêtes des utilisateurs de cet emplacement soient correctement acheminées.

Chaque emplacement que vous définissez apparaît dans un tableau qui présente le nom et la description, ainsi que des détails de configuration techniques, notamment le mode du proxy sélectionné, le type d'emplacement (adresse IP unique, plage d'adresses IP ou sous-réseau) et la ou les véritables adresses IP externes d'où proviennent les demandes.

Pour modifier une entrée existante, cliquez sur le **Nom** de l'emplacement, puis consultez la section *Modification des emplacements filtrés*, page 208.

Pour définir un nouvel emplacement, cliquez sur **Ajouter**, puis consultez la section *Ajout d'emplacements filtrés*, page 206.

Pour supprimer un emplacement, cochez la case accolée à son nom, puis cliquez sur **Supprimer**.

Pour ajouter et modifier les proxy explicites sur site à utiliser pour les emplacements filtrés, cliquez sur **Manage Explicit Proxies (Gérer les proxy explicites)**, puis consultez la section *Gestion des proxy explicites*, page 209.

Si vous avez ajouté ou modifié l'entrée d'un emplacement, 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)**.

Ajout d'emplacements filtrés

La page **Filtered Locations (Emplacements filtrés)** > **Add Filtered Location (Ajouter un emplacement filtré)** vous permet de définir un emplacement filtré par le service hybride (par exemple une filiale, un site distant ou un campus affilié) ou qui contient des utilisateurs filtrés par le service hybride lorsqu'ils ne sont pas sur site.

1. Entrez un **Nom** d'emplacement unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.

2. Entrez une brève **Description** de l'emplacement (jusqu'à 255 caractères). Cette description s'affiche à côté du nom de l'emplacement dans la page Filtered Locations (Emplacements filtrés) et doit permettre à n'importe quel administrateur d'identifier clairement cet emplacement.

   Les restrictions de caractères qui s'appliquent aux noms s'appliquent également aux descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).

3. Si vous ajoutez un emplacement filtré par le service hybride, sélectionnez le **Fuseau horaire** de cet emplacement. Les informations de fuseau horaire sont utilisées pour l'application des stratégies et garantissent l'application appropriée et au bon moment des filtres adéquats.

   Chaque emplacement filtré par le service hybride peut utiliser des paramètres de fuseau horaire distincts. Les emplacements filtrés via des proxy transparents ou explicites utilisent le fuseau horaire de l'ordinateur dans lequel s'exécute Filtering Service pour imposer les stratégies.

4. Dans le champ **Type**, indiquez comment cet emplacement doit être défini : sous forme d'**Adresse IP**, de **Plage d'adresses IP** ou de **Sous-réseau**.

   Si vous optez pour un sous-réseau, indiquez si ce dernier est identifié par plage de bits (**By bit range (CIDR)**) ou par **Masque de sous réseau**, puis sélectionnez la plage de bits ou le masque.

5. Entrez l'adresse IP externe, la plage ou le sous-réseau du ou des pare-feu par lesquels les clients filtrés à cet emplacement accèdent à Internet.
   - Dans le cas des emplacements filtrés par le service hybride, il s'agit des adresses IP externes, visibles depuis l'extérieur de votre réseau, et non des adresses internes (LAN).

     Important

     N'entrez pas d'adresses IP privées (plages 10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.31.255.255 et 192.168.0.0 à 192.168.255.255) pour identifier les emplacements filtrés par le service hybride. Ces adresses n'étant pas visibles à l'extérieur de votre réseau et étant utilisées dans de nombreux réseaux locaux, le service hybride ne considère pas les adresses IP privées comme des entrées valides.

     Si le mode du proxy de cet emplacement est Transparent ou Explicite, vous pouvez saisir des adresses IP privées.

   - N'incluez pas l'adresse IP d'un ordinateur Content Gateway utilisé par les composants sur site de Websense Web Security Gateway Anywhere.
   - Les adresses IP externes doivent être uniques dans votre organisation et ne pas être partagées avec une autre entité afin que le service hybride puisse associer les requêtes provenant de ces emplacements aux stratégies appartenant à votre organisation.
6. Définissez le mode de filtrage de l'emplacement : via le service hybride ou par le logiciel Websense local.
7. Si le site est filtré par le logiciel Websense local, sélectionnez le mode du proxy de cet emplacement : via un proxy **Transparent** ou un proxy **Explicite** sur site.

   Si vous sélectionnez Explicite, un proxy au moins doit être défini dans le tableau de configuration des proxy explicites. Pour ajouter un nouveau proxy explicite au tableau, cliquez sur **Ajouter**, sélectionnez un emplacement de proxy et un ordre favori dans la fenêtre contextuelle, puis cliquez sur **OK**. Pour plus d'informations sur les proxy explicites disponibles, consultez la section *Gestion des proxy explicites*, page 209.

   L'emplacement filtré utilise le premier proxy de la liste. Si ce proxy n'est pas disponible, les demandes de filtrage Web provenant de l'emplacement filtré sont redirigées vers le prochain proxy de la liste. Pour modifier l'ordre, sélectionnez l'un des proxy dans la liste, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier sa position.

   Pour retirer un proxy du tableau, cochez la case accolée à son nom, puis cliquez sur **Supprimer**. Le proxy supprimé n'est alors plus disponible pour cet emplacement filtré mais peut encore être sélectionné pour d'autres emplacements filtrés.
8. Cliquez sur **OK** pour revenir à la page Filtered Locations (Emplacements filtrés), 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)**.

Modification des emplacements filtrés

La page **Filtered Locations (Emplacements filtrés) > Edit Filtered Locations (Modifier les emplacements filtrés)** vous permet de modifier la définition du mode de filtrage d'un emplacement par le service hybride.

1. Si vous modifiez le **Nom** de l'emplacement, assurez-vous que ce nom soit unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez ou actualisez la **Description** de l'emplacement.

   Les restrictions de caractères qui s'appliquent aux noms s'appliquent également aux descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).
3. Vérifiez le **Fuseau horaire** de cet emplacement pour être certain que les stratégies soient correctement imposées.
4. Vérifiez la méthode utilisée pour définir cet emplacement : par **Adresse IP**, **Plage d'adresses IP** ou **Sous-réseau**.

   Si vous saisissez ou modifiez un sous-réseau, indiquez si ce dernier est identifié par plage de bits (**By bit range (CIDR)**) ou par **Masque de sous réseau**, puis sélectionnez la plage de bits ou le masque.
5. Actualisez l'adresse IP externe, la plage ou le sous-réseau du ou des pare-feu par lesquels les clients filtrés dans cet emplacement accèdent à Internet.
   - Dans le cas des emplacements filtrés par le service hybride, il s'agit des adresses IP externes, visibles depuis l'extérieur de votre réseau, et non des adresses internes (LAN).

     Important

     N'entrez pas d'adresses IP privées (plages 10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.31.255.255 et 192.168.0.0 à 192.168.255.255) pour identifier les emplacements filtrés par le service hybride. Ces adresses n'étant pas visibles à l'extérieur de votre réseau et étant utilisées dans de nombreux réseaux locaux, le service hybride ne considère pas les adresses IP privées comme des entrées valides.

     Si le mode du proxy de cet emplacement est Transparent ou Explicite, vous pouvez saisir des adresses IP privées.

   - Ces adresses ne doivent jamais inclure l'adresse IP de l'ordinateur Content Gateway. Content Gateway est uniquement utilisé par la partie sur site de votre logiciel Websense.
   - Les adresses IP externes doivent être uniques dans votre organisation et ne pas être partagées avec une autre entité afin que le service hybride puisse associer les requêtes provenant de ces emplacements aux stratégies appartenant à votre organisation.

Lorsqu'un emplacement filtré est déjà associé à une organisation et qu'une seconde organisation définit cette même adresse IP en tant qu'emplacement filtré, le filtrage hybride peut être interrompu temporairement pour la seconde d'organisation jusqu'à ce que le conflit soit résolu.

6. Vérifiez le mode de filtrage de l'emplacement : via le service hybride ou par le logiciel Websense local.
7. Si le site est filtré par le logiciel Websense local, sélectionnez le mode du proxy de cet emplacement : via un proxy **Transparent** ou un proxy **Explicite** sur site.

   Si vous sélectionnez Explicite, l'emplacement filtré utilise le premier proxy de la liste définie dans le tableau de configuration des proxy explicites. Si ce proxy n'est pas disponible, les demandes de filtrage Web provenant de l'emplacement filtré sont redirigées vers le prochain proxy de la liste. Pour modifier l'ordre de préférence, sélectionnez l'un des proxy dans la liste, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier sa position.

   Pour afficher les détails d'une entrée de tableau existante, cliquez sur le **Nom** du proxy.

   Pour ajouter un nouveau proxy explicite au tableau, cliquez sur **Ajouter**, sélectionnez un emplacement de proxy et un ordre favori dans la fenêtre contextuelle, puis cliquez sur **OK**. Pour plus d'informations sur les proxy explicites disponibles, consultez la section *Gestion des proxy explicites*, page 209.

   Pour retirer un proxy du tableau, cochez la case accolée à son nom, puis cliquez sur **Supprimer**. Le proxy supprimé n'est alors plus disponible pour cet emplacement filtré mais peut encore être sélectionné pour d'autres emplacements filtrés.
8. Cliquez sur **OK** pour revenir à la page Filtered Locations (Emplacements filtrés), 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)**.

Gestion des proxy explicites

Rubriques connexes :

- *Ajout d'un proxy explicite*, page 210
- *Modification d'un proxy explicite*, page 210

La page **Filtered Locations (Emplacements filtrés) > Manage Explicit Proxies (Gérer les proxy explicites)** vous permet de vérifier, d'ajouter et de modifier les proxy explicites sur site utilisables avec les emplacements filtrés.

Chaque proxy explicite que vous définissez apparaît dans un tableau qui présente son nom, son adresse IP ou son nom d'hôte, le ou les numéros des ports utilisés pour l'accès HTTP, SSL ou FTP, et les emplacements filtrés (le cas échéant) faisant actuellement référence au proxy.

Pour modifier une entrée existante, cliquez sur le **Nom** du proxy, puis consultez la section *Modification d'un proxy explicite*, page 210.

Pour définir un nouveau proxy explicite, cliquez sur **Ajouter**, puis consultez la section *Ajout d'un proxy explicite*, page 210.

Pour retirer un proxy, cochez la case accolée à son nom, puis cliquez sur **Supprimer**.

> **Remarque**
>
> Vous ne pouvez pas supprimer un proxy qui est actuellement utilisé par un ou plusieurs emplacements filtrés. Pour supprimer un tel proxy, commencez par modifier chaque emplacement filtré en retirant ce proxy dans le tableau de configuration des proxy explicites.

Ajout d'un proxy explicite

Lorsque vous gérez les proxy explicites, utilisez la page **Add Explicit Proxy (Ajouter un proxy explicite)** pour définir le proxy explicite local à utiliser pour vos emplacements filtrés.

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

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.
2. Saisissez l'**adresse IP ou le nom** du proxy explicite. Il doit s'agir de l'un des éléments suivants :
   - Une adresse IP (par exemple 123.45.67.89)
   - Un nom d'hôte (par exemple, mon.exemple.com)

   L'adresse IP ou le nom peut inclure un numéro de port, par exemple 123.45.67.89:443.
3. Saisissez au moins un numéro de port pour le proxy. Il peut s'agir d'un **port HTTP**, d'un **port SSL** ou d'un **port FTP**.
4. Cliquez sur **OK** pour revenir à la page Manage Explicit Proxies (Gérer les proxy explicites).

Modification d'un proxy explicite

Lorsque vous gérez les proxy explicites, utilisez la page **Edit Explicit Proxy (Modifier un proxy explicite)** pour modifier les détails d'un proxy explicite local déjà configuré.

1. Si vous modifiez le **Nom** du proxy, assurez-vous que ce nom soit unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.
2. Vérifiez ou actualisez l'**adresse IP ou le nom** du proxy explicite. Il doit s'agir de l'un des éléments suivants :
   - Une adresse IP (par exemple 123.45.67.89)
   - Un nom d'hôte (par exemple, mon.exemple.com)

   L'adresse IP ou le nom peut inclure un numéro de port, par exemple 123.45.67.89:443.
3. Si vous modifiez le port du proxy, saisissez au moins un numéro de port. Il peut s'agir d'un **port HTTP**, d'un **port SSL** ou d'un **port FTP**.
4. Cliquez sur **OK** pour revenir à la page Manage Explicit Proxies (Gérer les proxy explicites).

Configuration du basculement vers le service hybride

Pour les emplacements filtrés qui utilisent des proxy explicites, vous pouvez configurer le basculement vers le service hybride. 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.

Pour configurer le basculement vers le service hybride :

1. Dans la page **Hybrid Configuration (Configuration hybride) > Filtered Locations (Emplacements filtrés)**, sélectionnez le nom de l'emplacement filtré à modifier. Il doit s'agir d'un emplacement filtré par votre logiciel Websense local dont le mode de proxy est défini sur Explicite.
2. Cliquez sur **Avancé**.
3. Cochez la case **Enable failover to hybrid service (Activer le basculement vers le service hybride)**.
4. Entrez le **Nombre d'utilisateurs filtrés par cet emplacement filtré**.
5. Sélectionnez le **Centre de données le plus proche** de l'emplacement filtré.
6. Cliquez sur **OK** pour revenir à la page Filtered Locations (Emplacements filtrés), 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)**.

Lorsque le basculement d'un emplacement filtré est approuvé, une alerte s'affiche dans le tableau de bord Système et dans la page État > Alertes. Vous pouvez consulter l'état d'approbation de toutes les demandes de basculement dans la page État > Service hybride.

> **Remarque**
>
> Si la mise en cache automatique du proxy est désactivée dans Internet Explorer, les utilisateurs peuvent remarquer un certain retard dans l'affichage de chaque page consultée tandis que le navigateur vérifie la liste des proxy. Lorsque la mise en cache automatique du proxy est activée, le navigateur vérifie la liste des proxy uniquement au démarrage. Pour plus d'informations, consultez l'article de Microsoft, disponible à l'adresse http://support.microsoft.com/kb/271361.

Définition des sites non filtrés par le service hybride

Rubriques connexes :

- *Définition des emplacements filtrés*, page 205
- *Envoi de données d'utilisateur et de groupe au service hybride*, page 220
- *Planification de la communication avec le filtrage hybride*, page 227

La page **Paramètres > Hybrid Configuration (Configuration hybride) > Unfiltered Destinations (Destinations non filtrées)** vous permet de vérifier, ajouter ou modifier les informations relatives aux sites visés pour lesquels l'accès des clients ne doit pas être filtré. Les clients peuvent accéder à ces sites directement, sans envoyer leurs demandes au service hybride ni au proxy explicite local d'un emplacement filtré, lorsqu'un tel proxy est utilisé. En général, les destinations non filtrées incluent les sites de messagerie Web des organisations, les adresses IP internes et les sites de mise à jour Microsoft.

Conseil

En tant que pratique recommandée, ajoutez l'adresse de messagerie Web de votre organisation en tant que destination non filtrée. Vous serez ainsi certain :

- De pouvoir accéder aux messages envoyés par le Support technique lorsque des problèmes entraînent le blocage de toutes les requêtes par votre proxy ou le service hybride
- Que les utilisateurs hors site qui ont oublié (ou qui n'ont pas créé) leur mot de passe de filtrage hybride peuvent le récupérer par courrier électronique

Les destinations répertoriées ici sont ajoutées dans le fichier PAC (Proxy Auto-Configuration) qui définit le mode de connexion des navigateurs des utilisateurs filtrés au service hybride (voir *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214). Par défaut, le fichier PAC exclut toutes les plages d'adresses IP non routables et de multidiffusion du filtrage. Par conséquent, si vous utilisez des plages d'adresses IP privées définies selon les normes RFC 1918 ou RFC 3330, vous n'avez pas besoin de les saisir.

Chaque destination non filtrée que vous définissez apparaît dans un tableau qui présente son nom et sa description, ainsi que des détails de configuration techniques, notamment le mode de définition de la destination (adresse IP, domaine ou sous-réseau), et la véritable adresse IP ou le vrai domaine ou sous-réseau auquel les utilisateurs peuvent accéder directement.

Pour modifier une entrée existante, cliquez sur le **Nom** de l'emplacement, puis consultez la section *Modification des destinations non filtrées*, page 213.

Pour définir un nouvel emplacement, cliquez sur **Ajouter**, puis consultez la section *Ajout de destinations non filtrées*, page 212.

Pour retirer une destination non filtrée, cochez la case accolée à son nom, puis cliquez sur **Supprimer**.

Si vous avez ajouté ou modifié l'entrée d'une destination non filtrée, 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)**.

Ajout de destinations non filtrées

La page **Unfiltered Destinations (Destinations non filtrées) > Add Unfiltered Destination (Ajouter une destination non filtrée)** vous permet de définir un site ou un groupe de sites auquel les utilisateurs peuvent accéder directement, sans envoyer leurs demandes au service hybride ni au proxy explicite local.

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

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez une brève **Description** de la destination. Cette description s'affiche à côté du nom de la destination non filtrée dans la page Unfiltered Destinations (Destinations non filtrées) et doit permettre à tout administrateur d'identifier clairement le ou les sites non filtrés visés.

   Les restrictions de caractères qui s'appliquent aux noms s'appliquent également aux descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).
3. Dans le champ **Type**, indiquez comment cette destination doit être définie : en tant qu'**Adresse IP**, **Domaine** ou **Sous-réseau**.

   Si vous optez pour un sous-réseau, indiquez si ce dernier est identifié par plage de bits (**By bit range (CIDR)**) ou par **Masque de sous réseau**, puis sélectionnez la plage de bits ou le masque.
4. Entrez l'adresse IP, le domaine ou le sous-réseau auquel vos utilisateurs doivent pouvoir accéder sans envoyer leurs demandes au service hybride ni au proxy explicite local.
5. Sélectionnez le type de **Proxy** auquel s'applique cette destination non filtrée.
   - Sélectionnez **Hybride** pour autoriser tous les utilisateurs du filtrage hybride à accéder directement à la destination sans envoyer de requête au service hybride.
   - Sélectionnez **Explicite** pour autoriser tous les utilisateurs des emplacements filtrés qui utilisent un proxy explicite local à accéder directement à cette destination.
   - Sélectionnez **Hybride et Explicite** pour que tous les utilisateurs filtrés par le service hybride et un proxy explicite local d'emplacement filtré puissent accéder directement à cette destination.
6. Cliquez sur **OK** pour revenir à la page Unfiltered Destinations (Destinations non filtrées), 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)**.

Modification des destinations non filtrées

La page **Unfiltered Destinations (Destinations non filtrées) > Edit Unfiltered Destination (Modifier une destination non filtrée)** vous permet de modifier la définition d'un site ou d'un groupe de sites existant auquel les utilisateurs peuvent accéder directement, sans envoyer de requête au service hybride.

1. Si vous modifiez le **Nom** de la destination, assurez-vous que ce nom soit unique. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez ou actualisez la **Description** de la destination.

   Les restrictions de caractères qui s'appliquent aux noms s'appliquent également aux descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).

3. Vérifiez la méthode utilisée pour définir cette destination : **Adresse IP**, **Domaine** ou **Sous-réseau**.

   Si vous saisissez ou modifiez un sous-réseau, indiquez si ce dernier est identifié par une plage de bits (**By bit range (CIDR)**) ou par un **Masque de sous réseau**, puis sélectionnez la plage de bits ou le masque.
4. Actualisez l'adresse IP, le domaine ou le sous-réseau auquel vos utilisateurs doivent pouvoir accéder sans envoyer de demande au service hybride.
5. Actualisez le type de **Proxy** auquel s'applique cette destination non filtrée.
   - Sélectionnez **Hybride** pour autoriser tous les utilisateurs du filtrage hybride à accéder directement à la destination sans envoyer de requête au service hybride.
   - Sélectionnez **Explicite** pour autoriser tous les utilisateurs des emplacements filtrés qui utilisent un proxy explicite local à accéder directement à cette destination.
   - Sélectionnez **Hybride et Explicite** pour que tous les utilisateurs filtrés par le service hybride et un proxy explicite local d'emplacement filtré puissent accéder directement à cette destination.
6. Cliquez sur **OK** pour revenir à la page Unfiltered Destinations (Destinations non filtrées), 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)**.

Configuration de l'accès des utilisateurs au filtrage hybride

Pour exploiter le filtrage hybride, vous devez indiquer comment vos utilisateurs se connectent au service hybride et sont filtrés par ce dernier. Pour ce faire, sélectionnez **Paramètres > Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)**.

La section **Proxy Auto-Configuration (PAC) File (Fichier PAC)** présente l'URL à partir de laquelle les navigateurs des ordinateurs des utilisateurs filtrés récupèrent le fichier PAC (voir *Qu'est-ce qu'un fichier PAC ?*, page 219).

Le fichier PAC définit les requêtes que le navigateur doit envoyer au service hybride et les requêtes envoyées directement au site visé (voir *Définition des sites non filtrés par le service hybride*, page 211). Le fichier PAC contient également des informations sur les emplacements filtrés et sur la configuration du proxy des éventuels emplacements qui filtrent leurs utilisateurs par proxy explicite ou transparent lorsque les utilisateurs sont sur site, de sorte que le trafic puisse être acheminé correctement vers tous les emplacements.

Remarque

Le mécanisme précis de configuration du navigateur d'un utilisateur pour le fichier PAC dépend du navigateur et de votre environnement réseau. Par exemple, si vous utilisez Microsoft Active Directory et Internet Explorer ou Mozilla Firefox, vous pouvez automatiser ce processus grâce à des stratégies de groupe.

Le fichier PAC par défaut est récupéré via le port 8082. Si les utilisateurs demandent ce fichier PAC à partir d'un emplacement dont le port 8082 est verrouillé, ils ne peuvent pas y

accéder. Dans ce cas, utilisez la deuxième adresse du fichier PAC indiquée dans cette section, qui permet à l'utilisateur d'accéder au fichier PAC et au service hybride par le port 80. Les utilisateurs distants doivent également utiliser l'adresse du fichier PAC pour le port 80 lorsqu'ils demandent un accès à partir d'un réseau dont le port 8081 est verrouillé. Même lorsqu'ils peuvent accéder au fichier PAC via le port 8082, le port 8081 demeure le port standard requis pour que le filtrage hybride puisse être utilisé.

> **Remarque**
>
> Les fichiers PAC des versions précédentes de Web Security Gateway Anywhere utilisaient une autre URL que celle affichée dans la page User Access (Accès utilisateur). Si vous avez déployé un fichier PAC pour une version précédente, il n'est pas nécessaire de modifier l'URL, sauf si vous le souhaitez. Les URL des fichiers PAC fournies dans les versions précédentes de Web Security Gateway Anywhere fonctionnent toujours.

La section **Disponibilité** vous permet d'indiquer si l'ensemble des requêtes Internet doivent être autorisées ou bloquées lorsque le service hybride ne peut pas accéder aux informations des stratégies de votre organisation.

Sous **Fuseau horaire**, utilisez la liste déroulante pour sélectionner le fuseau horaire à utiliser par défaut lors de l'application des stratégies dans les cas suivants :

- Pour les utilisateurs qui se connectent au service hybride à partir d'une adresse IP qui ne fait pas partie d'un emplacement filtré existant (voir *Définition des emplacements filtrés*, page 205)

  Le fuseau horaire par défaut est par exemple utilisé par les utilisateurs hors site ou pour les autres utilisateurs qui s'auto-enregistrent auprès du service hybride.
- Dès que les informations du fuseau horaire ne sont pas disponibles pour un emplacement filtré

Utilisez la section **Custom End User Block Page (Page de blocage personnalisée pour les utilisateurs)** pour définir le logo et le texte personnalisés des pages de blocage affichées par le service hybride (voir *Personnalisation des pages de blocage du service hybride*, page 217).

Servez-vous de la section **Pages de notification HTTPS** pour que les utilisateurs qui envoient des demandes HTTPS puissent afficher les pages de notification Websense appropriées (voir *Activation des pages de notification HTTPS*, page 218).

Si le filtrage hybride identifie les utilisateurs via les données d'annuaire collectées par Websense Directory Agent, vous pouvez configurer les mots de passe du filtrage hybride des comptes des utilisateurs dans la page **Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées)** de TRITON - Web Security (voir *Envoi de données d'utilisateur et de groupe au service hybride*, page 220). Si votre organisation n'utilise pas les données d'annuaire collectées par Directory Agent pour identifier les utilisateurs qui se connectent au service hybride à partir d'emplacements filtrés extérieurs, vous pouvez laisser les utilisateurs **s'auto-enregistrer** auprès du service. Les utilisateurs dont les comptes de messagerie sont associés aux domaines que vous spécifiez dans la section **Registered Domains (Domaines enregistrés)** pourront ainsi s'identifier eux-mêmes auprès du service hybride.

Les utilisateurs qui demandent un accès Internet à partir d'une adresse IP non reconnue sont invités à s'auto-enregistrer. La partie domaine de l'adresse électronique de l'utilisateur sert à associer cet utilisateur à votre organisation, de sorte que la stratégie Par défaut appropriée soit appliquée.

Les utilisateurs qui ne peuvent pas être associés à une organisation sont filtrés par la stratégie Par défaut du service hybride.

- Cliquez sur **Ajouter** pour ajouter un domaine (voir *Ajout de domaines*, page 216).
- Cliquez sur l'entrée d'un domaine pour modifier ce domaine ou ses attributs (voir *Modification des domaines*, page 216).

Vous pouvez également appliquer le filtrage hybride aux utilisateurs hors site qui se connectent à partir d'adresses IP inconnues, quel que soit le mode de filtrage appliqué à ces utilisateurs lorsqu'ils sont connectés au réseau ou lorsqu'ils se connectent à partir d'un emplacement filtré. Sous Off-site Users (Utilisateurs hors site), cochez la case **Enable hybrid filtering of off-site users (Activer le filtrage hybride des utilisateurs hors site)**.

Si vous désactivez cette case à cocher, les utilisateurs qui se connectent à partir d'une adresse IP inconnue ne sont pas filtrés.

Pour plus d'informations, consultez la section *Filtrage hybride des utilisateurs hors site*, page 242.

Ajout de domaines

La page **User Access (Accès utilisateur) > Add Domain (Ajouter un domaine)** vous permet d'identifier les domaines et les sous-domaines (le cas échéant) appartenant à votre organisation. Les utilisateurs dont les adresses électroniques correspondent aux domaines spécifiés peuvent ainsi s'auto-enregistrer (s'authentifier eux-mêmes) auprès du filtrage hybride. Cette option n'est généralement utilisée que dans les organisations qui n'envoient pas les informations des utilisateurs au filtrage hybride via Directory Agent.

Le service hybride ne peut pas fournir les informations des noms des utilisateurs qui s'auto-enregistrent auprès des composants sur site pour les exploiter dans des rapports. Seule l'adresse IP d'où provient la demande est journalisée.

1. Entrez un nom de **Domaine** appartenant à votre organisation (au format **domaineexemple.org**).
2. Saisissez une **Description** claire du domaine pour simplifier l'administration du filtrage hybride.
3. Pour que les utilisateurs dont les adresses électroniques correspondent au domaine et à ses sous-domaines (par exemple **universite.edu** et **scienceshumaines.universite.edu**) puissent s'auto-enregistrer, cochez la case **Include subdomains (Inclure les sous-domaines)**.
4. Cliquez sur **OK** pour revenir à la page User Access (Accès utilisateur).
5. 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)**.

Modification des domaines

La page **User Access (Accès utilisateur) > Edit Domain (Modifier le domaine)** vous permet de modifier les entrées de domaine qui permettent aux utilisateurs de s'auto-enregistrer auprès du filtrage hybride.

1. Vérifiez le **Nom** du domaine et apportez éventuellement les modifications nécessaires.
2. Au besoin, actualisez sa **Description**.
3. Pour que les adresses électroniques des sous-domaines soient ou non considérées comme valides, activez ou désactivez la case à cocher **Include subdomains (Inclure les sous-domaines)**.
4. Cliquez sur **OK** pour revenir à la page User Access (Accès utilisateur).

5. 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)**.

Personnalisation des pages de blocage du service hybride

Lorsque le service hybride refuse l'accès à une ressource, il envoie une page de blocage par défaut. Vous pouvez utiliser cette page par défaut ou modifier son texte en fonction de vos besoins. Vous pouvez par exemple :

- Ajouter des informations sur les stratégies d'utilisation d'Internet dans votre organisation
- Fournir un moyen de contacter les Ressources humaines ou un administrateur Websense à propos des stratégies d'utilisation Internet
- Ajouter le logo de votre organisation

Personnalisation du logo

Pour personnaliser le logo qui apparaît sur la page de blocage du filtrage hybride, créez un répertoire nommé **logo** dans le répertoire **ssdata** de Websense (par défaut, \Program Files\Websense\Web Security\bin\ssdata\ sous Windows ou /opt/websense/bin/ssdata/ sous Linux). Placez ensuite le fichier de votre logo dans ce répertoire.

Le logo doit être un fichier JPEG, GIF ou PNG. Lorsque le répertoire **logo** contient un fichier présentant l'une de ces extensions, le service de synchronisation (Sync Service) le détecte et envoie les données au service hybride. Pour que le service de synchronisation puisse envoyer le fichier, la taille de ce dernier doit être supérieure à 0 Ko et ne pas dépasser 50 Ko. Sync Service détecte également la présence d'une version plus récente du fichier et actualise la version utilisée par le service hybride. Lorsque ce répertoire comprend plusieurs fichiers valides, Sync Service utilise le fichier le plus récent.

La page **Hybrid Service (Service hybride)** indique la date et l'heure auxquelles Sync Service a envoyé le logo de la page de blocage personnalisée au service hybride (voir *Surveillance de la communication avec le service hybride*, page 233).

Lorsque vous ne souhaitez plus utiliser un fichier de logo personnalisé, supprimez celui-ci dans le répertoire **logo**.

> **Remarque**
>
> La désactivation de l'option **Use a custom block page title and message (Utiliser un titre et un message de page de blocage personnalisée)** dans la page **Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)** n'entraîne pas automatiquement le retrait du logo personnalisé dans vos pages de blocage. Pour que Sync Service n'envoie plus ce fichier au service hybride, vous devez le supprimer dans le répertoire logo.

Personnalisation du texte

1. Dans la page **Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)** , cochez la case **Use a custom block page title and message (Utiliser un titre et un message de page de blocage personnalisée)**.
2. Saisissez le **Titre** et le **Message** de la page. Ces informations doivent être en texte brut et ne doivent pas contenir de balises HTML.

3. 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)**.

Activation des pages de notification HTTPS

SSL (Secure Sockets Layer) est la norme de l'industrie en matière de transmission sécurisée de données via Internet. Cette norme repose sur un système de certificats approuvés, publiés par des autorités de certification et reconnus par les serveurs.

Si vous installez le certificat SSL Websense pour le filtrage hybride, le proxy hybride peut établir de nouveaux canaux SSL auprès des navigateurs les plus récents (Internet Explorer 8 et Firefox 3.5 ou versions ultérieures) pour envoyer les pages de notification à l'utilisateur (par exemple, une page de blocage lorsque le site SSL appartient à une catégorie exigeant une notification, ou la page appropriée lorsque l'authentification est requise).

Pour préserver les performances, seul le trafic HTTPS est détourné de cette manière ; le trafic HTTP passe par le proxy pour atteindre le site demandé.

Pour garantir que les utilisateurs du filtrage hybride puissent voir les pages de notification lors d'une navigation via HTTPS, un certificat racine doit être installé dans chaque ordinateur client et jouer le rôle d'autorité de certification des requêtes SSL envoyées au proxy hybride.

> **Remarque**
>
> Les utilisateurs finaux qui exploitent Websense Authentication Service ont besoin de ce certificat racine pour que leur authentification transparente auprès des sites HTTPS soit garantie. Lorsque le certificat n'est pas installé pour les utilisateurs du service d'authentification, ces derniers doivent s'authentifier manuellement ou via l'identification NTLM, en fonction des paramètres définis dans la page Hybrid User Identification (Identification des utilisateurs du service hybride). Voir *Déploiement de Websense Authentication Service*, page 317.

Pour installer le certificat racine hybride dans tous les clients utilisant le filtrage hybride :

1. Dans la page **Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)**, cliquez sur **View Hybrid SSL Certificate (Afficher le certificat SSL hybride)**.
2. Enregistrez le fichier du certificat dans l'emplacement de votre choix.
3. Utilisez votre méthode d'administration ou de déploiement favorite (par exemple un Objet de stratégie de groupe Microsoft (GPO) ou un outil de déploiement tiers) pour déployer le certificat SSL auprès de vos utilisateurs du filtrage hybride.

Une fois le certificat distribué, cochez l'option **Use the hybrid SSL certificate to display a notification page for HTTPS requests when required (Utiliser le certificat SSL hybride afin d'afficher une page de notification pour les requêtes HTTPS si nécessaire)**, puis 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)**.

Qu’est-ce qu’un fichier PAC ?

Un fichier PAC (Proxy Auto-Configuration) est une définition de fonction JavaScript appelée par le navigateur pour déterminer le mode de gestion des requêtes. Le fichier PAC utilisé pour activer le filtrage hybride contient un certain nombre de paramètres globaux et vous permet de configurer les sites (par exemple, des sites intranet ou la messagerie Web de l’organisation) auxquels les utilisateurs peuvent accéder directement sans envoyer de demande au service hybride (voir *Définition des sites non filtrés par le service hybride*, page 211).

Pour utiliser le filtrage hybride dans les ordinateurs client, vous devez configurer les paramètres du navigateur de chacun de ces clients de sorte qu’il soit dirigé vers l’URL hébergeant le fichier PAC. Cette URL est indiquée dans la page **Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)** de TRITON - Web Security (voir *Configuration de l’accès des utilisateurs au filtrage hybride*, page 214).

Le mécanisme précis de configuration d’un navigateur pour qu’il utilise le fichier PAC dépend du navigateur et de votre environnement réseau. Par exemple, si vous utilisez Microsoft Active Directory et Internet Explorer ou Mozilla Firefox, vous pouvez automatiser ce processus grâce à des stratégies de groupe. Vous pouvez également demander aux utilisateurs de configurer leur navigateur manuellement.

- Pour Microsoft Internet Explorer 8 ou 9, sélectionnez **Outils > Options Internet** et ouvrez l’onglet **Connexions**. Cliquez sur **Paramètres réseau**, puis cochez l’option **Utiliser un script de configuration automatique**. Saisissez l’URL du fichier PAC dans le champ **Adresse**.
- Pour Mozilla Firefox 3.x, sélectionnez **Outils > Options**, cliquez sur l’icône **Avancé**, puis ouvrez l’onglet **Réseau**. Sous Connexion, cliquez sur **Paramètres**, puis sélectionnez **Adresse de configuration automatique du proxy**. Saisissez l’URL du fichier PAC dans le champ vide.

Le fichier PAC par défaut fourni par Websense contient les paramètres par défaut du service hybride et les modifications que vous avez éventuellement apportées dans les pages Hybrid Configuration (Configuration hybride). Pour personnaliser votre fichier PAC, créez un répertoire intitulé **pac** dans le répertoire **ssdata** de Websense (par défaut, \Program Files\Websense\Web Security\bin\ssdata\pac sous Windows, ou /opt/websense/bin/ssdata/pac sous Linux). Vous disposez ensuite des options suivantes :

- Pour utiliser votre propre fichier PAC, créez un fichier nommé *websense.pac* et placez-le dans le répertoire **pac** de Websense.
- Pour ajouter un fragment personnalisé dans le fichier PAC par défaut, placez ce fragment JavaScript dans un fichier nommé *customfinal.pac*, et placez ce dernier dans le répertoire **pac** de Websense. Ce fragment est alors ajouté dans le fichier PAC par défaut et remplace le jeton _CUSTOMFINALPAC_.

Remarque

Le fichier websense.pac personnalisé doit contenir la fonction suivante :

```
function FindProxyForURL(url, hôte) {}
```

Lorsque le fichier ne contient pas cette fonction, le service hybride le rejette.

Lorsque le répertoire **pac** contient l’un de ces fichiers, le service de synchronisation (Sync Service) le détecte et envoie les données au service hybride. Pour que le service de synchronisation puisse envoyer ce fichier, la taille de ce dernier doit être supérieure à 0 Ko et ne pas dépasser 50 Ko. Sync Service détecte également la présence d’une version plus récente du fichier PAC ou du fragment et actualise la version utilisée par le service hybride.

En matière de fichiers PAC personnalisés, il est recommandé de configurer un fichier personnalisé ou un fragment personnalisé, mais pas les deux. Si le répertoire **pac** contient les deux fichiers, nous vous conseillons de déterminer si le fichier PAC personnalisé complet ou le fragment personnalisé répond le mieux à vos besoins, puis de supprimer l'autre fichier dans ce répertoire.

Pour ne plus utiliser de fichier PAC ou de fragment personnalisé, supprimez le fichier ou le fragment en question dans le répertoire **pac**.

La page **Hybrid Service (Service hybride)** présente le type de fichier PAC utilisé et la date et l'heure auxquelles Sync Service a envoyé pour la dernière fois un fichier ou un fragment personnalisé au service hybride (voir *Surveillance de la communication avec le service hybride*, page 233).

Si vous ne maîtrisez pas suffisamment les fichiers PAC, il peut être utile de rechercher des informations de base sur Internet. Vous trouverez une bonne présentation de ce fichier sur Wikipedia, ainsi que davantage d'informations et plusieurs exemples de fichiers PAC sur le site http://www.findproxyforurl.com/.

Envoi de données d'utilisateur et de groupe au service hybride

Si votre organisation utilise un service d'annuaire de type LDAP pris en charge (Windows Active Directory (Mode natif), Oracle (Sun Java) Directory Server ou Novell eDirectory), vous pouvez collecter les données des utilisateurs et des groupes et les envoyer au service hybride. Deux composants Websense permettent d'effectuer cette opération :

- **Websense Directory Agent** collecte les informations des utilisateurs et des groupes auprès de Directory Server et les conserve pour le filtrage hybride.
- **Websense Sync Service** transmet les informations relatives aux stratégies, à la génération de rapports et au fichier PAC personnalisé et les données des utilisateurs/groupes entre les systèmes local et hybride.

Lorsque le filtrage hybride est correctement configuré, les informations issues de Directory Agent servent à appliquer le filtrage basé sur les utilisateurs et les groupes.

Si votre organisation exploite Windows Active Directory en mode mixte, les données des utilisateurs et des groupes ne peuvent pas être récupérées et envoyées au service hybride.

Lorsque le filtrage hybride exploite les données d'annuaire collectées par Directory Agent pour identifier les utilisateurs, vous avez deux possibilités :

- Configurez le service hybride pour qu'il crée automatiquement un mot de passe de connexion hybride pour tous les comptes d'utilisateur envoyés par Directory Agent. Les mots de passe sont envoyés à chaque adresse électronique d'utilisateur à intervalles échelonnés afin d'éviter tout afflux soudain de messages électroniques.
- Faites en sorte que les utilisateurs demandent leur propre mot de passe lorsqu'ils se connectent pour la première fois au service hybride à partir de l'extérieur d'un emplacement filtré. Dans ce cas, les utilisateurs doivent fournir une adresse électronique correspondant à un compte envoyé par Directory Agent. Le mot de passe est alors envoyé à cette adresse électronique.

  Vous devez de ce fait vous assurer que l'adresse de messagerie Web de votre organisation ait été ajoutée en tant que destination non filtrée. Voir *Définition des sites non filtrés par le service hybride*, page 211.

Configuration des paramètres de Directory Agent pour le filtrage hybride

Sélectionnez **Paramètres > Hybrid Configuration (Configuration hybride > Shared User Data (Données utilisateur partagées)** pour revoir et modifier la configuration actuelle de Directory Agent et configurer la communication entre Directory Agent et Sync Service.

Le tableau situé en haut de la page répertorie les catalogues globaux Active Directory identifiés dans la page **Paramètres > Général > Services d'annuaire**. Cette page vous permet d'ajouter ou de supprimer des serveurs de catalogues globaux ou de modifier le service d'annuaire utilisé par Websense.

> **Remarque**
>
> Lorsque vous supprimez un serveur Active Directory dans la page des services d'annuaire, exécutez également la procédure manuelle suivante afin de vous assurer que ce serveur a bien été supprimé dans les paramètres de Directory Agent :
>
> - Déploiements logiciels : supprimez tous les fichiers du répertoire **Websense/Web Security/bin/snapshots**. Sélectionnez ensuite **Paramètres > Hybrid Configuration (Configuration hybride) > Scheduling (Planification)**, puis cliquez sur **Envoyer** sous l'option Send Update Now (Envoyer la mise à jour maintenant).
> - Déploiements de dispositifs : contactez le Support technique de Websense pour toute assistance.

Pour affiner la méthode utilisée par Directory Agent pour effectuer des recherches dans l'annuaire et mettre en package les résultats pour le service hybride, cliquez sur une adresse IP ou un nom d'hôte dans le tableau. Voir *Configuration du mode de collecte des données pour le filtrage hybride*, page 222.

Pour afficher les contextes des catalogues globaux de l'annuaire, définis pour l'identification des utilisateurs hybrides, cliquez sur l'option **View Context (Afficher le contexte)** située sous Contextes dans le tableau. Voir *Ajout et modification de contextes d'annuaire*, page 224.

Pour que le service hybride génère des mots de passe pour tous les comptes d'utilisateur qu'il voit, faites défiler la section **Generate User Passwords (Générer des mots de passe d'utilisateur)** vers le bas et activez l'option **Automatically generate and email passwords (Générer et envoyer automatiquement les mots de passe par courrier électronique)**.

Pour que les données de Directory Agent soient envoyées au service hybride :

1. Faites défiler l'écran jusqu'à la section **Synchronize User Data (Synchroniser les données des utilisateurs)**.
2. Vérifiez le **Nom ou l'adresse IP** de l'ordinateur Sync Service et le **Port** utilisé pour la communication Sync Service (par défaut, 55832).

   Dans la plupart des configurations, ces champs sont renseignés automatiquement mais peuvent être au besoin actualisés manuellement.
3. Pour vérifier que Directory Agent peut envoyer les données au service de synchronisation, cliquez sur **Test Connection (Tester la connexion)**. Ce test peut prendre une minute ou davantage de temps.
   - Lorsque la connexion est établie, un message confirme le succès de l'opération.

- Si la connexion ne peut pas être établie, vérifiez l'adresse IP ou le nom d'hôte de l'ordinateur Sync Service, ainsi que le port de communication. Assurez-vous également que l'ordinateur Sync Service soit opérationnel, que le service de synchronisation s'exécute et que votre pare-feu réseau autorise les connexions au port de Sync Service.

4. Lorsque vous avez terminé, 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)**.

Configuration du mode de collecte des données pour le filtrage hybride

Pour affiner la méthode utilisée par Directory Agent pour effectuer des recherches dans le service d'annuaire sélectionné et mettre en package les informations relatives aux utilisateurs et aux groupes pour le service hybride, utilisez la page **Shared User Data (Données utilisateur partagées) > Active Directory (Mode natif)**.

Sous Root Context for Hybrid Filtering Users (Contexte racine des utilisateurs du filtrage hybride), cliquez sur **Ajouter** pour définir le **Contexte racine** à utiliser lors de la collecte des données des utilisateurs et des groupes dans l'annuaire. Pour accroître la vitesse et l'efficacité, limitez ce contexte. Voir *Ajout et modification de contextes d'annuaire*, page 224.

Avertissement

Le nombre de groupes pouvant être pris en charge par le service hybride est limité. Cette limite dépend d'un certain nombre de facteurs mais, lorsqu'elle est dépassée, les demandes des utilisateurs ne sont plus correctement filtrées (le service ne démarre plus).

Si votre organisation utilise une vaste forêt d'annuaire et des milliers de groupes, assurez-vous de configurer Directory Agent pour qu'il charge uniquement les informations requises pour filtrer les utilisateurs dont les demandes doivent être envoyées au service hybride. Vous pouvez ne sélectionner que des groupes spécifiques ou définir un contexte racine spécifique et limité.

Il est préférable de fournir des contextes incluant uniquement les utilisateurs filtrés par le service hybride.

Si vous utilisez Active Directory et plusieurs instances de Directory Agent, assurez-vous que chacune de ces instances soit associée à un contexte racine unique, sans chevauchement. Faites particulièrement attention à cela dans les cas suivants :

- Plusieurs instances de Directory Agent sont configurées pour se connecter aux contrôleurs de domaine gérant tous le même serveur Active Directory.
- Une seule instance de Directory Agent est configurée pour communiquer avec un domaine Active Directory parent, tandis qu'une autre instance est configurée pour communiquer avec un domaine Active Directory enfant (serveur de catalogue global distinct).

Vous pouvez affiner encore davantage les données envoyées au service hybride en définissant des modèles (ou filtres de recherche) visant à retirer les doublons ou les entrées non désirées des résultats de recherche de l'annuaire. Pour plus d'informations, consultez la section *Optimisation des résultats des recherches*, page 226.

Oracle (Sun Java) Directory Server et filtrage hybride

Si votre organisation utilise Oracle (Sun Java) Directory Server, sélectionnez **Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées)** pour affiner la méthode utilisée par Directory Agent pour effectuer des recherches dans l'annuaire et mettre en package les informations relatives aux utilisateurs et aux groupes pour le service hybride.

Important

Pour pouvoir utiliser l'une des versions de Sun Java System Directory ou Oracle Directory Server pour envoyer les informations relatives aux utilisateurs et aux groupes au service hybride, vous devez modifier la configuration de Directory Agent.

Ouvrez le fichier **das.ini** (situé dans le répertoire **bin** de Websense de l'ordinateur Directory Agent) et localisez la section suivante :

```
# Enable next two parameters if your DS is Sun Java
# GroupMembershipAttribute=uniqueMember
# MemberOfAttribute=memberOf
```

Activez les paramètres GroupMembershipAttribute et MemberOfAttribute en supprimant le symbole # présent au début de ces lignes, enregistrez le fichier, puis redémarrez Directory Agent.

1. Sous Root Context for Hybrid Filtering Users (Contexte racine des utilisateurs du filtrage hybride), cliquez sur **Ajouter** pour définir le **Contexte racine** à utiliser lors de la collecte des données des utilisateurs et des groupes dans l'annuaire. Pour accroître la vitesse et l'efficacité, limitez ce contexte. Voir *Ajout et modification de contextes d'annuaire*, page 224.

   Définissez un contexte incluant uniquement les utilisateurs filtrés par le service hybride.
2. Sous Synchronize User Data (Synchroniser les données des utilisateurs), vérifiez le **Nom ou l'adresse IP** de l'ordinateur Sync Service et le **Port** utilisé pour la communication Sync Service (par défaut, 55832).

   Ces champs sont renseignés automatiquement mais peuvent être au besoin actualisés manuellement.
3. Pour vérifier que Directory Agent peut envoyer les données au service de synchronisation, cliquez sur **Test Connection (Tester la connexion)**. Ce test peut prendre une minute ou davantage de temps.
   - Lorsque la connexion est établie, un message confirme le succès de l'opération.
   - Si la connexion ne peut pas être établie, vérifiez l'adresse IPv4 ou le nom d'hôte de l'ordinateur Sync Service, ainsi que le port de communication. Assurez-vous également que l'ordinateur Sync Service soit opérationnel, que le service de synchronisation s'exécute et que votre pare-feu réseau autorise les connexions au port de Sync Service.

Vous pouvez affiner encore davantage les données envoyées au service hybride en définissant des modèles (ou filtres de recherche) visant à retirer les doublons ou les entrées non désirées des résultats de recherche de l'annuaire. Pour plus d'informations, consultez la section *Optimisation des résultats des recherches*, page 226.

Novell eDirectory et filtrage hybride

Si votre organisation utilise Novell eDirectory, sélectionnez **Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées)** pour affiner la méthode utilisée par Directory Agent pour effectuer des recherches dans l'annuaire et mettre en package les informations relatives aux utilisateurs et aux groupes pour le service hybride.

1. Sous Root Context for Hybrid Filtering Users (Contexte racine des utilisateurs du filtrage hybride), cliquez sur **Ajouter** pour définir le **Contexte racine** à utiliser lors de la collecte des données des utilisateurs et des groupes dans l'annuaire. Pour accroître la vitesse et l'efficacité, limitez ce contexte. Voir *Ajout et modification de contextes d'annuaire*, page 224.

   Définissez un contexte incluant uniquement les utilisateurs filtrés par le service hybride.
2. Sous Synchronize User Data (Synchroniser les données des utilisateurs), vérifiez le **Nom ou l'adresse IP** de l'ordinateur Sync Service et le **Port** utilisé pour la communication Sync Service (par défaut, 55832).

   Ces champs sont renseignés automatiquement mais peuvent être au besoin actualisés manuellement.
3. Pour vérifier que Directory Agent peut envoyer les données au service de synchronisation, cliquez sur **Test Connection (Tester la connexion)**. Ce test peut prendre une minute ou davantage de temps.
   - Lorsque la connexion est établie, un message confirme le succès de l'opération.
   - Si la connexion ne peut pas être établie, vérifiez l'adresse IPv4 ou le nom d'hôte de l'ordinateur Sync Service, ainsi que le port de communication. Assurez-vous également que l'ordinateur Sync Service soit opérationnel, que le service de synchronisation s'exécute et que votre pare-feu réseau autorise les connexions au port de Sync Service.

Vous pouvez affiner encore davantage les données envoyées au service hybride en définissant des modèles (ou filtres de recherche) visant à retirer les doublons ou les entrées non désirées des résultats de recherche de l'annuaire. Pour plus d'informations, consultez la section *Optimisation des résultats des recherches*, page 226.

Ajout et modification de contextes d'annuaire

Pour affiner la méthode utilisée par Directory Agent pour effectuer des recherches dans l'annuaire des utilisateurs et mettre en package les informations relatives aux utilisateurs et aux groupes pour le service hybride, utilisez la page **Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées) > Add Context (Ajouter un contexte)**.

Avertissement

Le nombre de groupes pouvant être pris en charge par le service hybride est limité. Cette limite dépend d'un certain nombre de facteurs mais, lorsqu'elle est dépassée, les demandes des utilisateurs ne sont plus correctement filtrées (le service ne démarre plus).

Si votre organisation utilise une vaste forêt d'annuaire et des milliers de groupes, assurez-vous de configurer Directory Agent pour qu'il charge uniquement les informations requises pour filtrer les utilisateurs dont les demandes doivent être envoyées au service hybride. Vous pouvez ne sélectionner que des groupes spécifiques ou définir un contexte racine spécifique et limité.

Vous pouvez sélectionner plusieurs contextes au sein de l'annuaire. Il est préférable d'inclure des contextes comprenant uniquement les utilisateurs filtrés par le service hybride : par exemple, vous pouvez avoir des utilisateurs hybrides dans plusieurs unités d'organisation. À l'inverse, si vous souhaitez synchroniser tous les utilisateurs d'un certain nombre de groupes spécifiques, vous pouvez dans ce cas sélectionner un contexte pour chaque groupe, chaque contexte étant alors le nom complet du groupe.

Par défaut, Directory Agent emploie les filtres d'utilisateurs et de groupes définis sous *Paramètres avancés de l'annuaire* dans la page **Paramètres > Général > Services d'annuaire**. Au besoin, vous pouvez personnaliser ces filtres pour chaque contexte de filtrage hybride, par exemple pour n'inclure que les utilisateurs membres d'un groupe filtré par le service hybride.

Vous pouvez également choisir d'exclure certains contextes de la recherche de Directory Agent. Cette opération peut se révéler utile lorsqu'un contexte spécifique n'est pas nécessaire ou est susceptible de générer des problèmes avec le service hybride, par exemple un groupe d'administrateurs incluant plusieurs adresses électroniques dans un même enregistrement. Vous ne pouvez exclure un contexte que s'il fait partie d'un contexte d'annuaire inclus.

1. Développez l'arborescence des entrées d'annuaire afin de localiser le contexte à exploiter lors de la collecte des données des utilisateurs et des groupes dans l'annuaire. Pour accroître la vitesse et l'efficacité, limitez ce contexte.

   Au besoin, servez-vous du champ de recherche pour localiser le nom du contexte. Vous pouvez lancer des recherches dans des unités d'organisation, des groupes, des utilisateurs ou dans toutes les entrées de l'annuaire. Lorsque les résultats de la recherche présentent plusieurs contextes, sélectionnez-en un, puis cliquez sur **Show in Tree (Afficher dans l'arborescence)** pour voir son emplacement dans l'arborescence des entrées de l'annuaire.
2. Cochez ce contexte, puis cliquez sur **Specify Include Context (Spécifier le contexte à inclure)**.
3. Dans la fenêtre contextuelle qui s'affiche, indiquez à quelle profondeur Directory Agent doit rechercher des utilisateurs et des groupes dans ce contexte racine.
   - Sélectionnez **Context Only (Contexte uniquement)** pour limiter les recherches au contexte racine seulement.
   - Sélectionnez **One Level (Un seul niveau)** pour limiter les recherches au contexte racine et à un niveau au-dessous.
   - Sélectionnez **All Levels (Tous les niveaux)** pour étendre les recherches au contexte racine et à tous les niveaux inférieurs.
4. Si vous sélectionnez One Level (Un seul niveau) ou All Levels (Tous les niveaux) pour les recherches de groupes, cochez l'option **Include all users in selected groups, regardless of context (Inclure tous les utilisateurs des groupes sélectionnés, quel que soit le contexte)** pour être certain d'inclure tous les utilisateurs des groupes détectés dans la recherche de l'annuaire, y compris lorsque le contexte diffère pour certains de ces utilisateurs. Cette option est sélectionnée par défaut pour Active Directory.
5. Pour affiner les filtres de recherche utilisés par Directory Agent pour ce contexte, cliquez sur **Customize Search Filters (Personnaliser les filtres de recherche)**.
6. Cochez l'option **Customize search filters (Personnaliser les filtres de recherche)**, puis modifiez les filtres de recherche d'utilisateurs et de groupes en fonction de vos besoins.
7. Cliquez sur **OK** pour enregistrer ce contexte d'annuaire.

8. Lorsque vous indiquez qu'un contexte est inclus, tous les contextes situés au-dessous de celui-ci dans l'arborescence sont également inclus par défaut. Pour exclure un contexte situé dans un contexte inclus, cochez le contexte qui ne doit pas être envoyé au service hybride, puis cliquez sur **Specify Exclude Context (Spécifier le contexte à exclure)**. Vous pouvez au besoin sélectionner plusieurs contextes.
9. Dans la fenêtre contextuelle qui s'affiche, notez que l'option **Set as exclude context (Définir en tant que contexte exclu)** est sélectionnée. L'option **Remove exclude context (Supprimer le contexte à exclure)** n'est disponible que si vous avez sélectionné un contexte exclu existant et cliqué sur **Specify Exclude Context (Spécifier le contexte à exclure)** pour le modifier.
10. Indiquez à quelle profondeur Directory Agent doit rechercher les utilisateurs et les groupes dans ce contexte racine.
    - Sélectionnez **Context Only (Contexte uniquement)** pour limiter les recherches au contexte spécifié seulement.
    - Sélectionnez **One Level (Un seul niveau)** pour limiter les recherches au contexte spécifié et à un niveau au-dessous.
    - Sélectionnez **All Levels (Tous les niveaux)** pour étendre les recherches au contexte spécifié et à tous les niveaux inférieurs.

    Notez que les niveaux d'utilisateurs et de groupes d'un contexte exclu ne peuvent pas être supérieurs aux niveaux définis pour son contexte racine. Par exemple, si le niveau de recherche des utilisateurs ou des groupes du contexte racine est défini sur Context Only (Contexte uniquement), le niveau de recherche des utilisateurs ou des groupes correspondant du contexte exclu est également défini sur Context Only (Contexte uniquement) et n'est pas modifiable.

    Si vous sélectionnez All Levels (Tous les niveaux) pour les utilisateurs et les groupes, tous les éléments situés au-dessous du contexte sélectionné sont exclus et vous ne pouvez pas parcourir les niveaux inférieurs de l'arborescence des entrées de l'annuaire.
11. Cliquez sur **OK** pour enregistrer le contexte exclu.

Lorsque vous avez terminé, cliquez sur **OK** pour fermer la page Add Context (Ajouter un contexte) et mettre à jour le tableau Root Context for Hybrid Filtering Users (Contexte racine des utilisateurs du filtrage hybride). Vous devez également cliquer sur **OK** dans la page Shared User Data (Données utilisateur partagées) pour mettre vos modifications en cache.

Optimisation des résultats des recherches

L'optimisation des résultats des recherches affine encore davantage les données envoyées au service hybride en définissant les modèles (ou filtres de recherche) utilisés pour retirer les doublons ou les entrées non désirées des résultats de recherche de l'annuaire. Cette optimisation permet également de modifier l'attribut **mail** des entrées d'annuaire collectées par Directory Agent avant leur envoi au service hybride.

Si, par exemple, l'attribut **mail** de votre service d'annuaire contient une référence à une adresse électronique partielle ou interne, vous pouvez utiliser un filtre de recherche pour remplacer ces informations partielles ou internes par des informations externes utilisables par le service hybride. Ce fonctionnement peut se révéler utile lorsque le service hybride est configuré pour créer automatiquement les mots de passe des utilisateurs de sorte que ces derniers puissent se connecter au filtrage hybride lorsqu'ils sont hors site (voir *Configuration du filtrage hybride pour les utilisateurs hors site*, page 243).

Tous les filtres de recherche que vous créez dans TRITON - Web Security sont appliqués aux données d'annuaires collectées par Directory Agent avant que ces données ne soient envoyées au service hybride.

Cliquez sur **Optimize Search Results (Optimiser les résultats des recherches)** pour voir les filtres de recherche actuels ou en créer de nouveaux à l'aide de caractères génériques ou d'expressions régulières. Il existe deux types de filtres de recherche : l'un permet de filtrer les entrées des utilisateurs, l'autre les entrées des groupes.

- Pour créer un nouveau filtre de recherche, cliquez sur **Ajouter** sous le tableau approprié.
- Pour modifier un filtre de recherche existant, cliquez sur l'option **Find String (Rechercher une chaîne)** associée.

La boîte de dialogue contextuelle qui s'affiche vous invite alors à modifier ou à saisir les éléments suivants :

- **Find string (Rechercher une chaîne)** : texte à rechercher dans les données d'annuaire d'origine collectées par Directory Agent
- **Replace string (Remplacer une chaîne)** : nouveau texte à substituer au texte d'origine dans les données envoyées au service hybride

Lorsque vous avez terminé, cliquez sur **OK** pour fermer la boîte de dialogue et mettre à jour le tableau Filter User Results (Filtrer les résultats des utilisateurs) ou Filter Group Results (Filtrer les résultats des groupes). Vous devez également cliquer sur **OK** dans la page Shared User Data (Données utilisateur partagées) pour mettre vos modifications en cache.

À ce stade, Directory Agent applique les filtres de recherche que vous avez créés uniquement à l'attribut **mail**.

Planification de la communication avec le filtrage hybride

Pour définir la fréquence d'envoi des données d'annuaire collectées par Directory Agent au service hybride et la fréquence de collecte des données de rapport, sélectionnez **Paramètres > Hybrid Configuration (Configuration hybride) > Scheduling (Planification)**.

Remarque

Les données de stratégie sont collectées chaque fois que vous cliquez sur **Save and Deploy (Enregistrer et déployer)** dans TRITON - Web Security et sont par défaut envoyées au service hybride toutes les 15 minutes. Si la modification apportée à vos stratégies est importante et que vous souhaitez envoyer immédiatement les informations relatives aux utilisateurs et aux groupes, cliquez sur l'option **Envoyer** située sous Send Policy Data Now (Envoyer les données de stratégie maintenant).

Pour configurer la fréquence d'envoi des informations d'annuaire au service hybride :

1. Sous **Send User Data (Envoyer les données des utilisateurs)**, sélectionnez le ou les jours de la semaine auxquels les informations relatives aux utilisateurs et aux groupes doivent être envoyées au service hybride. Si vous exploitez les informations de votre annuaire pour identifier les utilisateurs, vous devez envoyer les données Directory Agent une fois par semaine au moins.
2. Saisissez les heures de début et de fin pour définir la période au cours de laquelle Sync Service tente d'envoyer les données de l'annuaire au service hybride. En général, les données de l'annuaire sont envoyées au cours des périodes de faible trafic dans votre réseau.

3. Si la modification apportée aux données de votre service d'annuaire est importante et que vous souhaitez envoyer immédiatement les informations relatives aux utilisateurs et aux groupes, cliquez sur l'option **Envoyer** située sous Send Update Now (Envoyer la mise à jour maintenant).

   Si TRITON - Web Security reçoit la confirmation de Sync Service, un message s'affiche pour confirmer l'opération. Cela signifie que Sync Service enverra les données, pas que le service hybride les a reçues.

Pour configurer ou non la collecte des données de rapports par le service hybride et la fréquence de récupération des données par Sync Service :

Important

Pour que Sync Service puisse transmettre les données de rapports hybrides à Log Server, un port de communication hybride doit être configuré dans la page Paramètres > Général > Journalisation. Pour plus d'informations, consultez la section *Configuration du mode de journalisation des requêtes filtrées*, page 398.

Si vous utilisez la journalisation distribuée, Sync Service doit être configuré pour communiquer avec l'instance centrale de Log Server. Les données de la journalisation hybride des instances distantes de Log Server ne peuvent pas être transmises à l'instance centrale de Log Server.

---

1. Sous Collect and Retrieve Reporting Data (Collecter et récupérer les données de rapport), cochez la case **Have the hybrid service collect reporting data for the clients it filters (Le service hybride doit collecter les données de rapports des clients qu'il filtre)**.

   Si vous désactivez cette case à cocher, les données des journaux ne sont pas enregistrées pour les utilisateurs du filtrage hybride. Dans ce cas, aucune information relative à l'activité Internet de ces utilisateurs ne s'affiche dans les rapports.
2. Sélectionnez le ou les jours de la semaine au cours desquels Sync Service doit demander les données de rapports au service hybride. Vous devez récupérer ces données une fois par semaine au moins.
3. Saisissez les heures de début et de fin pour définir la période au cours de laquelle Sync Service doit récupérer les données auprès du service hybride. Il est généralement préférable de récupérer ces données au cours des périodes de faible trafic dans votre réseau.
4. Sélectionnez la fréquence à laquelle Sync Service doit demander les données de rapports au service hybride au cours de la période de début et de fin définie.

   Sync Service ne peut pas télécharger les données de rapports plus fréquemment que toutes les 15 minutes. Cela signifie qu'un certain délai s'écoule entre le moment où le filtrage hybride envoie les demandes Internet et le moment où ces demandes s'affichent dans les rapports de TRITON - Web Security.

Si le trafic entre Sync Service et le service hybride doit être acheminé via un serveur proxy ou un pare-feu :

1. Sous Route Sync Service Traffic (Acheminer le trafic Sync Service), cochez la case **Route Sync Service traffic through a proxy server or firewall (Acheminer le trafic Sync Service via un serveur proxy ou un pare-feu)**.
2. Saisissez l'adresse IP ou le nom d'hôte du serveur proxy ou du pare-feu et définissez le port à utiliser.
3. Si le serveur spécifié requiert une authentification, saisissez le nom d'utilisateur et le mot de passe que Sync Service doit utiliser pour y accéder.

Lorsque vous avez terminé, 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)**.

Définition de paramètres d'authentification personnalisés

Pour ajouter et modifier des règles personnalisées et changer le comportement d'authentification par défaut d'applications ou de sites spécifiques, utilisez la page **Paramètres > Hybrid Configuration (Configuration hybride) > Custom Authentication (Authentification personnalisée)**.

Il arrive parfois que certaines applications Internet et certains sites Web ne puissent pas s'authentifier auprès du service hybride. Cela peut se produire, par exemple, avec les programmes de messagerie instantanée, les mises à jour d'antivirus ou les services de mises à jour logicielles.

Pour que certaines applications puissent contourner l'authentification lorsqu'elles ne gèrent pas correctement le processus d'authentification, vous pouvez spécifier des agents utilisateurs, des domaines ou des URL, ou une combinaison de ces options.

Un agent utilisateur est une chaîne envoyée de votre navigateur ou d'une application Internet au serveur hébergeant le site consulté. Cette chaîne identifie le navigateur ou l'application utilisé(e), son numéro de version et les détails relatifs à votre système, par exemple votre système d'exploitation et sa version. Le serveur de destination utilise ensuite ces informations pour fournir un contenu approprié à votre navigateur ou application spécifique.

Voici par exemple un agent utilisateur pour Firefox :

```
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6)
```

Dans cet exemple, Windows NT 5.1 précise que le système d'exploitation est Windows XP et que la langue utilisée est l'anglais US.

Pour obtenir la chaîne de l'agent utilisateur de votre navigateur, entrez ce qui suit dans la barre d'adresse du navigateur :

```
javascript:alert(navigator.userAgent)
```

Vous pouvez voir quels agents utilisateurs ont envoyé des demandes d'authentification via le service hybride dans le rapport User Agents by Volume (Agents utilisateurs par volume), disponible dans la page Custom Authentication (Authentification personnalisée) et dans la page **Main (Principal) > État > Service hybride**. Si l'un des agents utilisateurs de ce rapport est associé à un grand nombre de demandes d'authentification, il est possible qu'il rencontre des problèmes pour s'authentifier. Vous pouvez sélectionner un agent utilisateur dans le rapport, puis cliquer sur **Create Rule (Créer une règle)** pour lui ajouter une nouvelle règle d'authentification personnalisée. Voir *Affichage du rapport Volume par agent utilisateur*, page 235.

Pour définir une règle d'authentification personnalisée, cliquez sur **Ajouter**, puis consultez la section *Ajout de règles d'authentification personnalisées*, page 230.

Pour modifier une règle existante, cliquez sur son **Nom**, puis consultez la section *Modification des règles d'authentification personnalisées*, page 231.

Pour supprimer une règle d'authentification personnalisée, cochez la case accolée à son nom, puis cliquez sur **Supprimer**.

Si vous avez ajouté ou modifié une règle d'authentification personnalisée, 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)**.

Ajout de règles d'authentification personnalisées

Utilisez la page **Custom Authentication (Authentification personnalisée) > Add Custom Authentication Rule (Ajouter une règle d'authentification personnalisée)** pour définir un ou plusieurs agents utilisateurs, domaines ou URL qui ne parviennent pas à s'authentifier auprès du service hybride.

1. Entrez le **Nom** de la règle. Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

   Les noms peuvent comprendre des espaces, des tirets et des apostrophes.

2. Définissez les **Agents utilisateurs**, le cas échéant, de la règle :
   - Pour établir une correspondance avec toutes les chaînes d'agent utilisateur, sélectionnez **All user agents (Tous les agents utilisateurs)**. Cette opération peut se révéler utile pour configurer une règle personnalisée s'appliquant à tous les navigateurs de tous les systèmes d'exploitation présents dans votre organisation.
   - Si l'application n'envoie pas de chaîne d'agent utilisateur vers Internet, sélectionnez **No user agent header sent (Pas d'envoi d'en-tête d'agent utilisateur)**.

     Cette option est associée à toutes les applications qui n'envoient pas d'agent utilisateur. Dans ce cas, affinez la règle en saisissant une ou plusieurs URL ou des domaines dans le champ **Destinations**.
   - Pour appliquer l'authentification personnalisée à un ou plusieurs agents utilisateurs, sélectionnez **Custom user agents (Agents utilisateurs personnalisés)**. Entrez chaque agent utilisateur sur une ligne distincte. Servez-vous du caractère astérisque pour associer une même ligne à plusieurs chaînes d'agent utilisateur, par exemple Mozilla/5.0*.

   > **Remarque**
   > Si vous créez directement une nouvelle règle à partir du rapport User Agents by Volume (Agents utilisateurs par volume), les agents utilisateurs que vous avez sélectionnés dans ce rapport sont déjà renseignés dans ce champ.

3. Définissez les URL ou les domaines (au besoin) de la règle dans le champ **Destinations** :
   - Pour établir une correspondance avec tous les domaines et URL, sélectionnez **All destinations (Toutes les destinations)**. Cette opération peut se révéler utile si vous configurez une règle personnalisée s'appliquant à un agent utilisateur spécifique qui accède à plusieurs sites.
   - Pour appliquer l'authentification personnalisée à un ou plusieurs domaines ou URL spécifiques, sélectionnez **Custom destinations (Destinations personnalisées)**. Entrez chaque URL ou domaine sur une ligne distincte.

     Dans les URL, la partie du protocole (http://) doit être insérée au début et une barre oblique (/) à la fin (par exemple, http://www.google.fr/). En l'absence de ces éléments, la chaîne est traitée comme un domaine. Les domaines ne peuvent pas inclure de barre oblique à la fin (par exemple, mondomaine.com).

     Servez-vous du caractère astérisque pour associer une même ligne à plusieurs destinations : Par exemple, l'entrée *.mondomaine.com assure une correspondance pour tous les domaines se terminant par « mondomaine.com ».

4. Sélectionnez la **Méthode d'authentification** de la règle personnalisée.
   - **Par défaut** : cette option utilise votre méthode d'authentification par défaut.
   - **NTLM** : cette option utilise l'identification NTLM pour les agents utilisateurs et destinations spécifiés. Lorsqu'une application ne prend pas en charge l'identification NTLM, l'authentification de base la remplace.

     Remarque

     Pour que cette option soit disponible, l'identification NTLM doit être activée pour votre compte.

   - **Secure form authentication (Formulaire d'authentification sécurisée)** : cette option utilise un formulaire d'authentification sécurisée afin de présenter un formulaire de connexion sécurisée à l'utilisateur final. Pour plus d'informations, consultez la section *Identification des utilisateurs du filtrage hybride*, page 311.
   - **Basic Authentication (Authentification de base)** : cette option utilise le mécanisme d'authentification de base pris en charge par la plupart des navigateurs Web. Aucune page d'accueil ne s'affiche. Pour plus d'informations sur l'authentification de base, consultez la section *Identification des utilisateurs du filtrage hybride*, page 311.
   - **Welcome page (Page d'accueil)** : cette option présente une page d'accueil aux utilisateurs avant qu'ils se servent de l'authentification de base pour continuer.
   - **Aucune** : cette option ignore toutes les méthodes d'authentification et d'identification présentes dans le service hybride. Sélectionnez cette option pour les applications Internet qui ne peuvent pas effectuer d'authentification.
5. Vous pouvez éventuellement sélectionner **Bypass content scanning (Ignorer l'analyse du contenu)** pour contourner le filtrage des agents utilisateurs et destinations spécifiés.

   Important

   Sélectionnez cette option **uniquement** pour les applications et sites qui, pour une raison quelconque, ne fonctionnent pas bien avec le filtrage Web hybride et auxquels vous faites confiance. La sélection de cette option peut autoriser l'entrée de virus et autres programmes malveillants dans votre réseau.

6. Cliquez sur **OK** pour revenir à la page Custom Authentication (Authentification personnalisée), 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)**.

Modification des règles d'authentification personnalisées

Utilisez la page **Custom Authentication (Authentification personnalisée) > Edit Custom Authentication Rule (Modifier une règle d'authentification personnalisée)** pour modifier les agents utilisateurs, domaines ou URL qui ne parviennent pas à s'authentifier auprès du service hybride.

1. Lorsque vous modifiez le **Nom** de la règle, assurez-vous qu'il comprenne entre 1 et 50 caractères et ne comporte pas les caractères suivants :

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

Les noms peuvent comprendre des espaces, des tirets et des apostrophes.

2. Le cas échéant, définissez ou mettez à jour les **agents utilisateurs** de la règle :
   - Pour établir une correspondance avec toutes les chaînes d'agent utilisateur, sélectionnez **All user agents (Tous les agents utilisateurs)**. Cette opération peut se révéler utile si vous configurez une règle personnalisée s'appliquant à tous les navigateurs de tous les systèmes d'exploitation présents dans votre organisation.
   - Si l'application n'envoie pas de chaîne d'agent utilisateur vers Internet, sélectionnez **No user agent header sent (Pas d'envoi d'en-tête d'agent utilisateur)**.

     Cette option sera associée à toutes les applications qui n'envoient pas d'agent utilisateur. Dans ce cas, nous vous conseillons d'affiner la règle en saisissant une ou plusieurs URL ou un ou plusieurs domaines dans le champ **Destinations**.
   - Pour appliquer l'authentification personnalisée à un ou plusieurs agents utilisateurs, sélectionnez **Custom user agents (Agents utilisateurs personnalisés)**. Entrez chaque agent utilisateur sur une ligne distincte. Servez-vous du caractère astérisque pour associer une même ligne à plusieurs chaînes d'agent utilisateur, par exemple Mozilla/5.0*.
3. Définissez ou mettez à jour les URL ou les domaines (au besoin) de la règle dans le champ **Destinations** :
   - Pour établir une correspondance avec tous les domaines et URL, sélectionnez **All destinations (Toutes les destinations)**. Cette opération peut se révéler utile si vous configurez une règle personnalisée s'appliquant à un agent utilisateur spécifique qui accède à plusieurs sites.
   - Pour appliquer l'authentification personnalisée à un ou plusieurs domaines ou URL spécifiques, sélectionnez **Custom destinations (Destinations personnalisées)**. Entrez chaque URL ou domaine sur une ligne distincte.

     Dans les URL, la partie du protocole (http://) doit être insérée au début et une barre oblique (/) à la fin (par exemple, http://www.google.fr/). En l'absence de ces éléments, la chaîne est traitée comme un domaine. Les domaines ne peuvent pas inclure de barre oblique à la fin (par exemple, mondomaine.com).

     Servez-vous du caractère astérisque pour associer une même ligne à plusieurs destinations : Par exemple, l'entrée *.mondomaine.com assure une correspondance pour tous les domaines se terminant par « mondomaine.com ».
4. Vérifiez ou mettez à jour la **Méthode d'authentification** de la règle personnalisée.
   - **Par défaut :** cette option utilise votre méthode d'authentification par défaut.
   - **NTLM :** cette option utilise l'identification NTLM pour les agents utilisateurs et destinations spécifiés. Lorsqu'une application ne prend pas en charge l'identification NTLM, l'authentification de base la remplace.

     Remarque

     Pour que cette option soit disponible, l'identification NTLM doit être activée pour votre compte.
   - **Form Authentication (Formulaire d'authentification) :** cette option utilise un formulaire d'authentification sécurisée afin de présenter un formulaire de connexion sécurisée à l'utilisateur final. Pour plus d'informations, consultez la section *Identification des utilisateurs du filtrage hybride*, page 311.

- **Basic Authentication (Authentification de base) :** cette option utilise le mécanisme d'authentification de base pris en charge par la plupart des navigateurs Web. Aucune page d'accueil ne s'affiche. Pour plus d'informations sur l'authentification de base, consultez la section *Identification des utilisateurs du filtrage hybride*, page 311.
- **Welcome page (Page d'accueil) :** cette option présente une page d'accueil aux utilisateurs avant qu'ils se servent de l'authentification de base pour continuer.
- **Aucune :** cette option ignore toutes les méthodes d'authentification et d'identification présentes dans le service hybride. Sélectionnez cette option pour les applications Internet qui ne peuvent pas effectuer d'authentification.

5. Vous pouvez éventuellement sélectionner **Bypass content scanning (Ignorer l'analyse du contenu)** pour contourner le filtrage des agents utilisateurs et destinations spécifiés.

   Important

   Sélectionnez cette option **uniquement** pour les applications et sites qui, pour une raison quelconque, ne fonctionnent pas bien avec le filtrage Web hybride et auxquels vous faites confiance. La sélection de cette option peut autoriser l'entrée de virus et autres programmes malveillants dans votre réseau.

6. Cliquez sur **OK** pour revenir à la page Custom Authentication (Authentification personnalisée), 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)**.

Surveillance de la communication avec le service hybride

Vous pouvez afficher l'état du service hybride dans la page **État > Tableau de bord > Service hybride** de TRITON - Web Security. Cette page indique à quel moment les données ont été envoyées ou reçues pour la dernière fois par le service hybride. En cas d'échec de l'envoi ou de la réception des données, vous pouvez voir à quel moment l'opération n'a pas pu être effectuée et les composants impliqués.

La page indique la date et l'heure auxquelles Sync Service a effectué les opérations suivantes pour la dernière fois :

- Connexion ou tentative de connexion au service hybride pour une raison quelconque
- Envoi ou tentative d'envoi des informations de l'annuaire au service hybride
- Récupération ou tentative de récupération des données de journaux (rapports) auprès du service hybride
- Envoi ou tentative d'envoi des données des journaux à Log Server
- Envoi ou tentative d'envoi des informations de compte au service hybride
- Envoi ou tentative d'envoi des informations de stratégie au service hybride

Si vous n'avez pas encore configuré de connexion entre les parties sur site et hybride de Websense Web Security Gateway Anywhere, un message indique que « aucune communication n'a été établie ».

Sous Last Directory Agent Sync Results (Derniers résultats de Directory Agent Sync), la page indique :

- La date et l'heure auxquelles Directory Agent a envoyé des données au service hybride pour la dernière fois
- Le nombre total d'utilisateurs et de groupes traités par Directory Agent
- Le nombre d'utilisateurs et de groupes ayant été mis à jour dans le service hybride
- Le nombre de groupes éliminés par le filtrage parce qu'ils contenaient des valeurs non valides
- Le nombre d'utilisateurs éliminés par le filtrage parce qu'ils comprenaient des adresses électroniques non valides
- Le nombre de nouveaux utilisateurs et groupes synchronisés avec le service hybride
- Le nombre d'utilisateurs et de groupes obsolètes retirés du service hybride

Cette page vous permet également d'accéder aux rapports relatifs aux méthodes d'authentification et aux agents utilisateurs du service hybride (voir *Affichage des rapports d'authentification du service hybride*, page 234, et *Affichage du rapport Volume par agent utilisateur*, page 235) et indique le type de fichier PAC utilisé :

- Fichier PAC par défaut du service hybride
- Fichier PAC personnalisé chargé depuis le répertoire **pac** de Websense (voir *Qu'est-ce qu'un fichier PAC ?*, page 219)
- Fichier PAC par défaut contenant un fragment personnalisé chargé

Si vous utilisez un fichier ou un fragment personnalisé, la page précise depuis quand ce fichier ou fragment est utilisé.

Si l'option **Secondary date stamp (Horodatage secondaire)** s'affiche pour le fichier PAC, cela signifie que Sync Service a chargé à la fois un fichier PAC personnalisé et un fragment personnalisé à partir du répertoire **pac**. En matière de fichiers PAC personnalisés, il est recommandé de configurer un fichier personnalisé ou un fragment personnalisé, mais pas les deux. Pour modifier ce comportement, accédez au répertoire **pac** (par défaut, \Program Files\Websense\Web Security\bin\data\pac sous Windows, ou /opt/websense/bin/data/pac sous Linux) et supprimez le fichier websense.pac ou customfinal.pac.

Si vous utilisez un logo avec votre page de blocage personnalisée, cette page présente la date et l'heure auxquelles le fichier du logo a été chargé vers le service hybride.

Affichage des rapports d'authentification du service hybride

Pour télécharger les données de rapports issus du service hybride et voir le détail de l'identification ou de l'authentification des utilisateurs du filtrage hybride auprès du service, sélectionnez l'option **View Report (Afficher le rapport)** située sous Authentication Report (Rapport d'authentification) dans la page **Main (Principal) > État > Service hybride**.

Le rapport comprend un graphique en secteurs et un tableau, et présente le nombre de clients ayant utilisé chaque méthode d'authentification disponible au cours des 7 derniers jours. Les options **Web Endpoint**, **Authentication Service (Service d'authentification)**, **NTLM identification (Identification NTLM)**, **Form authentication (Formulaire d'authentification)** et **Manual authentication (Authentification manuelle)** sont toutes configurées pour les clients dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification des utilisateurs hybrides) (voir *Identification des utilisateurs du filtrage hybride*, page 311).

L'authentification **X-Authenticated-User** est disponible si vous avez déployé l'un des éléments suivants en tant que serveur proxy chaîné en aval :

- Serveur Microsoft® Internet Security and Acceleration (ISA) ou serveur Forefront™ Threat Management Gateway (TMG)
- BlueCoat Proxy SG

Le serveur proxy en aval effectue l'authentification des utilisateurs et transmet les requêtes au proxy hybride en utilisant l'en-tête X-Authenticated-User.

Cliquez sur une méthode d'authentification du tableau pour voir la liste des utilisateurs qui se sont récemment authentifiés par cette méthode. Vous ne pouvez pas cliquer sur une méthode d'authentification que vous n'avez pas déployée ou qui n'est pas utilisée actuellement.

Chaque rapport de méthode d'authentification peut contenir jusqu'à 1 000 utilisateurs. Les utilisateurs sont répertoriés par nom, adresse électronique et date de dernière connexion. Pour afficher les pages précédentes ou suivantes, cliquez sur les flèches situées au bas du rapport.

Les rapports affichés dans le panneau de contenu ne peuvent pas être imprimés ni enregistrés dans un fichier. Pour imprimer ce rapport ou l'enregistrer dans un fichier, cliquez sur **Export to PDF (Exporter au format PDF)** ou **Export to XLS (Exporter au format XLS)** pour afficher le rapport dans le format de sortie approprié.

Important

Pour pouvoir afficher les rapports d'authentification au format PDF, Adobe Reader v7.0 ou une version ultérieure doit être installé dans l'ordinateur à partir duquel vous accédez à TRITON - Web Security.

Pour pouvoir afficher les rapports d'authentification au format XLS, Excel 2003 ou une version ultérieure doit être installé dans l'ordinateur à partir duquel vous accédez à TRITON - Web Security.

Chaque rapport indique la date et l'heure de sa dernière mise à jour. Les mises à jour ne sont pas automatiques : pour télécharger les données de rapport les plus récentes depuis le service hybride, cliquez sur **Update (Mettre à jour)**.

Affichage du rapport Volume par agent utilisateur

Pour voir quels agents utilisateurs ont envoyé des demandes d'authentification via le service hybride, sélectionnez l'option **View Report (Afficher le rapport)** située sous User Agent Volume Report (Rapport Volume par agent utilisateur) dans la page **Main (Principal) > État > Service hybride**.

Le résultat du rapport est un tableau qui présente le nombre de demandes d'authentification et le nombre total de requêtes effectuées par chaque agent utilisateur. Lorsqu'une règle d'authentification personnalisée est déjà associée à un agent utilisateur, vous pouvez survoler la colonne **Règle** avec votre souris pour voir les détails de cette règle personnalisée.

Vous pouvez filtrer les résultats du rapport comme suit :

- Saisissez un terme de recherche, puis cliquez sur **Rechercher**.
- Sélectionnez une **plage horaire** dans la liste déroulante. Si vous sélectionnez une plage de dates personnalisée, sélectionnez une période comprise entre 1 et 14 jours.
- Cochez la case **View only user agents with rules (Afficher uniquement les agents utilisateurs associés à des règles)** pour afficher uniquement les agents utilisateurs auxquels des règles d'authentification personnalisées sont associées.

Lorsque les résultats ne tiennent pas dans une seule page, cliquez sur les flèches situées au bas du rapport pour afficher les pages précédentes ou suivantes.

Si l'un des agents utilisateurs de ce rapport est associé à un grand nombre de demandes d'authentification, il est possible qu'il rencontre des problèmes pour s'authentifier. Pour ajouter une nouvelle règle d'authentification personnalisée à un ou plusieurs agents utilisateurs du rapport, cochez la case de chaque agent, puis cliquez sur **Create Rule (Créer une règle)**. Les agents utilisateurs sélectionnés apparaissent automatiquement dans le champ **Custom user agents (Agents utilisateurs personnalisés)** de la page Add Custom Authentication Rule (Ajouter une règle d'authentification personnalisée). Voir *Ajout de règles d'authentification personnalisées*, page 230.

Les rapports affichés dans le panneau de contenu ne peuvent pas être imprimés ni enregistrés dans un fichier. Pour imprimer ce rapport ou l'enregistrer dans un fichier, cliquez sur **Export to PDF (Exporter au format PDF)** ou **Export to XLS (Exporter au format XLS)** pour afficher le rapport dans le format de sortie approprié.

Important

Pour pouvoir afficher les rapports d'authentification au format PDF, Adobe Reader v7.0 ou une version ultérieure doit être installé dans l'ordinateur à partir duquel vous accédez à TRITON - Web Security.

Pour pouvoir afficher les rapports d'authentification au format XLS, Excel 2003 ou une version ultérieure doit être installé dans l'ordinateur à partir duquel vous accédez à TRITON - Web Security.

Chaque rapport indique la date et l'heure de sa dernière mise à jour. Les mises à jour ne sont pas automatiques : pour télécharger les données de rapport les plus récentes depuis le service hybride, cliquez sur **Update (Mettre à jour)**.

11 Filtrage des utilisateurs hors site

Rubriques connexes :

- *Fonctionnement du logiciel Remote Filtering*, page 238
- *Filtrage hybride des utilisateurs hors site*, page 242

En plus de filtrer les utilisateurs du réseau de votre organisation, les options des solutions de sécurité Web de Websense permettent de filtrer les utilisateurs hors du réseau.

- Pour surveiller l'activité Internet des utilisateurs situés à l'extérieur du réseau, installez le logiciel de filtrage à distance (Remote Filtering). Voir *Fonctionnement du logiciel Remote Filtering*, page 238.

  Remote Filtering est inclus dans les abonnements Websense Web Security Gateway Anywhere et est proposé sous forme d'option aux clients de Websense Web Filter, Websense Web Security et Websense Web Security Gateway.
- Le filtrage hybride vous permet de surveiller l'activité Internet des utilisateurs situés à l'extérieur du réseau, quel que soit le mode de filtrage qui leur est appliqué lorsqu'ils sont dans le réseau. Voir *Filtrage hybride des utilisateurs hors site*, page 242.

  Le filtrage hybride est uniquement disponible avec Websense Web Security Gateway Anywhere.

Ces méthodes permettent par exemple de filtrer les utilisateurs qui travaillent à domicile, ceux qui utilisent des ordinateurs portables professionnels lors de leurs déplacements, ou les étudiants qui utilisent des ordinateurs portables au sein et à l'extérieur du campus.

Important

Websense Web Security Gateway Anywhere vous permet d'exploiter le logiciel de filtrage à distance pour certains utilisateurs hors site et le filtrage hybride pour d'autres. Le service hybride ne permet cependant pas de surveiller l'activité Internet des ordinateurs dans lesquels le client Remote Filtering est également installé.

Fonctionnement du logiciel Remote Filtering

Rubriques connexes :

- *Lorsque la communication du serveur échoue*, page 239
- *Configuration des paramètres de Remote Filtering*, page 240

Par défaut, les composants de Remote Filtering surveillent le trafic HTTP, SSL et FTP et appliquent une stratégie basée sur les utilisateurs ou la stratégie Par défaut. Remote Filtering n'applique pas de stratégie aux adresses IP (plages d'ordinateurs ou réseau).

- Le filtrage basé sur la bande passante n'est pas appliqué aux clients du filtrage à distance, et la bande passante générée par le trafic du filtrage à distance n'est pas incluse dans les mesures et les rapports sur la consommation de la bande passante.
- Remote Filtering peut uniquement bloquer ou autoriser les requêtes FTP et SSL (HTTPS). Les sites FTP et HTTPS des catégories auxquelles est affectée une action de temps contingenté ou de confirmation sont bloqués lorsque l'utilisateur est à l'extérieur du réseau.
- Bien que Remote Filtering surveille systématiquement le trafic HTTP, vous pouvez le configurer pour qu'il ignore le trafic FTP, le trafic HTTPS ou les deux. Voir *Configuration du filtrage à distance pour ignorer le trafic FTP ou HTTPS*, page 241.

Remote Filtering comprend les composants suivants :

- **Remote Filtering Server** est installé au sein du pare-feu le plus éloigné du réseau et configuré de sorte que les ordinateurs filtrés hors du réseau puissent communiquer avec lui.
- Le client **Remote Filtering Client** est installé dans les ordinateurs Microsoft Windows utilisés à l'extérieur du réseau.

> **Remarque**
>
> Pour déployer ces composants, suivez attentivement les recommandations du Centre Installation et déploiement. Pour les installer, consultez le document technique Remote Filtering Software (Logiciel Remote Filtering).

Toutes les communications entre le client et le serveur Remote Filtering sont authentifiées et cryptées.

Par défaut, lorsqu'une demande HTTP, SSL ou FTP provient d'un ordinateur dans lequel le client Remote Filtering est installé :

1. Le client commence par déterminer si cet ordinateur est situé à l'intérieur ou à l'extérieur du réseau en envoyant une **pulsation** au serveur Remote Filtering dans la zone DMZ.
2. Si l'ordinateur est **à l'intérieur** du réseau, le client Remote Filtering ne déclenche aucune action. La requête est transmise à Network Agent ou à un produit d'intégration, puis est filtrée comme toute autre activité Internet provenant de l'intérieur du réseau.

3. Si l'ordinateur est **à l'extérieur** du réseau, le client Remote Filtering communique avec le serveur Remote Filtering via le port configuré (par défaut, 80).
4. Le serveur Remote Filtering contacte alors Filtering Service (installé à l'intérieur du réseau) pour identifier l'action à appliquer à la requête.
5. Filtering Service évalue la requête et envoie une réponse au serveur Remote Filtering.
6. Pour finir, le serveur Remote Filtering répond au client Remote Filtering en autorisant le site ou en envoyant le message de blocage approprié.

Lorsqu'il démarre pour la première fois, le client Remote Filtering crée un fichier journal qui surveille ses activités de filtrage, par exemple les entrées et les sorties du réseau, les échecs d'ouverture ou de fermeture et les redémarrages du client. Vous pouvez contrôler la présence et la taille de ce fichier journal. Voir *Configuration des paramètres de Remote Filtering*, page 240.

Vous trouverez des informations complètes sur la planification, le déploiement et la configuration du logiciel Remote Filtering dans le document technique Remote Filtering Software (Logiciel Remote Filtering), disponible sur notre portail support.websense.com.

Lorsque la communication du serveur échoue

Rubriques connexes :

- *Fonctionnement du logiciel Remote Filtering*, page 238
- *Configuration des paramètres de Remote Filtering*, page 240

Le filtrage intervient lorsqu'un client Remote Filtering, extérieur au réseau, réussit à communiquer avec le serveur Remote Filtering.

Vous pouvez configurer l'action appliquée par le client Remote Filtering lorsqu'il ne peut pas contacter le serveur Remote Filtering.

- Par défaut, le client Remote Filtering autorise toutes les requêtes HTTP, SSL et FTP tout en continuant de tenter de contacter le serveur Remote Filtering (échec d'ouverture). Dès que la communication est établie, la stratégie de filtrage appropriée est imposée.
- Lorsque le client Remote Filtering est configuré pour bloquer toutes les requêtes (échec de fermeture), une valeur d'expiration est appliquée (par défaut, 15 minutes). Ce compteur commence au démarrage de l'ordinateur distant. Le client Remote Filtering tente immédiatement de se connecter au serveur Remote Filtering et poursuit son cycle par l'intermédiaire des serveurs Remote Filtering disponibles jusqu'à ce qu'il réussisse.

  Si l'utilisateur a accès à Internet au démarrage, le filtrage n'intervient pas (toutes les requêtes sont autorisées) jusqu'à ce que le client Remote Filtering se connecte au serveur Remote Filtering.

  Si le client Remote Filtering ne peut pas se connecter pendant la période d'expiration configurée, l'accès Internet est bloqué (échec de fermeture) jusqu'à ce que la connexion au serveur Remote Filtering soit établie.

> **Remarque**
>
> Si, pour une raison ou une autre, le serveur Remote Filtering ne peut pas se connecter à Filtering Service, une erreur est renvoyée au client Remote Filtering et le filtrage reste sur Échec d'ouverture.

Cette période d'expiration permet aux utilisateurs qui payent l'accès Internet en déplacement de démarrer l'ordinateur et de disposer d'une connexion sans être bloqués. Si l'utilisateur n'accède pas à Internet avant l'expiration du délai de 15 minutes, l'accès à Internet ne peut pas être établi au cours de cette session. Dans ce cas, l'utilisateur doit redémarrer son ordinateur pour commencer un nouvel intervalle de délai d'expiration.

Pour modifier les paramètres qui définissent le blocage ou l'autorisation lorsque le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering et modifier la valeur d'expiration, consultez la section *Configuration des paramètres de Remote Filtering*, page 240.

Configuration des paramètres de Remote Filtering

Rubriques connexes :

- *Lorsque la communication du serveur échoue*, page 239
- *Configuration du filtrage à distance pour ignorer le trafic FTP ou HTTPS*, page 241
- *Configuration de l'intervalle des pulsations du client Remote Filtering*, page 242

La page **Paramètres > Général > Remote Filtering (Filtrage à distance)** permet de configurer les options qui affectent tous les clients Remote Filtering associés à cette installation.

Pour plus d'informations sur le fonctionnement de Remote Filtering, les composants impliqués et leur déploiement, consultez le document technique Remote Filtering Software (Logiciel Remote Filtering).

1. Cochez la case **Block all requests... (Bloquer toutes les requêtes)** pour empêcher les utilisateurs d'accéder à Internet lorsque le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering (échec de fermeture).

   Par défaut, les utilisateurs disposent d'un accès non filtré à Internet lorsque le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering (échec d'ouverture).

   Pour plus d'informations, consultez la section *Lorsque la communication du serveur échoue*, page 239.

2. Pour les clients Remote Filtering **v7.5.x** uniquement : si vous avez activé l'option de blocage de toutes les requêtes, définissez un **Intervalle d'expiration** (par défaut, 15 minutes). Pendant la période du délai d'expiration, toutes les requêtes HTTP, SSL et FTP sont autorisées.

Si le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering pendant l'intervalle d'expiration, l'accès Internet est bloqué jusqu'à ce que la communication soit rétablie.

L'activation de l'option **Aucun délai d'attente** peut verrouiller un ordinateur distant avant que l'utilisateur ne puisse établir une connexion Internet depuis un hôtel ou un fournisseur payant.

Avertissement

Websense, Inc. ne recommande pas d'utiliser l'option **Aucun délai d'attente**, ni de définir une période de délai trop basse.

3. Sélectionnez la **taille maximale** du fichier journal (en méga-octets) du client Remote Filtering (jusqu'à 10 Mo). Pour désactiver la journalisation, sélectionnez **Aucun journal**.

   Cette option contrôle la taille et l'existence du fichier journal créé par l'ordinateur distant lorsqu'il est initialement déconnecté du serveur Remote Filtering. Ce fichier journal surveille les événements suivants :

   - L'ordinateur quitte le réseau.
   - L'ordinateur rejoint le réseau.
   - Le client Remote Filtering redémarre.
   - Une condition d'échec d'ouverture se produit.
   - Une condition d'échec de fermeture se produit.
   - Le client Remote Filtering reçoit une mise à jour de stratégie.

   L'ordinateur conserve les deux journaux les plus récents. Ces journaux peuvent être utilisés pour dépanner des problèmes de connexion ou d'autres problèmes liés à Remote Filtering.

Configuration du filtrage à distance pour ignorer le trafic FTP ou HTTPS

Vous pouvez configurer Remote Filtering de sorte qu'il ignore le trafic FTP, le trafic HTTPS ou les deux. Le trafic HTTP est systématiquement surveillé.

Si vous utilisez plusieurs serveurs Remote Filtering, répétez cette procédure pour chaque instance.

1. Dans le serveur Remote Filtering, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
2. Ouvrez le fichier de configuration **securewispproxy.ini** dans un éditeur de texte.
3. Pour désactiver le filtrage FTP pour cette instance de Remote Filtering Server, ajoutez la ligne suivante dans ce fichier :

   ```
   FilterFTP=0
   ```

   Si, par la suite, vous voulez réactiver le filtrage FTP, remplacez la valeur « 0 » du paramètre par « 1 ».
4. Pour désactiver le filtrage HTTPS pour cette instance de Remote Filtering Server, ajoutez la ligne suivante dans ce fichier :

   ```
   FilterHTTPS=0
   ```

Si, par la suite, vous voulez réactiver le filtrage HTTPS, remplacez la valeur « 0 » du paramètre par « 1 ».

5. Enregistrez et fermez le fichier.
6. Redémarrez le service ou le démon Remote Filtering Server.

Configuration de l'intervalle des pulsations du client Remote Filtering

Pour déterminer s'il est situé à l'intérieur ou à l'extérieur du réseau, le client Remote Filtering envoie des pulsations au serveur Remote Filtering. Si la connexion des pulsations réussit, le client Remote Filtering sait qu'il est situé à l'intérieur du réseau. Par défaut, le client Remote Filtering continue à envoyer des pulsations toutes les 15 minutes afin de vérifier que son état n'a pas changé.

Si vous préférez que le client Remote Filtering envoie des pulsations plus fréquemment après avoir déterminé qu'il était situé à l'intérieur du réseau, vous pouvez augmenter cet intervalle de pulsations. Dans ce cas, le client Remote Filtering n'enverra de pulsations plus fréquentes que s'il enregistre une modification dans le réseau.

Pour modifier l'intervalle des pulsations :

1. Dans le serveur Remote Filtering, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
2. Ouvrez le fichier de configuration **securewisppproxy.ini** dans un éditeur de texte.
3. Localisez le paramètre **HeartbeatRetryInterval** et modifiez sa valeur. Par exemple :

   ```
   HeartbeatRetryInterval=360
   ```

   Dans cet exemple, des pulsations sont envoyées toutes les 360 minutes (6 heures).

   - La valeur définie peut correspondre à n'importe quel nombre de minutes compris entre 0 et 1440 (24 heures).
   - La valeur par défaut est 15 minutes.
4. Enregistrez et fermez le fichier.
5. Redémarrez le service ou le démon Remote Filtering Server.

Filtrage hybride des utilisateurs hors site

Rubriques connexes :

- *Configuration du filtrage hybride pour les utilisateurs hors site*, page 243
- *Auto-enregistrement des utilisateurs hors site*, page 243

Dans les déploiements Websense Web Security Gateway Anywhere, le filtrage hybride peut s'appliquer aux utilisateurs hors site, quel que soit le mode de filtrage dont ils font l'objet lorsqu'ils sont au sein du réseau.

- Pour les utilisateurs filtrés par les composants sur site (Filtering Service) lorsqu'ils sont à l'intérieur du réseau, vous pouvez configurer le fichier PAC du navigateur de sorte qu'il détermine si l'utilisateur est au sein du réseau ou hors site avant d'envoyer une requête Internet au filtrage.

  Si vous utilisez le fichier PAC généré par le service hybride, cette configuration intervient automatiquement conformément aux paramètres définis dans TRITON - Web Security.
- Pour les utilisateurs filtrés par le filtrage hybride au sein et à l'extérieur du réseau, aucune modification du fichier PAC n'est requise. Lorsqu'ils envoient une requête Internet, les utilisateurs hors site sont invités à se connecter au filtrage hybride de sorte que la stratégie d'utilisateur ou de groupe appropriée puisse être appliquée.

> **Important**
>
> Bien que vous puissiez exploiter le logiciel de filtrage à distance pour certains utilisateurs hors site et le filtrage hybride pour d'autres, le service hybride ne permet pas de surveiller l'activité Internet des ordinateurs dans lesquels le client Remote Filtering est également installé.

Configuration du filtrage hybride pour les utilisateurs hors site

Pour configurer le filtrage hybride des utilisateurs situés à l'extérieur d'un emplacement filtré :

- Si le filtrage hybride exploite les données d'un annuaire collectées par Websense Directory Agent pour identifier les utilisateurs, vous pouvez configurer le service hybride pour qu'il crée automatiquement un mot de passe de connexion hybride pour tous les comptes d'utilisateur envoyés par Directory Agent (voir *Envoi de données d'utilisateur et de groupe au service hybride*, page 220) ou laisser les utilisateurs demander leur propre mot de passe lorsqu'ils se connectent pour la première fois au service hybride à partir d'un emplacement non filtré (voir *Auto-enregistrement des utilisateurs hors site*, page 243).
- Si votre organisation n'exploite pas les données d'annuaire collectées par Directory Agent pour identifier les utilisateurs qui se connectent au service hybride, vous pouvez laisser les utilisateurs **s'auto-enregistrer** auprès du service. Voir *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214.
- Après avoir établi une stratégie d'identification des utilisateurs hors site, cochez la case **Enable off-site users (Activer les utilisateurs hors site)** dans la page **Paramètres > Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)** de TRITON - Web Security. Voir *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214.

Auto-enregistrement des utilisateurs hors site

Si vous n'envoyez pas les données d'un service d'annuaire au service hybride (en d'autres termes, si vous n'avez pas activé Directory Agent), les utilisateurs doivent s'auto-enregistrer pour être filtrés correctement lorsqu'ils sont hors site (à l'extérieur d'un emplacement filtré).

Pour que les utilisateurs soient autorisés à s'auto-enregistrer, vous devez d'abord identifier les domaines associés à votre organisation dans la page **Paramètres > Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)** de TRITON - Web Security (voir *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214).

Les utilisateurs qui se connectent au filtrage hybride à partir d'un emplacement non filtré sont invités à saisir un nom d'utilisateur et un mot de passe, ou à s'enregistrer. Pour s'enregistrer auprès du service hybride :

1. L'utilisateur fournit un nom et une adresse électronique.
2. Le filtrage hybride envoie alors un mot de passe à l'utilisateur par courrier électronique, de même qu'un lien qui permet de modifier ce mot de passe.
3. L'utilisateur clique sur ce lien et est invité à saisir le mot de passe.
4. L'enregistrement est terminé.

Lorsque les utilisateurs enregistrés se connectent au service hybride à partir d'un emplacement non filtré, ils doivent saisir leur adresse électronique et leur mot de passe. Le filtrage hybride applique alors la stratégie Par défaut de votre organisation à leurs requêtes Internet.

12 Protection des informations vitales

Websense Web Security protège votre entreprise contre les menaces provenant du Web, les problèmes de responsabilité légale et les pertes de productivité. Mais qu'en est-il lorsque vous souhaitez, ou devez, protéger des données sensibles, telles que des numéros de sécurité sociale ou de carte bancaire, contre toute fuite via le Web ? Ou si vous souhaitez surveiller de telles données dans des périphériques amovibles, des imprimantes, des messages instantanés, des opérations de copier/coller ou dans la messagerie ?

Pour vous protéger contre les pertes de données via le Web, vous pouvez déployer Websense Web Security Gateway Anywhere. Pour vous protéger contre les pertes de données via d'autres canaux, y compris le Web, vous pouvez acheter Websense Data Protect, Data Monitor, Data Discover, Data Endpoint ou la suite complète Data Security, en tant que compléments de votre logiciel de sécurité Web.

Les solutions de sécurité des données et du Web de Websense interagissent en profondeur, en fournissant au logiciel de sécurité l'accès aux informations sur les utilisateurs (collectées par User Service) et à la catégorisation des URL (à partir de la base de données principale).

En combinant la sécurité du Web et des données, vous pouvez créer des stratégies de prévention de perte de données (DLP) avec des règles basées sur les catégories d'URL. Par exemple, vous pouvez définir une règle stipulant que les numéros de carte bancaire ne peuvent pas être publiés dans des sites connus pour être frauduleux. Vous pouvez également définir des règles basées sur les utilisateurs et les ordinateurs, plutôt que sur les adresses IP. Par exemple, Jean Dupont ne peut pas publier des données financières dans des sites FTP.

Pour une description complète de la configuration de la protection contre les pertes de données via le Web, consultez notre portail Centre Installation et déploiement. Ce portail décrit l'installation, le déploiement et la configuration des divers composants, y compris Websense Content Gateway.

Pour obtenir des instructions sur la création des stratégies de sécurité des données, consultez l'Aide de TRITON - Data Security.

13 Réglage des stratégies de filtrage

Dans sa configuration la plus simple, le filtrage de l'activité Internet ne requiert qu'une seule stratégie appliquant un filtre de catégories et un filtre de protocoles 24 heures sur 24 et 7 jours sur 7. Websense propose toutefois des outils qui vont bien au-delà de ce filtrage de base pour obtenir le niveau de granularité dont vous avez précisément besoin pour gérer l'utilisation d'Internet dans votre entreprise. Vous pouvez :

- Créer des **filtres d'accès limité** pour bloquer l'accès à tous les sites à l'exception d'une liste de sites pour certains utilisateurs (voir *Limitation des utilisateurs à une liste définie d'URL*, page 247)
- Créer des **catégories personnalisées** permettant de redéfinir le filtrage des sites sélectionnés (voir *Fonctionnement des catégories*, page 254)
- **Recatégoriser des URL** pour déplacer des sites spécifiques de leur catégorie par défaut dans la base de données principale vers une autre catégorie définie par Websense ou personnalisée (voir *Redéfinition du filtrage pour des sites spécifiques*, page 260)
- Implémenter des restrictions de **bande passante** qui empêchent les utilisateurs d'accéder à des catégories et des protocoles autrement autorisés lorsque la consommation de la bande passante atteint un seuil défini (voir *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270)

  Dans les environnements Websense Web Security Gateway Anywhere, les restrictions basées sur la bande passante ne sont pas imposées aux utilisateurs du filtrage hybride.
- Définir des **mots-clés** utilisés pour bloquer des sites appartenant à des catégories autrement autorisées lorsque le blocage des mots-clés est activé (voir *Filtrage par mots-clés*, page 258)
- Définir des **types de fichiers** permettant de bloquer le téléchargement des types de fichiers sélectionnés appartenant à des catégories autrement autorisées lorsque le blocage des types de fichiers est activé (voir *Gestion du trafic en fonction du type de fichiers*, page 273)

Limitation des utilisateurs à une liste définie d'URL

Rubriques connexes :

- *Filtres d'accès limité et priorités du filtrage*, page 248
- *Création d'un filtre d'accès limité*, page 249
- *Modification d'un filtre d'accès limité*, page 250

Les filtres d'accès limité constituent une méthode de filtrage très précise. Chaque filtre d'accès limité est une liste d'URL ou d'adresses IP individuelles. Comme les filtres de catégories, les filtres d'accès limité sont ajoutés à des stratégies et imposés pendant une période définie. Lorsqu'un filtre d'accès limité est actif dans une stratégie, les utilisateurs affectés à cette stratégie ne peuvent visiter que les URL de la liste. Tous les autres sites sont bloqués.

Par exemple, si la stratégie Premier niveau impose un filtre d'accès limité incluant seulement certains sites de référence et d'enseignement, les étudiants régis par cette stratégie ne peuvent visiter que ces sites, et aucun autre.

Lorsqu'un filtre d'accès limité est actif, une page de blocage est renvoyée pour toute URL demandée non incluse dans ce filtre.

Websense peut prendre en charge jusqu'à 2 500 filtres d'accès limité contenant 25 000 URL au total.

Filtres d'accès limité et priorités du filtrage

Dans certains cas, plusieurs stratégies de filtrage peuvent s'appliquer à un même utilisateur. Cela se produit lorsqu'un utilisateur est membre de plusieurs groupes régis par des stratégies différentes.

Lorsque plusieurs stratégies de groupe s'appliquent à un utilisateur, le paramètre **Utiliser le blocage le plus restrictif** (voir *Ordre du filtrage*, page 95) détermine comment l'utilisateur est filtré. Par défaut, ce paramètre est désactivé.

Websense identifie le paramètre de filtrage le moins restrictif au niveau du filtre. Lorsqu'un utilisateur est filtré par plusieurs stratégies, dont l'une impose un filtre d'accès limité, « moins restrictif » peut se révéler difficile à interpréter.

Lorsque l'option **Utiliser le blocage le plus restrictif** est **OFF (Désactivée)** :

- Si le filtre de catégories **Bloquer tout** et un filtre d'accès limité peuvent s'appliquer, le filtre d'accès limité est toujours considéré comme le moins restrictif.
- Si un autre filtre de catégories et un filtre d'accès limité peuvent s'appliquer, le filtre de catégories est considéré comme le moins restrictif.

  Cela signifie que, même lorsque le filtre d'accès limité autorise le site alors que le filtre de catégories le bloque, le site est bloqué.

Lorsque l'option **Utiliser le blocage le plus restrictif** est **ON (Activée)**, un filtre d'accès limité est considéré comme moins restrictif que tout autre filtre de catégories, à l'exception de Bloquer tout.

Le tableau suivant résume les effets du paramètre **Utiliser le blocage le plus restrictif** sur le filtrage lorsque plusieurs stratégies peuvent s'appliquer :

	Option *Utiliser le blocage le plus restrictif* désactivée	**Option *Utiliser le blocage le plus restrictif* activée**
Filtre d'accès limité + Filtre de catégories **Bloquer tout**	Filtre d'accès limité (requête autorisée)	**Bloquer tout** (requête bloquée)
Filtre d'accès limité + Catégorie autorisée	Filtre de catégories (requête autorisée)	Filtre d'accès limité (requête autorisée)
Filtre d'accès limité + Catégorie bloquée	Filtre de catégories (requête bloquée)	Filtre d'accès limité (requête autorisée)
Filtre d'accès limité + Catégorie Temps contingenté/Confirmer	Filtre de catégories (requête limitée par Temps contingenté/Confirmer)	Filtre d'accès limité (requête autorisée)

Création d'un filtre d'accès limité

Rubriques connexes :

- *Fonctionnement des filtres*, page 59
- *Limitation des utilisateurs à une liste définie d'URL*, page 247
- *Modification d'un filtre d'accès limité*, page 250

Utilisez la page **Ajouter un filtre d'accès limité** (accessible via la page **Filtres** ou **Modifier la stratégie**) pour donner à votre nouveau filtre un nom unique et une description. Une fois le filtre créé, entrez une liste d'URL autorisées, affectez le filtre à une stratégie, puis appliquez cette dernière à des clients.

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

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

   Les noms de filtre peuvent comprendre des espaces, des tirets et des apostrophes.
2. Entrez une brève **Description** du filtre. Cette description apparaît à côté du nom du filtre dans la section Filtres d'accès limité de la page Filtres. Elle doit décrire l'objectif du filtre afin de simplifier la gestion ultérieure des stratégies par les administrateurs.

   Les restrictions de caractères qui s'appliquent aux noms des filtres s'appliquent également à leurs descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).
3. Pour voir et modifier le nouveau filtre, cliquez sur **OK**. Pour abandonner vos modifications et revenir à la page Filtres, cliquez sur **Annuler**.

Lorsque vous créez un nouveau filtre d'accès limité, il est ajouté dans la liste **Gestion des stratégies > Filtres > Filtres d'accès limité**. Cliquez sur le nom du filtre à modifier.

Pour finir de personnaliser votre nouveau filtre, continuez avec la section *Modification d'un filtre d'accès limité*.

Modification d’un filtre d’accès limité

Rubriques connexes :

- *Limitation des utilisateurs à une liste définie d’URL*, page 247
- *Filtres d’accès limité et priorités du filtrage*, page 248
- *Création d’un filtre d’accès limité*, page 249
- *Modification d’une stratégie*, page 93

Un filtre d’accès limité est une liste d’URL, d’adresses IP et d’expressions régulières, qui sert à identifier les sites Web spécifiques auxquels les utilisateurs peuvent accéder. Lorsque le filtre est appliqué à des clients, ces derniers ne peuvent visiter aucun autre site que ceux de cette liste.

Important

Lorsqu’une URL autorisée par un filtre d’accès limité est infectée par du code malveillant, les requêtes des utilisateurs pour ce site sont bloquées tant que les catégories Sécurité le sont également.

Pour obtenir des instructions sur la modification de ce comportement, consultez la section *Définition de la priorité de la catégorisation Risques de sécurité*, page 262.

La page **Gestion des stratégies > Filtres > Modifier le filtre d’accès limité** permet de modifier un filtre d’accès limité existant. Vous pouvez modifier le nom et la description du filtre, voir la liste des stratégies qui l’imposent et gérer les URL, les adresses IP et les expressions régulières incluses dans ce filtre.

Lorsque vous modifiez un filtre d’accès limité, les changements affectent toutes les stratégies qui imposent ce filtre.

1. Vérifiez le nom et la description du filtre. Pour modifier le nom du filtre, cliquez sur **Renommer**, puis entrez un nouveau nom. Ce nom est mis à jour dans toutes les stratégies qui imposent le filtre d’accès limité sélectionné.
2. Servez-vous du champ **Stratégies utilisant ce filtre** pour connaître le nombre de stratégies qui imposent actuellement ce filtre. Si une ou plusieurs stratégies l’appliquent, cliquez sur **Afficher les stratégies** pour en voir la liste.
3. Sous Ajouter ou supprimer des sites, entrez les URL et les adresses IP que vous souhaitez ajouter au filtre d’accès limité. Les adresses IP peuvent utiliser le format IPv4 ou IPv6.

   Entrez une URL ou une adresse IP par ligne.

   - Dans le cas des sites HTTP, il n’est pas nécessaire d’inclure le préfixe **http://**.
   - Lorsqu’un site HTTP est filtré en fonction de sa catégorie dans la base de données principale, Websense établit la correspondance entre l’URL et son adresse IP équivalente. Ce n’est pas le cas pour les filtres d’accès limité. Pour autoriser l’URL et l’adresse IP d’un site Web, ajoutez les deux dans le filtre.
   - Dans le cas des sites FTP et HTTPS, ajoutez le préfixe et fournissez l’adresse IP, plutôt que le nom d’hôte (domaine).

4. Cliquez sur la flèche droite (>) pour déplacer les URL et les adresses IP vers la liste des sites autorisés.
5. En plus d'ajouter des sites individuels au filtre d'accès limité, vous pouvez lui ajouter des expressions régulières qui correspondent à plusieurs sites. Pour créer des expressions régulières, cliquez sur **Avancé**.
   - Entrez une expression régulière par ligne, puis cliquez sur la flèche droite pour déplacer les expressions vers la liste des sites autorisés.
   - Pour vérifier qu'une expression régulière correspond aux sites prévus, cliquez sur **Tester**.
   - Pour plus d'informations sur l'utilisation d'expressions régulières pour le filtrage, consultez la section *Utilisation d'expressions régulières*, page 281.
6. Vérifiez les URL, les adresses IP et les expressions régulières dans la liste **Sites autorisés**.
   - Pour modifier un site ou une expression, sélectionnez son entrée, puis cliquez sur **Éditer**.
   - Pour retirer un site ou une expression de la liste, sélectionnez son entrée, puis cliquez sur **Supprimer**.
7. Après avoir modifié le filtre, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Filtres. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout de sites depuis la page Modifier la stratégie

Rubriques connexes :

- *Limitation des utilisateurs à une liste définie d'URL*, page 247
- *Filtres d'accès limité et priorités du filtrage*, page 248
- *Création d'un filtre d'accès limité*, page 249
- *Modification d'une stratégie*, page 93

La page **Stratégies > Modifier la stratégie > Ajouter des sites** permet d'ajouter des URL et des adresses IP à un filtre d'accès limité.

Entrez une URL ou une adresse IP par ligne. Si vous ne spécifiez pas de protocole, Websense ajoute automatiquement le préfixe **http://**.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier la stratégie. Cliquez également sur **OK** dans la page Modifier la stratégie pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Les modifications apportées à un filtre d'accès limité affectent toutes les stratégies qui imposent ce filtre.

Copie de filtres et de stratégies vers des rôles

Rubriques connexes :

- *Création d'un filtre de catégories*, page 60
- *Création d'un filtre de protocoles*, page 63
- *Création d'un filtre d'accès limité*, page 249
- *Création d'une stratégie*, page 92

Les Super administrateurs peuvent utiliser les pages **Filtres > Copier des filtres dans le rôle** et **Stratégies > Copier des stratégies dans le rôle** pour copier un ou plusieurs filtres ou stratégies vers un rôle d'administration déléguée. Une fois que le filtre ou la stratégie a été copié(e), les administrateurs délégués peuvent les utiliser pour filtrer leurs clients gérés.

- Dans le rôle cible, la mention « (Copié) » est ajoutée à la fin du nom du filtre ou de la stratégie. Un nombre est également ajouté si le même filtre ou la même stratégie est copié(e) plusieurs fois. Par exemple, « (Copié 2) ».
- Les administrateurs délégués peuvent renommer ou modifier les filtres et les stratégies qui ont été copiés dans leur rôle.
- Les filtres de catégories copiés dans un rôle d'administration déléguée définissent l'action de filtrage sur Autoriser pour les catégories personnalisées créées dans ce rôle. Il est préférable que les administrateurs délégués actualisent les filtres de catégories copiés afin de définir l'action désirée pour les catégories personnalisées propres à leur rôle.
- Les modifications apportées par un administrateur délégué à un filtre ou une stratégie copié(e) dans son rôle par un Super administrateur n'affectent pas le filtre ou la stratégie original(e) du Super administrateur, ni les autres rôles qui ont reçu une copie de ce filtre ou de cette stratégie.
- Les restrictions du verrouillage de filtre n'affectent pas le filtre ou la stratégie du Super administrateur, mais affectent la copie du filtre ou de la stratégie de l'administrateur délégué.
- Les administrateurs délégués étant régis par les restrictions du verrouillage de filtre, le filtre de catégories Autoriser tout et les filtres de protocoles ne peuvent pas être copiés dans un rôle d'administration déléguée.

Pour copier un filtre ou une stratégie :

1. Dans la page Copier des filtres dans le rôle ou Copier des stratégies dans le rôle, assurez-vous que les stratégies ou les filtres appropriés s'affichent dans la liste en haut de la page.
2. Utilisez la liste déroulante **Sélectionner un rôle** pour choisir le rôle de destination.
3. Cliquez sur **OK**.

   Une fenêtre contextuelle signale que les stratégies ou les filtres sélectionné(e)s sont copié(e)s. Le processus de copie peut prendre un certain temps.

   Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Lorsque le processus de copie est terminé, les stratégies ou les filtres copié(e)s seront à la disposition des administrateurs délégués dans le rôle sélectionné lors de leur prochaine connexion à TRITON - Web Security. Si un administrateur délégué est connecté au rôle pendant que les filtres ou les stratégies sont copié(e)s, il ne voit pas les nouveaux filtres ni les nouvelles stratégies avant de s'être déconnecté et reconnecté.

Construction de composants de filtres

La page **Gestion des stratégies > Composants de filtre** propose des outils qui permettent d'affiner et de personnaliser la façon dont Websense impose les stratégies d'accès à Internet de votre organisation. Les 3 boutons de l'écran sont associés aux tâches suivantes :

Modifier les catégories	• Recatégorisez une URL, (voir *Redéfinition du filtrage pour des sites spécifiques*, page 260). Par exemple, si votre stratégie de filtrage Internet bloque la catégorie Shopping, mais que vous souhaitez autoriser l'accès à certains sites de partenaires ou de fournisseurs, vous pouvez déplacer ces sites vers une catégorie autorisée telle que Commerce et économie. • Définissez ou modifiez des catégories personnalisées (voir *Création d'une catégorie personnalisée*, page 257). Créez des sous-catégories supplémentaires dans les catégories parentes définies par Websense ou dans la catégorie parente Définie par l'utilisateur, puis affectez des URL à ces nouvelles catégories. • Affectez des mots-clés à une catégorie (voir *Filtrage par mots-clés*, page 258). Pour recatégoriser et bloquer l'accès aux sites dont l'URL contient une chaîne spécifique, définissez d'abord des mots-clés, puis activez le blocage par mots-clés dans un filtre de catégories. • Créez des expressions régulières (voir *Utilisation d'expressions régulières*, page 281) ou des modèles pouvant correspondre à plusieurs URL et affectez-les à une catégorie.
Modifier les protocoles	Créez ou modifiez des définitions de protocole personnalisées (voir *Création d'un protocole personnalisé*, page 268, et *Modification des protocoles personnalisés*, page 266). Par exemple, si certains membres de votre organisation utilisent un outil de messagerie personnalisé, vous pouvez créer une définition de protocole personnalisée autorisant l'utilisation de cet outil tout en bloquant les autres protocoles de messagerie instantanée ou de conversation.
Types de fichiers	Créez ou modifiez les définitions de types de fichiers utilisées pour bloquer des fichiers associés à des extensions spécifiques appartenant à des catégories sinon autorisées (voir *Gestion du trafic en fonction du type de fichiers*, page 273).

Fonctionnement des catégories

Rubriques connexes :

- *Modification des catégories et de leurs attributs*, page 254
- *Création d'une catégorie personnalisée*, page 257
- *Filtrage par mots-clés*, page 258
- *Redéfinition du filtrage pour des sites spécifiques*, page 260

Websense fournit plusieurs méthodes pour filtrer les sites qui ne sont pas dans la base de données principale et pour modifier la manière dont les sites individuels de cette base de données sont filtrés.

- Pour un filtrage et des rapports plus précis, créez des **catégories personnalisées**.
- Servez-vous des **URL recatégorisées** pour définir les catégories des sites non classés ou pour modifier la catégorie des sites apparaissant dans la base de données principale.
- Définissez des **mots-clés** pour recatégoriser tous les sites dont l'URL contient une certaine chaîne.

Pour activer ou désactiver la journalisation des tentatives d'accès à une catégorie dans la base de données d'activité, consultez la section *Configuration du mode de journalisation des requêtes filtrées*, page 398. Lorsqu'une catégorie n'est pas journalisée, les requêtes des clients pour cette catégorie ne s'affichent pas dans les rapports.

Modification des catégories et de leurs attributs

Rubriques connexes :

- *Création d'une catégorie personnalisée*, page 257
- *Vérification de tous les attributs des catégories personnalisées*, page 255
- *Modification du filtrage global des catégories*, page 256
- *Filtrage par mots-clés*, page 258
- *Redéfinition du filtrage pour des sites spécifiques*, page 260

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories** permet de créer et de modifier des catégories personnalisées, des URL recatégorisées et des mots-clés.

Les catégories existantes, définies par Websense et personnalisées, sont énumérées dans la partie gauche du panneau de contenu. Pour voir les paramètres actuellement associés à une catégorie, ou pour créer de nouvelles définitions personnalisées, commencez par sélectionner une catégorie dans cette 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 plus d'informations, consultez la section *Vérification de tous les attributs des catégories personnalisées*, page 255.

- Pour créer une nouvelle catégorie, cliquez sur **Ajouter**, puis passez à la section *Création d'une catégorie personnalisée*, page 257, pour d'autres instructions.

  Pour retirer une catégorie personnalisée existante, sélectionnez-la, puis cliquez sur **Supprimer**. Vous ne pouvez pas supprimer les catégories définies par Websense.
- Pour modifier le nom ou la description d'une catégorie personnalisée, sélectionnez-la, puis cliquez sur **Renommer** (voir *Modification du nom d'une catégorie personnalisée*, page 256).
- Pour modifier l'action de filtrage associée à une catégorie dans tous les filtres de catégories, cliquez sur **Remplacer l'action** (voir *Modification du filtrage global des catégories*, page 256).
- La liste **URL recatégorisées** présente les sites recatégorisés (URL et adresses IP) affectés à cette catégorie.
  - Pour ajouter un site dans la liste, cliquez sur **Ajouter des URL**. Consultez la section *Redéfinition du filtrage pour des sites spécifiques*, page 260, pour plus d'instructions.
  - Pour modifier une catégorie recatégorisée existante, sélectionnez l'URL ou l'adresse IP, puis cliquez sur **Éditer**.
- La liste **Mots-clés** présente les mots-clés associés à cette catégorie.
  - Pour définir un mot-clé associé à la catégorie sélectionnée, cliquez sur **Ajouter des mots-clés**. Consultez la section *Filtrage par mots-clés*, page 258, pour plus d'instructions.
  - Pour modifier la définition d'un mot-clé existant, sélectionnez-le, puis cliquez sur **Éditer**.
- Outre les URL et les mots-clés, vous pouvez définir des **Expressions régulières** pour la catégorie. Chaque expression régulière est un modèle utilisé pour associer plusieurs sites à la catégorie.

  Pour voir ou créer des expressions régulières pour la catégorie, cliquez sur **Avancé**.
  - Pour définir une expression régulière, cliquez sur Ajouter des expressions (voir *Utilisation d'expressions régulières*, page 281).
  - Pour modifier une expression régulière existante, sélectionnez-la, puis cliquez sur **Éditer**.
- Pour retirer une URL, une expression régulière ou un mot clé recatégorisé(e), sélectionnez l'élément, puis cliquez sur **Supprimer**.

Lorsque vos modifications sont terminées dans la page Modifier les catégories, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Composants de filtre. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Vérification de tous les attributs des catégories personnalisées

La page **Composants de filtre > Modifier les catégories > Afficher l'ensemble des URL/mots-clés personnalisés** permet de revoir les définitions personnalisées d'URL, de mots-clés et d'expressions régulières. Vous pouvez également supprimer les définitions qui ne sont plus nécessaires.

La page présente trois tableaux similaires, un pour chaque attribut de catégorie : URL, mots-clés ou expressions régulières personnalisés. Dans chaque tableau, l'attribut est affiché à côté du nom de la catégorie à laquelle il est associé.

Pour retirer un attribut de catégorie, cochez la case appropriée, puis cliquez sur **Supprimer**.

Pour revenir à la page Modifier les catégories, cliquez sur **Fermer**. Si vous supprimez des éléments dans la page Afficher l'ensemble des URL/mots-clés personnalisés, cliquez sur **OK** dans la page Modifier les catégories pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Modification du filtrage global des catégories

La page **Composants de filtre** > **Modifier les catégories** > **Remplacer l'action** permet de modifier l'action appliquée à une catégorie dans tous les filtres de catégories existants. Elle permet également de déterminer l'action appliquée par défaut à la catégorie dans les nouveaux filtres.

Bien que cette modification remplace l'action appliquée à la catégorie dans tous les filtres existants, les administrateurs peuvent ensuite modifier ces filtres pour appliquer une action différente.

Avant de modifier les paramètres de filtrage appliqués à une catégorie, vérifiez que le nom de la catégorie appropriée s'affiche à côté de **Catégorie sélectionnée**. Vous pouvez ensuite :

1. Choisissez une nouvelle **Action** (Autoriser, Bloquer, Confirmer ou Temps contingenté). Pour plus d'informations, consultez la section *Actions de filtrage*, page 57.

   Par défaut, l'option **Ne pas modifier les paramètres actuels** est sélectionnée pour toutes les options de la page.
2. Spécifiez si vous souhaitez ou non **Bloquer des mots-clés**. Pour plus d'informations, consultez la section *Filtrage par mots-clés*, page 258.
3. Spécifiez ensuite si vous souhaitez ou non **Bloquer des types de fichiers**, puis personnalisez les paramètres du blocage. Pour plus d'informations, consultez la section *Gestion du trafic en fonction du type de fichiers*, page 273.
4. Sous **Filtrage avancé**, spécifiez si vous souhaitez ou non exploiter Bandwidth Optimizer pour gérer l'accès aux sites HTTP, puis personnalisez les paramètres du blocage. Pour plus d'informations, consultez la section *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.

   Important

   Les modifications apportées ici affectent tous les filtres de catégories existants, à l'exception des filtres **Bloquer tout** et **Autoriser tout**.
5. Cliquez sur **OK** pour revenir à la page Modifier les catégories (voir *Modification des catégories et de leurs attributs*, page 254). Pour mettre vos modifications en cache, cliquez sur **OK** dans la page Modifier les catégories.

Modification du nom d'une catégorie personnalisée

La page **Composants de filtre** > **Modifier les catégories** > **Renommer la catégorie** permet de modifier le nom et la description associés à une catégorie personnalisée.

- Utilisez le champ **Nom du filtre** pour modifier le nom de la catégorie. Le nouveau nom doit être unique et ne doit pas dépasser 50 caractères.

  Ce nom ne doit pas inclure les caractères suivants :

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

- Utilisez le champ **Description** pour modifier la description de la catégorie. La description ne doit pas dépasser 255 caractères.

  Les restrictions de caractères qui s'appliquent aux noms des filtres s'appliquent également à leurs descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier les catégories. Pour mettre vos modifications en cache, cliquez sur **OK** dans la page Modifier les catégories.

Création d'une catégorie personnalisée

Rubriques connexes :

- *Modification des catégories et de leurs attributs*, page 254
- *Filtrage par mots-clés*, page 258
- *Redéfinition du filtrage pour des sites spécifiques*, page 260

En plus des catégories définies par Websense et présentes dans la base de données principale (plus de 90), vous pouvez définir vos propres **catégories personnalisées** pour obtenir un filtrage et des rapports plus précis. Créez par exemple des catégories personnalisées telles que :

- **Voyage d'affaires**, pour regrouper des sites d'agences de voyage approuvées que les employés peuvent utiliser pour acheter leurs billets d'avion, louer une voiture et réserver un hôtel.
- **Matériaux de référence**, pour regrouper les sites d'encyclopédies et de dictionnaires en ligne considérés comme appropriés pour les élèves des écoles primaires.
- **Développement professionnel**, pour regrouper les sites de formation et d'autres ressources que les employés sont encouragés à utiliser pour développer leurs compétences.

La page **Gestion des stratégies** > **Composants de filtre** > **Modifier les catégories** > **Ajouter une catégorie** permet d'ajouter des catégories personnalisées à toute catégorie parente. Vous pouvez créer jusqu'à 100 catégories personnalisées.

1. Entrez un **Nom de catégorie** descriptif et unique. Ce nom ne doit pas inclure les caractères suivants :

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

2. Entrez la **Description** de la nouvelle catégorie.

   Les restrictions de caractères qui s'appliquent aux noms des filtres s'appliquent également à leurs descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).

3. Sélectionnez une catégorie parente dans la liste **Ajouter à**. Par défaut, l'option **Toutes les catégories** est sélectionnée.
4. Entrez les sites (URL ou adresses IP) à ajouter à cette catégorie. Pour plus d'informations, consultez la section *Redéfinition du filtrage pour des sites spécifiques*, page 260.

   Vous pourrez également modifier cette liste après la création de la catégorie.
5. Entrez les mots-clés que vous souhaitez associer à cette catégorie. Pour plus d'informations, consultez la section *Filtrage par mots-clés*, page 258.

   Vous pourrez également modifier cette liste après la création de la catégorie.

6. Définissez une **Action** de filtrage par défaut à appliquer à cette catégorie dans tous les filtres de catégories existants. Vous pourrez ensuite modifier cette action dans les filtres individuels.

   Remarque
   Les filtres de catégories copiés dans un rôle d'administration déléguée définissent l'action de filtrage sur Autoriser pour les catégories personnalisées créées dans ce rôle. Il est préférable que les administrateurs délégués actualisent les filtres de catégories copiés afin de définir l'action désirée pour les catégories personnalisées propres à leur rôle.

7. Activez éventuellement les actions de **Filtrage avancé** (blocage par mots-clés, par types de fichiers ou par bande passante) devant être appliquées à cette catégorie dans tous les filtres de catégories existants.
8. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Modifier les catégories. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

La nouvelle catégorie est ajoutée dans la liste des catégories et les informations d'URL personnalisées et de mots-clés de la catégorie s'affichent.

Filtrage par mots-clés

Rubriques connexes :

- *Redéfinition du filtrage pour des sites spécifiques*, page 260
- *Configuration des paramètres de filtrage de Websense*, page 67
- *Création d'un filtre de catégories*, page 60
- *Modification d'un filtre de catégories*, page 61
- *Fonctionnement des catégories*, page 254

Les mots-clés sont associés à des catégories, puis utilisés pour assurer une protection contre les sites qui n'ont pas été explicitement ajoutés dans la base de données principale ni définis comme URL personnalisée. L'activation du blocage par mots-clés comprend trois étapes :

1. Activez le blocage par mots-clés au niveau global (voir *Configuration des paramètres de filtrage de Websense*, page 67).
2. Définissez les mots-clés associés à une catégorie (voir *Définition des mots-clés*, page 259).
3. Activez le blocage par mots-clés pour la catégorie dans le filtre de catégories actif (voir *Modification d'un filtre de catégories*, page 61).

Lorsque des mots-clés ont été définis et le blocage par mots-clés activé pour une catégorie spécifique, Websense tente d'établir la correspondance du mot-clé pour chaque URL demandée, comme suit :

- Si le mot-clé contient uniquement des caractères ASCII, la correspondance du mot-clé est établie sur les parties domaine, chemin d'accès et requête d'une URL.

  Par exemple, si vous associez le mot-clé « nba » à la catégorie autorisée Sports, les URL suivantes sont bloquées :

  - sports.espn.go.com/**nba**/
  - moder**nba**kery.com
  - fashio**nba**r.com
- Si le mot-clé contient des caractères non ASCII, la correspondance du mot-clé est uniquement établie sur les parties chemin d'accès et requête de la chaîne.

  Par exemple, si vous associez le mot-clé « fútbol » à la catégorie autorisée Sports :

  - « www.**fútbol**.com » est **autorisé** (la partie domaine de l'URL n'a pas de correspondance).
  - « es.wikipedia.org/wiki/**Fútbol** » est **bloqué** (la partie chemin d'accès de l'URL a une correspondance).

Lorsqu'un site est bloqué par un mot-clé, il est recatégorisé en fonction de la correspondance du mot-clé. Les rapports présentent la catégorie du mot-clé et non la catégorie de la base de données principale pour ce site.

Définissez les mots-clés avec précaution afin d'éviter tout blocage non intentionnel.

> **Important**
> Évitez d'associer des mots-clés à l'une des sous-catégories de la protection étendue. Le blocage par mots-clés n'est en effet pas imposé pour ces catégories.

Lorsqu'une requête est bloquée par un mot-clé, la page de blocage Websense reçue par l'utilisateur le signale.

Définition des mots-clés

Rubriques connexes :

- *Modification d'un filtre de catégories*, page 61
- *Fonctionnement des catégories*, page 254
- *Filtrage par mots-clés*, page 258
- *Utilisation d'expressions régulières*, page 281

Un mot-clé est une chaîne de caractères (par exemple un mot, une phrase ou un acronyme) pouvant se trouver dans une URL. Affectez des mots-clés à une catégorie, puis activez le blocage par mots-clés dans un filtre de catégories.

La page **Gestion des stratégies > Composants de filtre > Modifier les catégories > Ajouter des mots-clés** permet d'associer des mots-clés à des catégories. Pour modifier la définition d'un mot-clé, utilisez la page **Modifier les mots-clés**.

Définissez les mots-clés avec précaution afin d'éviter tout blocage non intentionnel. Par exemple, si vous utilisez le mot clé « sex » pour bloquer l'accès aux sites réservés aux adultes, vous pouvez également bloquer les requêtes des moteurs de recherche pour des termes comme Sextuplé ou Ville d'Essex, et des sites comme m**sex**change.org (Informatique), vega**sex**perience.com (Voyage) et sci.esa.int/mar**sex**press (Institutions d'enseignement).

Entrez un mot-clé par ligne.

- N'insérez pas d'espaces dans les mots-clés. Les chaînes URL et CGI ne contiennent jamais d'espace entre les mots.
- Insérez une barre oblique inversée (\) avant les caractères spéciaux tels que :

  ```
  . , # ? * +
  ```

  Si vous n'insérez pas de barre oblique inversée, Websense ignore le caractère spécial.
- Évitez d'associer des mots-clés à l'une des sous-catégories de la protection étendue. Le blocage par mots-clés n'est en effet pas imposé pour ces catégories.

Lorsque les ajouts ou les modifications sont terminé(e)s, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Modifier les catégories. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Pour que le blocage par mots-clés soit imposé, vous devez également :

1. Activer le blocage par mots-clés via la page **Paramètres > Filtrage** (voir *Configuration des paramètres de filtrage de Websense*, page 67)
2. Activer le blocage par mots-clés dans un ou plusieurs filtres de catégories actifs (voir *Modification d'un filtre de catégories*, page 61)

Redéfinition du filtrage pour des sites spécifiques

Rubriques connexes :

- *Création d'une catégorie personnalisée*, page 257
- *Filtrage par mots-clés*, page 258
- *Redéfinition du filtrage pour des sites spécifiques*, page 260

Vous pouvez utiliser TRITON - Web Security pour modifier la catégorie affectée à un site. Les sites qui ont été ajoutés à une nouvelle catégorie sont appelés URL personnalisées ou URL recatégorisées.

- La page **Gestion des stratégies > Composants de filtre > Modifier les catégories > Recatégoriser les URL** permet d'ajouter des sites dans une nouvelle catégorie.
- Pour modifier les sites recatégorisés existants, utilisez la page **Modifier des URL**.

Cette fonction vous permet de :

- Affiner le filtrage des sites qui n'apparaissent pas dans la base de données principale Websense

  Par défaut, ces sites sont regroupés dans la catégorie **Divers\Non catégorisé**.

- Filtrer les sites autrement qu'en fonction de leur catégorie dans la base de données principale. Des sites peuvent être ajoutés dans :
  - Une autre catégorie définie par Websense
  - Une catégorie personnalisée quelconque (voir *Création d'une catégorie personnalisée*, page 257)
- Veillez à ce qu'un site récemment déplacé vers un nouveau domaine soit correctement filtré, en particulier lorsque les utilisateurs peuvent encore être envoyés vers la nouvelle URL via une redirection HTTP.

Une URL recatégorisée n'est pas bloquée par défaut. Elle est filtrée en fonction de l'action appliquée à sa nouvelle catégorie dans chaque filtre de catégories actif.

Important

Lorsqu'un site est reclassé dans une catégorie autorisée et est ensuite infecté par du code malveillant, les requêtes des utilisateurs pour ce site sont bloquées tant que les catégories Sécurité le sont également.

Pour obtenir des instructions sur la modification de ce comportement, consultez la section *Définition de la priorité de la catégorisation Risques de sécurité*, page 262.

Lorsque vous recatégorisez des sites :

- Entrez chaque URL ou adresse IP sur une ligne distincte.
  - Si un site est accessible via plusieurs URL, définissez chaque URL susceptible d'être utilisée pour accéder au site en tant qu'URL personnalisée pour vous assurer que ce site soit autorisé ou bloqué comme prévu.
  - Lorsque des URL recatégorisées sont filtrées, la correspondance de l'URL et de son adresse IP équivalente n'est pas établie automatiquement. Pour être sûr de bien filtrer le site, spécifiez à la fois son URL et son adresse IP.
- Incluez le protocole pour les sites non HTTP. Si vous ne précisez pas le protocole, Websense filtre le site en tant que site HTTP.

  Pour les sites HTTPS, incluez également le numéro de port (https://63.212.171.196:443/, https://www.onlinebanking.com:443/).
- Websense reconnaît les URL personnalisées exactement telles qu'elles ont été saisies. Si la catégorie Moteurs de recherche et portails est bloquée, mais que vous classez **www.yahoo.com** dans une catégorie autorisée, ce site n'est autorisé que si les utilisateurs tapent l'adresse complète. Si l'utilisateur tape images.search.yahoo.com ou seulement yahoo.com, le site reste bloqué. Toutefois, si vous recatégorisez **yahoo.com**, tous les sites dont l'adresse contient yahoo.com sont autorisés.

Lorsque l'ajout ou la modification des sites recatégorisés est terminé(e), cliquez sur **OK** pour revenir à la page Modifier les catégories. Cliquez également sur **OK** dans la page Modifier les catégories 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)**.

Websense recherche d'abord les définitions d'URL personnalisées pour un site avant de consulter la base de données principale. Il filtre donc le site en fonction de la catégorie affectée à l'URL recatégorisée.

Après avoir enregistré les URL recatégorisées, utilisez l'outil **Catégorie d'URL** situé dans le panneau de raccourcis à droite pour vérifier que le site est affecté à la catégorie appropriée. Voir *Utilisation de la boîte à outils pour vérifier le comportement du filtrage*, page 282.

Définition de la priorité de la catégorisation Risques de sécurité

Par défaut, lorsqu'un site est classé dans une catégorie Risques de sécurité, il est filtré en fonction de sa classification Risques de sécurité, y compris lorsque le site :

- Est ajouté en tant qu'URL recatégorisée dans une catégorie autorisée
- Apparaît dans un filtre d'accès limité

> **Remarque**
> Bien que les catégories de la protection étendue soient, par défaut, membres de la classe Risques de sécurité, comme elles regroupent des sites tout de même analysés, elles obtiennent une priorité plus faible que les autres catégories. En conséquence, la catégorisation personnalisée est toujours prioritaire sur celle de la protection étendue.

Lorsque Filtering Service ou le service hybride affecte un site à une catégorie de la classe Risques de sécurité (sur la base de la catégorie de la base de données principale ou de l'analyse de Content Gateway) :

- Lorsqu'un filtre de catégorie est en vigueur et que la catégorie liée à la sécurité est bloquée, le site est également bloqué.
- Lorsqu'un filtre d'accès limité est en vigueur, le site est bloqué.

Pour configurer les catégories appartenant à la classe Risques de sécurité, utilisez la page **Paramètres > Général > Classes de risque** dans TRITON - Web Security.

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) :

1. Dans l'ordinateur Filtering Service, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) et ouvrez le fichier de configuration **eimserver.ini** dans un éditeur de texte.
2. Localisez la section **[FilteringManager]** et ajoutez la ligne suivante :
   ```
   SecurityCategoryOverride=OFF
   ```
3. Enregistrez et fermez le fichier.
4. Redémarrez Filtering Service.
   - *Sous Windows* : utilisez la boîte de dialogue Services (Démarrer > Outils d'administration > Services) pour redémarrer Websense Filtering Service.
   - *Sous Linux* : utilisez la commande /opt/Websense/WebsenseDaemonControl pour arrêter et redémarrer Filtering Service.

Dans les environnements Websense Web Security Gateway Anywhere, vous pouvez également désactiver cette fonction pour le filtrage hybride :

1. Dans l'ordinateur Sync Service, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) et ouvrez le fichier de configuration **syncservice.ini** dans un éditeur de texte.
2. Si elle n'existe pas encore, ajoutez une section **[hybrid]**, puis le paramètre **SecurityCategoryOverride**, tel qu'indiqué ici :

   ```
   [hybrid]
   SecurityCategoryOverride=false
   ```

3. Enregistrez et fermez le fichier.
4. Redémarrez Sync Service.
   - *Sous Windows* : utilisez la boîte de dialogue Services (Démarrer > Outils d'administration > Services) pour redémarrer Websense Sync Service.
   - *Sous Linux* : utilisez la commande /opt/Websense/WebsenseDaemonControl pour arrêter et redémarrer Sync Service.

Blocage des publications destinées à des sites de certaines catégories

Par défaut, lorsque les utilisateurs sont autorisés à accéder à une catégorie, par exemple à Tableaux d'affichage et forums électroniques, ils peuvent à la fois afficher les sites de la catégorie et ajouter des publications.

Vous pouvez configurer Websense pour qu'il bloque les publications destinées à des sites de catégories spécifiques via le paramètre de configuration **BlockMessageBoardPosts**.

- Si ce paramètre est défini sur **ON**, les utilisateurs ne peuvent envoyer de publications qu'aux sites de la catégorie Tableaux d'affichage et forums électroniques.
- Ce paramètre peut également accepter une liste d'identifiants de catégorie séparés par des virgules (au format **112,122,151**). Dans ce cas, les utilisateurs ne peuvent pas publier dans les sites des catégories répertoriées.

Pour activer cette fonction pour les composants sur site :

1. Dans l'ordinateur Filtering Service, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) et ouvrez le fichier de configuration **eimserver.ini** dans un éditeur de texte.
2. Localisez la section **[WebsenseServer]** et ajoutez la ligne suivante :

   ```
   BlockMessageBoardPosts=<valeur>
   ```

   Ici, la <*valeur*> peut être **ON** ou une liste d'identifiants de catégorie séparés par des virgules.
3. Enregistrez et fermez le fichier.
4. Redémarrez Filtering Service.
   - *Sous Windows* : utilisez la boîte de dialogue Services (Démarrer > Outils d'administration > Services) pour redémarrer Websense Filtering Service.

- *Sous Linux* : utilisez la commande /opt/Websense/WebsenseDaemonControl pour arrêter et redémarrer Filtering Service.

Dans les environnements Websense Web Security Gateway Anywhere, pour activer cette fonction pour le filtrage hybride :

1. Dans l'ordinateur Sync Service, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) et ouvrez le fichier de configuration **syncservice.ini** dans un éditeur de texte.
2. Si elle n'existe pas encore, ajoutez une section **[hybrid]**, puis le paramètre **BlockMessageBoardPosts**, tel qu'indiqué ici :

   ```
   [hybrid]
   BlockMessageBoardPosts=<valeur>
   ```

   Ici, la <*valeur*> est une liste d'identifiants de catégorie séparés par des virgules.
3. Enregistrez et fermez le fichier.
4. Redémarrez Sync Service.
   - *Sous Windows* : utilisez la boîte de dialogue Services (Démarrer > Outils d'administration > Services) pour redémarrer Websense Sync Service.
   - *Sous Linux* : utilisez la commande /opt/Websense/WebsenseDaemonControl pour arrêter et redémarrer Sync Service.

Fonctionnement des protocoles

La base de données principale Websense contient les définitions utilisées pour filtrer les protocoles Internet autres que HTTP, HTTPS et FTP. Ces définitions comprennent les applications Internet et les méthodes de transfert de données, telles que celles utilisées pour la messagerie instantanée, la diffusion multimédia (streaming), le partage et le transfert de fichiers, la messagerie Internet et diverses autres opérations de base de données ou de réseau.

Ces définitions de protocoles peuvent même être utilisées pour filtrer les applications ou les protocoles qui contournent un pare-feu en créant un tunnel à travers les ports habituellement utilisés par le trafic HTTP. Les données de la messagerie instantanée, par exemple, peuvent pénétrer dans un réseau dont le pare-feu bloque les protocoles de messagerie instantanée en créant un tunnel via les ports HTTP. Websense identifie précisément ces protocoles et les filtre en fonction des stratégies que vous configurez.

Remarque

Dans les déploiements Websense Web Filter et Websense Web Security, l'agent Network Agent doit être installé pour que le filtrage à base de protocoles puisse s'effectuer.

Websense Web Security Gateway permet de filtrer les protocoles non HTTP qui effectuent une mise en tunnel via les ports HTTP sans utiliser Network Agent. Pour plus d'informations, consultez la section *Détection des protocoles mis en tunnel*, page 186.

Outre les définitions de protocole définies par Websense, vous pouvez définir des protocoles personnalisés pour votre filtrage. Les définitions de protocoles personnalisées peuvent être basées sur les adresses IP ou sur les numéros de port, et peuvent être modifiées.

Pour bloquer le trafic passant par un port spécifique, associez le numéro de ce port à un protocole personnalisé, puis attribuez à ce dernier l'action par défaut **Bloquer**.

Pour utiliser des définitions de protocoles personnalisées, sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Protocoles**. Pour plus d'informations, consultez les sections *Modification des protocoles personnalisés*, page 266, et *Création d'un protocole personnalisé*, page 268.

Filtrage des protocoles

Rubriques connexes :

- *Fonctionnement des protocoles*, page 264
- *Modification des protocoles personnalisés*, page 266
- *Création d'un protocole personnalisé*, page 268
- *Ajout ou modification d'identificateurs de protocole*, page 266
- *Ajout à un protocole défini par Websense*, page 270

Lorsque Network Agent est installé, ou dans le cas d'un déploiement Websense Web Security Gateway, Websense peut bloquer le contenu Internet transmis via certains ports ou certaines adresses IP, ou marqué par des signatures particulières, quelle que soit la nature des données. Par défaut, le blocage d'un port intercepte tout le contenu Internet pénétrant dans votre réseau par ce port, quelle qu'en soit la source.

Remarque

Il peut arriver que le trafic réseau interne envoyé via un port particulier ne soit pas bloqué, même lorsque le protocole qui utilise ce port l'est. Le protocole peut envoyer les données via un serveur interne plus vite que Network Agent ne peut capturer et traiter les données. Cela ne se produit pas avec les données provenant de l'extérieur du réseau.

Lorsqu'une requête de protocole intervient, Websense utilise la procédure suivante pour déterminer si elle doit être bloquée ou autorisée :

1. Il identifie le nom du protocole (ou de l'application Web).
2. Il identifie le protocole en fonction de l'adresse de destination demandée.
3. Il recherche des numéros de port ou des adresses IP associé(e)s dans les définitions de protocoles personnalisées.
4. Il recherche des numéros de port, des adresses IP ou des signatures associé(e)s dans les définitions de protocoles définies par Websense.

Si Websense ne trouve aucune de ces informations, l'ensemble du contenu associé au protocole est autorisé.

Modification des protocoles personnalisés

Rubriques connexes :

- *Fonctionnement des protocoles*, page 264
- *Création d'un protocole personnalisé*, page 268
- *Création d'un filtre de protocoles*
- *Modification d'un filtre de protocoles*
- *Fonctionnement des catégories*

La page **Gestion des stratégies > Composants de filtre > Modifier les protocoles** permet de créer et de modifier les définitions de protocoles personnalisées et de revoir les définitions de protocoles définies par Websense. Les définitions de protocoles définies par Websense ne sont pas modifiables.

La liste Protocoles comprend tous les protocoles personnalisés et définis par Websense. Cliquez sur un protocole ou sur un groupe de protocoles pour obtenir des informations sur l'élément sélectionné dans la partie droite du panneau de contenu.

Pour ajouter un nouveau protocole personnalisé, cliquez sur **Ajouter un protocole** et poursuivez l'opération avec la section *Création d'un protocole personnalisé*, page 268.

Pour modifier la définition d'un protocole :

1. Sélectionnez le protocole dans la liste Protocoles. La définition du protocole s'affiche à droite de la liste.
2. Cliquez sur **Remplacer l'action** pour modifier l'action de filtrage appliquée à ce protocole dans tous les filtres de protocoles (voir *Modification du filtrage global des protocoles*, page 267).
3. Cliquez sur **Ajouter un identificateur** pour définir d'autres identificateurs pour ce protocole (voir *Ajout ou modification d'identificateurs de protocole*, page 266).
4. Sélectionnez un identificateur dans la liste, puis cliquez sur **Éditer** pour modifier le **Port**, la **Plage d'adresses IP** ou la **Méthode de transport** défini(e) par cet identificateur.
5. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Pour retirer la définition d'un protocole, sélectionnez un élément dans la liste Protocoles, puis cliquez sur **Supprimer**.

Ajout ou modification d'identificateurs de protocole

La page **Composants de filtre > Modifier les protocoles > Ajouter un identificateur de protocole** permet de définir d'autres identificateurs pour un protocole personnalisé existant. Pour modifier un identificateur défini précédemment, utilisez la page **Modifier l'identificateur de protocole**.

Avant de créer ou de modifier un identificateur, vérifiez que le nom du protocole approprié s'affiche à côté de **Protocole sélectionné**.

Lorsque vous utilisez des identificateurs de protocole, n'oubliez pas qu'un critère au moins (port, adresse IP ou méthode de transport) doit être unique pour chaque protocole.

1. Spécifiez les **Ports** inclus dans cet identificateur.
   - Si vous sélectionnez **Tous les ports**, ce critère se superpose à tous les autres ports ou adresses IP saisi(e)s dans les autres définitions de protocoles.
   - Les plages de ports ne sont pas considérées comme uniques lorsqu'elles se chevauchent. Par exemple, la plage de ports 80-6000 chevauche la plage 4000-9000.
   - Soyez prudent(e) lorsque vous définissez un protocole sur le port 80 ou 8080, car Network Agent est à l'écoute des requêtes Internet sur ces ports.

     Vous pouvez configurer Network Agent pour ignorer ces ports en liaison avec un déploiement Websense Web Security Gateway.

     Les protocoles personnalisés étant prioritaires sur les protocoles Websense, si vous définissez un protocole personnalisé à l'aide du port 80, tous les autres protocoles qui utilisent le port 80 sont filtrés et journalisés comme le protocole personnalisé.
2. Spécifiez les **Adresses IP** incluses dans cet identificateur.
   - Si vous sélectionnez **Toutes les adresses IP externes**, ce critère se superpose à toutes les autres adresses IP saisies dans les autres définitions de protocoles.
   - Les plages d'adresses IP ne sont pas considérées comme uniques lorsqu'elles se chevauchent.
3. Spécifiez la méthode de **Transport de protocole** incluse dans cet identificateur.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Modifier les protocoles. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Modification du nom d'un protocole personnalisé

La page **Composants de filtre > Modifier les protocoles > Renommer un protocole** permet de modifier le nom d'un protocole personnalisé ou de le déplacer vers un autre groupe de protocoles.

- Utilisez le champ **Nom** pour modifier le nom du protocole. Le nouveau nom ne doit pas dépasser 50 caractères.

  Ce nom ne doit pas inclure les caractères suivants :

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```
- Pour déplacer le protocole vers un autre groupe, sélectionnez le nouveau groupe dans le champ **Dans le groupe**.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier les protocoles. Cliquez également sur **OK** dans la page Modifier les protocoles pour mettre vos modifications en cache.

Modification du filtrage global des protocoles

La page **Composants de filtre > Modifier les protocoles > Remplacer l'action** permet de modifier le filtrage d'un protocole dans tous les filtres de protocoles existants. Elle permet également de déterminer l'action appliquée par défaut au protocole dans les nouveaux filtres.

Bien que cette modification remplace l'action de filtrage appliquée dans tous les filtres de protocoles existants, les administrateurs peuvent ensuite modifier ces filtres pour appliquer une action différente.

1. Vérifiez que le nom du protocole approprié s'affiche à côté de **Protocole sélectionné**.
2. Sélectionnez une nouvelle **Action** (Autoriser ou Bloquer) à appliquer à ce protocole. Par défaut, l'option **Ne pas modifier l'action actuelle** est sélectionnée. Pour plus d'informations, consultez la section *Actions de filtrage*, page 57.
3. Définissez les nouvelles options de **Journalisation**. Le trafic des protocoles doit être journalisé pour apparaître dans les rapports et permettre les alertes d'utilisation de protocoles.
4. Précisez si **Bandwidth Optimizer** est utilisé pour gérer l'accès à ce protocole. Pour plus d'informations, consultez la section *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.

> **Important**
>
> Les modifications apportées ici affectent tous les filtres de protocoles existants, à l'exception des filtres **Bloquer tout** et **Autoriser tout**.

5. Lorsque vous avez terminé, cliquez sur **OK** pour revenir à la page Modifier les protocoles (voir *Modification des protocoles personnalisés*, page 266). Cliquez également sur **OK** dans la page Modifier les protocoles pour mettre vos modifications en cache.

Création d'un protocole personnalisé

Rubriques connexes :

- *Fonctionnement des protocoles*, page 264
- *Filtrage des protocoles*, page 265
- *Modification des protocoles personnalisés*, page 266
- *Ajout à un protocole défini par Websense*, page 270

La page **Composants de filtre** > **Protocoles** > **Ajouter un protocole** permet de définir un nouveau protocole personnalisé.

1. Entrez le **Nom** du protocole.

   Ce nom ne doit pas inclure les caractères suivants :

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

   Un protocole personnalisé peut porter le même nom qu'un protocole défini par Websense afin d'étendre le nombre d'adresses IP ou de ports associés au protocole original. Pour plus d'informations, consultez la section *Ajout à un protocole défini par Websense*, page 270.
2. Développez la liste déroulante **Ajouter un protocole à ce groupe** et sélectionnez un groupe de protocoles. Le nouveau protocole apparaît dans ce groupe pour tous les filtres et toutes les listes de protocoles.

3. Définissez un **Identificateur de protocole** unique (jeu de **ports**, d'**adresses IP** et de **méthodes de transport**) pour ce groupe. Vous pouvez par la suite ajouter d'autres identificateurs dans la page Modifier les protocoles.

   Pour créer des identificateurs de protocoles, suivez ces instructions :

   - Un critère au moins (port, adresse IP ou méthode de transport) doit être unique pour chaque définition de protocole.
   - Si vous sélectionnez **Tous les ports** ou **Toutes les adresses IP externes**, ce critère se superpose à tout autre port ou adresse IP saisi(e) dans les autres définitions de protocoles.
   - Les plages de ports ou d'adresses IP ne sont pas considérées comme uniques lorsqu'elles se chevauchent. Par exemple, la plage de ports 80-6000 chevauche la plage 4000-9000.

Remarque

Soyez prudent(e) lorsque vous définissez un protocole sur le port 80 ou 8080, car Network Agent est à l'écoute des requêtes Internet sur ces ports. (Dans les déploiements Websense Web Security Gateway, vous pouvez configurer Network Agent pour qu'il ignore ces ports.)

Les protocoles personnalisés étant prioritaires sur les protocoles Websense, si vous définissez un protocole personnalisé à l'aide du port 80, tous les autres protocoles qui utilisent le port 80 sont filtrés et journalisés comme le protocole personnalisé.

Le tableau suivant présente des exemples de définitions de protocole valides et non valides :

Port	Adresse IP	Méthode de transport	Combinaison acceptée ?
70	N'IMPORTE LAQUELLE	TCP	Oui - le numéro de port rend chaque identificateur de protocole unique.
90	N'IMPORTE LAQUELLE	TCP	

Port	Adresse IP	Méthode de transport	Combinaison acceptée ?
70	N'IMPORTE LAQUELLE	TCP	Non - les adresses IP ne sont pas uniques. L'adresse 10.2.1.201 fait partie de l'ensemble N'IMPORTE LAQUELLE.
70	10.2.1.201	TCP	

Port	Adresse IP	Méthode de transport	Combinaison acceptée ?
70	10.2.3.212	TCP	Oui - les adresses IP sont uniques.
70	10.2.1.201	TCP	

4. Sous Action par défaut, définissez l'action par défaut (**Autoriser** ou **Bloquer**) devant s'appliquer à ce protocole dans tous les filtres de protocoles actifs :
   - Indiquez si le trafic qui utilise ce protocole doit être **journalisé**. Le trafic des protocoles doit être journalisé pour apparaître dans les rapports et permettre les alertes d'utilisation de protocoles.
   - Indiquez si l'accès à ce protocole doit être régulé par **Bandwidth Optimizer** (voir *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270).
5. Lorsque vous avez terminé, cliquez sur **OK** pour revenir à la page Modifier les protocoles. La nouvelle définition de protocole apparaît dans la liste Protocoles.
6. Cliquez de nouveau sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout à un protocole défini par Websense

Vous ne pouvez pas ajouter directement un numéro de port ou une adresse IP dans un protocole défini par Websense. Vous pouvez cependant créer un protocole personnalisé portant le même nom que le protocole défini par Websense, puis ajouter des ports ou des adresses IP à sa définition.

Lorsqu'un protocole personnalisé et un protocole défini par Websense portent le même nom, Websense surveille le trafic des protocoles au niveau des adresses IP et des ports spécifiés dans les définitions des deux protocoles.

Dans les rapports, les noms des protocoles personnalisés sont précédés de « C_ ». Par exemple, si vous créez un protocole personnalisé pour SQL_NET et spécifiez des numéros de port supplémentaires, les rapports affichent C_SQL_NET lorsque le protocole utilise les numéros de port du protocole personnalisé.

Exploitation de Bandwidth Optimizer pour gérer la bande passante

Rubriques connexes :

- *Fonctionnement des catégories*, page 254
- *Fonctionnement des protocoles*, page 264
- *Configuration des limites par défaut de Bandwidth Optimizer*, page 272

Lorsque vous créez un filtre de catégories ou de protocoles, vous pouvez choisir de limiter l'accès à une catégorie ou à un protocole en fonction de l'utilisation de la bande passante.

- Bloquez l'accès aux catégories ou aux protocoles en fonction de l'utilisation totale de la bande passante du réseau.
- Bloquez l'accès aux catégories en fonction de la bande passante totale utilisée par le trafic HTTP.

- Bloquez l'accès à un protocole spécifique en fonction de la bande passante utilisée par ce protocole.

> **Remarque**
> Si vous utilisez Websense Web Security Gateway Anywhere, n'oubliez pas que le filtrage hybride n'impose pas les restrictions de bande passante.

Par exemple :

- Bloquez le protocole AOL Instant Messager (AIM) lorsque l'utilisation totale de la bande passante du réseau dépasse 50 % de la bande passante disponible, ou lorsque l'utilisation actuelle de la bande passante pour AIM dépasse 10 % de la bande passante totale du réseau.
- Bloquez la catégorie Sports lorsque l'utilisation totale de la bande passante du réseau atteint 75 %, ou lorsque la bande passante utilisée par l'ensemble du trafic HTTP atteint 60 % de la bande passante disponible.

L'utilisation de la bande passante d'un protocole comprend le trafic passant par tous les ports, adresses IP ou signatures défini(e)s pour ce protocole. Cela signifie que, lorsqu'un protocole ou une application Internet utilise plusieurs ports pour le transfert des données, le trafic traversant tous les ports inclus dans la définition du protocole est compté dans l'utilisation totale de la bande passante de ce protocole. Par contre, lorsqu'une application Internet utilise un port non inclus dans la définition du protocole, le trafic passant par ce port n'est pas inclus dans les mesures d'utilisation de la bande passante.

Websense enregistre la bande passante utilisée par les protocoles filtrés de type TCP et UDP.

Websense, Inc. actualise régulièrement les définitions des protocoles Websense pour assurer la précision des mesures de la bande passante.

Network Agent envoie les données de la bande passante du réseau à Filtering Service à intervalles prédéfinis. Websense surveille ainsi plus précisément l'utilisation de la bande passante et reçoit des mesures plus proches de la moyenne.

Dans un déploiement Websense Web Security Gateway, Content Gateway collecte les données de bande passante des protocoles FTP, HTTP et, lorsque cette option est activée, les protocoles individuels mis en tunnel sur HTTP (voir *Détection des protocoles mis en tunnel*, page 186). Les mesures et la génération des rapports sont similaires à ceux qu'utilise Network Agent. Vous pouvez définir les données utilisées pour déterminer le filtrage des protocoles selon la bande passante dans les paramètres de Bandwidth Optimizer.

1. Dans TRITON - Web Security, sélectionnez **Paramètres > Général > Filtrage**.
2. Cochez la case **Bandwidth Monitoring (Surveillance de la bande passante)**.
3. Lorsque vous avez terminé, 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)**.

Lorsque les options de filtrage par bande passante sont actives, Websense commence le filtrage de bande passante 10 minutes après la configuration initiale et 10 minutes après chaque redémarrage de Websense Policy Server. Ce délai assure une mesure précise des données de bande passante et de l'utilisation de ces données dans le filtrage.

Lorsqu'une requête est bloquée par des limites de bande passante, la page de blocage Websense affiche cette information dans le champ **Raison**. Pour plus d'informations, consultez la section *Pages de blocage*, page 115.

Configuration des limites par défaut de Bandwidth Optimizer

Rubriques connexes :

- *Modification d'un filtre de catégories*, page 61
- *Modification d'un filtre de protocoles*, page 64
- *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270

Avant de définir des paramètres de bande passante dans des stratégies, vérifiez les seuils de bande passante par défaut qui déclenchent le filtrage de la bande passante. Les valeurs définies par Websense sont :

- Bande passante par défaut du réseau : **50 %**
- Bande passante par défaut par protocole : **20 %**

Les valeurs de bande passante par défaut sont stockées par Policy Server et imposées par toutes les instances associées de Network Agent. Si vous utilisez plusieurs serveurs Policy Server, les modifications apportées aux valeurs de bande passante par défaut dans une instance de Policy Server n'affectent pas les autres instances de Policy Server.

Pour modifier les valeurs de bande passante par défaut :

1. Dans TRITON - Web Security, sélectionnez **Paramètres** > **Général** > **Filtrage**.
2. Entrez les seuils d'utilisation de bande passante qui déclenchent le filtrage de la bande passante lorsque ce type de filtrage est activé.
   - Lorsqu'une catégorie ou un protocole est bloqué(e) en fonction du trafic de l'ensemble du réseau, **Bande passante par défaut pour le réseau** définit le seuil de filtrage par défaut.
   - Lorsqu'une catégorie ou un protocole est bloqué(e) en fonction du trafic lié au protocole, **Bande passante par défaut par protocole** définit le seuil de filtrage par défaut.

   Vous pouvez remplacer les valeurs de seuil par défaut pour chaque catégorie ou protocole dans tous les filtres de protocoles ou de catégories.
3. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Toutes les modifications apportées aux valeurs par défaut ont un effet potentiel sur les filtres de catégories ou de protocoles qui imposent les restrictions de Bandwidth Optimizer.

- Pour gérer l'utilisation de la bande passante associée à un protocole particulier, modifiez le ou les filtres de protocoles actifs.
- Pour gérer l'utilisation de la bande passante associée à une catégorie d'URL particulière, modifiez le ou les filtres de catégories appropriés.

  Lorsque vous filtrez des catégories en fonction de l'utilisation de la bande passante HTTP, Websense mesure l'utilisation totale de la bande passante HTTP sur tous les sports spécifiés en tant que ports HTTP pour Websense.

Gestion du trafic en fonction du type de fichiers

Rubriques connexes :

- *Filtrage basé sur l'extension des fichiers*, page 274
- *Filtrage basé sur l'analyse des fichiers*, page 277
- *Fonctionnement des définitions des types de fichiers*, page 279
- *Ajout de types de fichiers personnalisés*, page 280
- *Ajout d'extensions à un type de fichiers*, page 280

Lorsque vous créez ou modifiez un filtre de catégories, vous pouvez configurer le blocage de type de fichier pour les catégories autorisées. Cette approche permet à votre organisation de limiter l'accès à des types de fichiers particuliers issus de sites Web de certaines catégories ou de toutes les catégories autorisées. Par exemple, vous pouvez autoriser l'accès à la catégorie Sports, tout en bloquant l'accès aux fichiers multimédia (audio et vidéo) de cette catégorie.

Le mode d'implémentation du blocage des types de fichiers dépend de votre solution Websense Web Security.

- Websense Web Filter et Websense Web Security (pas Content Gateway ni le proxy du service hybride) vous permettent de bloquer des types de fichiers en fonction de leur seule extension (voir *Filtrage basé sur l'extension des fichiers*, page 274).

  Par exemple :

  1. La catégorie E-mail général est autorisée dans le filtre de catégories actif, mais le blocage de type de fichier est activé pour les Fichiers compressés de la catégorie.
  2. Un utilisateur tente de télécharger un fichier d'extension .zip (par exemple « mon fichier.zip »).
  3. L'utilisateur obtient une page de blocage qui lui indique que le téléchargement a été bloqué du fait du type de fichier, car l'extension de fichier « .zip » est associée au type Fichiers compressés.

- Websense Web Security Gateway et Gateway Anywhere (Content Gateway et service hybride compris) autorisent un blocage de type de fichier en deux parties, combinant une extension de fichier (voir *Filtrage basé sur l'extension des fichiers*, page 274) et l'analyse des fichiers demandés (voir *Filtrage basé sur l'analyse des fichiers*, page 277).

  Par exemple :

  1. La catégorie E-mail général est autorisée dans le filtre de catégories actif, mais le blocage de type de fichier est activé pour les Fichiers compressés de la catégorie.
  2. Un utilisateur tente de télécharger un fichier d'extension .zip (par exemple « mon fichier.zip »).
  3. L'utilisateur obtient une page de blocage qui lui indique que le téléchargement a été bloqué du fait du type de fichier, car l'extension de fichier « .zip » est associée au type Fichiers compressés.

4. L’utilisateur tente de télécharger un autre fichier via le courrier électronique. L’extension de ce fichier n’est pas reconnue (par exemple, « monfichier.111 »).
5. L’analyse du fichier recherche son type.
   - Si l’analyse détermine que le fichier correspond à un format compressé, l’utilisateur obtient une page de blocage qui lui indique que le téléchargement est bloqué du fait du type de fichier.
   - Si l’analyse détermine que le fichier n’est pas compressé, la demande de téléchargement est autorisée.

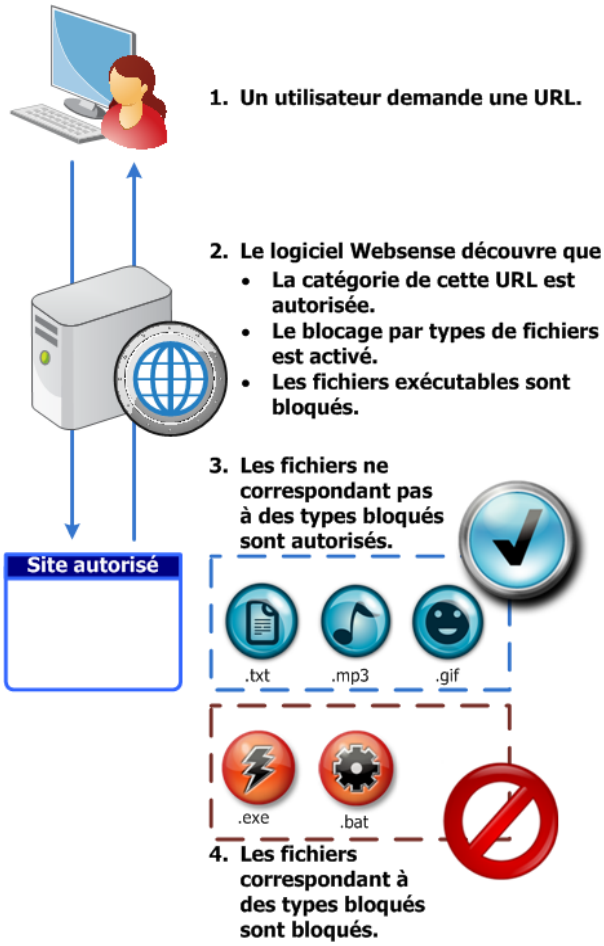
Pour implémenter un filtrage complet des supports Internet vidéo et audio, combinez un filtrage basé sur les protocoles avec un filtrage des types de fichiers. Le filtrage de protocoles traite le contenu diffusé en streaming, alors que le filtrage de types de fichiers traite les fichiers pouvant être téléchargés et lus.

Filtrage basé sur l’extension des fichiers

Rubriques connexes :

- *Activation du blocage des types de fichier dans un filtre de catégorie*, page 278
- *Fonctionnement des définitions des types de fichiers*, page 279
- *Ajout de types de fichiers personnalisés*, page 280
- *Ajout d’extensions à un type de fichiers*, page 280

Lorsque l’utilisateur demande une URL d’une catégorie autorisée pour laquelle le blocage de type de fichier est activé, Filtering Service examine les fichiers associés à l’URL pour voir si l’extension de l’un d’entre eux est affectée à un type de fichier bloqué. Dans l’affirmative, la requête est bloquée et l’utilisateur obtient une page de blocage qui lui indique que sa demande a été bloquée du fait du type du fichier.



Si l'extension n'est pas associée à un type de fichier bloqué, la suite dépend de votre solution Web Security :

- *Websense Web Security* et *Web Filter* : le fichier est autorisé.
- *Websense Web Security Gateway* et *Gateway Anywhere* : le fichier est analysé et son vrai type de fichier identifié, et la requête est ensuite autorisée ou bloquée en conséquence (voir *Filtrage basé sur l'analyse des fichiers*, page 277).

Plusieurs types de fichiers prédéfinis (groupes d'extensions de fichiers) sont inclus dans le produit. Ces définitions de types de fichiers sont stockées dans la base de données principale et peuvent être modifiées lors du processus de mise à jour de cette base de données.

Vous pouvez effectuer le filtrage à l'aide de types de fichiers prédéfinis, modifier les définitions de types de fichiers existantes et créer de nouveaux types de fichiers. Vous ne pouvez cependant pas supprimer les types de fichiers définis par Websense, ni les extensions de fichiers associées à ces derniers.

Toutes les extensions de fichiers associées à un type de fichier défini par Websense peuvent être ajoutées à un type de fichier personnalisé. L'extension de fichier est ensuite filtrée et journalisée en fonction des paramètres associés au type de fichier personnalisé.

Les définitions de types de fichiers peuvent contenir autant d'extensions de fichier que nécessaire pour le filtrage. Les types de fichiers définis par Websense, par exemple, comprennent les extensions suivantes :

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

Lorsqu'un utilisateur demande un site, Websense :

1. Détermine la catégorie de l'URL
2. Vérifie l'extension du fichier
3. (*Websense Web Security Gateway* et *Gateway Anywhere*) Si l'extension n'est pas bloquée, le fichier est analysé et son vrai type de fichier est identifié.

> **Remarque**
> Lorsque plusieurs stratégies de groupe peuvent s'appliquer à la requête d'un utilisateur, le blocage du type de fichier n'est pas effectué.

Lorsqu'un utilisateur tente d'accéder à un type de fichier bloqué, le champ **Raison** de sa page de blocage Websense indique que ce type de fichier a été bloqué (voir *Pages de blocage*, page 115).

La page de blocage standard ne s'affiche pas lorsqu'une image bloquée se compose d'une partie seulement de page autorisée, mais la zone de l'image s'affiche vide. Cela permet d'éviter l'affichage d'une petite partie de page de blocage en plusieurs emplacements d'une page sinon autorisée.

Pour afficher les définitions de types de fichiers existantes, modifier des types de fichiers ou créer des types de fichiers personnalisés pour le filtrage selon l'extension, sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Types de fichiers**. Pour plus d'informations, consultez la section *Fonctionnement des définitions des types de fichiers*, page 279.

Pour activer le blocage des types de fichier, consultez la section *Activation du blocage des types de fichier dans un filtre de catégorie*, page 278.

Filtrage basé sur l'analyse des fichiers

Rubriques connexes :

- *Activation du blocage des types de fichier dans un filtre de catégorie*, page 278
- *Risques de sécurité : Analyse des fichiers*, page 188

Si le trafic des utilisateurs passe par Websense Content Gateway ou par le service hybride, les fichiers demandés sont analysés de sorte que leur type soit défini lorsque tous les éléments suivants sont vrais :

1. L'utilisateur demande une URL appartenant à une catégorie autorisée.
2. Dans le filtre de catégories actif, le blocage de type de fichier est activé pour la catégorie.
3. Aucune extension de fichier ne correspond à un type de fichier bloqué (voir *Filtrage basé sur l'extension des fichiers*, page 274).

Dans ce cas, le type de fichier renvoyé pour le filtrage décrit l'objet ou le comportement des fichiers similaires, indépendamment de l'extension. En conséquence, l'analyse du type de fichier interdit toute tentative de dissimulation de fichier exécutable via l'attribution d'une extension « .txt » ou d'une autre extension inoffensive.

Les définitions de types de fichier sont gérées dans les bases de données d'analyse et peuvent être modifiées dans le cadre du processus de mise à jour de Content Gateway ou du service hybride.

Les types de fichier identifiés par l'analyse des fichiers sont les suivants :

Type de fichier	Description
Fichiers compressés	Fichiers mis en package pour occuper moins d'espace, tels que les archives ZIP, RAR ou JAR
Documents	Documents au format binaire, tels que DOCX ou PDF
Exécutables	Programmes exécutables dans votre ordinateur, tels que les fichiers EXE ou BAT
Images	Formats d'image, tels que JPG, BMP et GIF
Multimédia	Formats audiovisuels, tels que MP3, WMV et MOV
Applications Internet multimédia	Applications Web s'exécutant dans un navigateur, par exemple Flash
Texte	Fichiers de texte non mis en forme, tels que les fichiers HTML et TXT
Menaces	Applications dangereuses pour votre ordinateur ou votre réseau, telles que les logiciels espions, les vers ou les virus

Lorsqu'un utilisateur demande un site, les solutions Websense Web Security Gateway commencent par identifier la catégorie du site, puis vérifient les types de fichier filtrés (d'abord sur la base de l'extension, puis de l'analyse).

> **Remarque**
>
> Lorsque plusieurs stratégies de groupe peuvent s'appliquer à la requête d'un utilisateur, le blocage du type de fichier n'est pas effectué.

Lorsqu'un utilisateur tente d'accéder à un type de fichier bloqué, le champ **Raison** de sa page de blocage Websense indique que ce type de fichier a été bloqué (voir *Pages de blocage*, page 115).

La page de blocage standard ne s'affiche pas lorsqu'une image bloquée se compose d'une partie seulement de page autorisée, mais la zone de l'image s'affiche vide. Cela permet d'éviter l'affichage d'une petite partie de page de blocage en plusieurs emplacements d'une page sinon autorisée.

Pour afficher les extensions existantes d'un type de fichier, modifier des types de fichiers ou créer des types de fichiers personnalisés pour le filtrage selon l'extension, sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Types de fichiers**. Pour plus d'informations, consultez la section *Fonctionnement des définitions des types de fichiers*, page 279.

Pour activer le blocage des types de fichier, consultez la section *Activation du blocage des types de fichier dans un filtre de catégorie*, page 278.

Activation du blocage des types de fichier dans un filtre de catégorie

Pour que les utilisateurs ne puissent pas accéder à certains types de fichier normalement autorisés par les catégories :

1. Ouvrez la page **Gestion des stratégies > Filtres** et cliquez sur le nom d'un filtre de catégorie.

   Notez que vous pouvez également modifier les filtres de catégorie via une stratégie.
2. Sélectionnez une catégorie dans la liste **Catégories**.
3. Cochez la case **Bloquer des types de fichiers** située sous Filtrage avancé sur le côté droit de la page.

   La liste des types de fichier s'affiche.
4. Servez-vous des cases à cocher pour sélectionner un ou plusieurs types de fichiers à bloquer.
5. Pour bloquer les types de fichier sélectionnés dans toutes les catégories autorisées par ce filtre de catégorie, cliquez sur **Apply to All Categories (Appliquer à toutes les catégories)**.
6. Cliquez sur **OK**, puis sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Fonctionnement des définitions des types de fichiers

Rubriques connexes :

- *Gestion du trafic en fonction du type de fichiers*, page 273
- *Modification d'un filtre de catégories*, page 61
- *Filtrage d'un site*, page 98

La page **Gestion des stratégies > Composants de filtre > Modifier les types de fichiers** vous permet de créer et de gérer jusqu'à 32 types de fichiers (groupes d'extensions de fichier) pouvant être explicitement bloqués dans les filtres de catégorie (voir *Gestion du trafic en fonction du type de fichiers*, page 273).

Important

Les types de fichier personnalisés et les ajouts personnalisés apportés aux types prédéfinis sont utilisés dans le filtrage basé sur l'extension, mais pas dans l'analyse du véritable type de fichier de Websense Web Security Gateway ou de Gateway Anywhere. Pour plus d'informations, consultez *Filtrage basé sur l'extension des fichiers*, page 274, et *Filtrage basé sur l'analyse des fichiers*, page 277.

- Cliquez sur un type de fichiers pour voir les extensions qui lui sont associées.
- Pour ajouter des extensions au type de fichiers sélectionné, cliquez sur **Ajouter des extensions**, puis passez à la section *Ajout d'extensions à un type de fichiers*, page 280, pour d'autres instructions.
- Pour créer un nouveau type de fichiers, cliquez sur **Ajouter un type de fichier**, puis passez à la section *Ajout de types de fichiers personnalisés*, page 280, pour d'autres instructions.
- Pour retirer une extension ou un type de fichiers personnalisé, sélectionnez un élément, puis cliquez sur **Supprimer**.

  Vous ne pouvez pas supprimer les types de fichiers définis par Websense ni les extensions de fichiers associées à ces derniers.

  Vous pouvez cependant ajouter les extensions de fichiers associées à un type de fichiers défini par Websense à un type de fichiers personnalisé. L'extension de fichier est ensuite filtrée et journalisée en fonction des paramètres associés au type de fichier personnalisé. Vous ne pouvez pas ajouter la même extension à plusieurs types de fichiers personnalisés.

Lorsque vos modifications sont terminées, cliquez sur **OK**. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout de types de fichiers personnalisés

La page **Composants > Modifier les types de fichiers > Ajouter un type de fichier** permet de définir des types de fichiers personnalisés.

> **Important**
>
> Les types de fichier personnalisés et les ajouts personnalisés apportés aux types prédéfinis sont utilisés dans le filtrage basé sur l'extension, mais pas dans l'analyse du véritable type de fichier de Websense Web Security Gateway ou de Gateway Anywhere. Pour plus d'informations, consultez *Filtrage basé sur l'extension des fichiers*, page 274, et *Filtrage basé sur l'analyse des fichiers*, page 277.

1. Entrez un **Nom de type de fichier** unique.

   Vous pouvez créer un type de fichiers personnalisé portant le même nom qu'un type de fichiers défini par Websense pour ajouter d'autres extensions au type de fichiers existant.
2. Entrez les extensions de fichier, une par ligne, dans la liste **Extensions de fichier**. Il n'est pas nécessaire d'ajouter le point (« . ») avant chaque extension.
3. Cliquez sur **OK** pour revenir à la page Modifier les types de fichiers. Le nouveau type de fichier apparaît dans la liste Types de fichier.
4. Lorsque vos modifications sont terminées, cliquez sur **OK** dans la page Modifier les types de fichiers. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout d'extensions à un type de fichiers

La page **Composants de filtre > Modifier les types de fichiers > Ajouter des extensions de fichier** permet d'ajouter des extensions de fichier au type de fichiers sélectionné.

> **Important**
>
> Les types de fichier personnalisés et les ajouts personnalisés apportés aux types prédéfinis sont utilisés dans le filtrage basé sur l'extension, mais pas dans l'analyse du véritable type de fichier de Websense Web Security Gateway ou de Gateway Anywhere. Pour plus d'informations, consultez *Filtrage basé sur l'extension des fichiers*, page 274, et *Filtrage basé sur l'analyse des fichiers*, page 277.

1. Vérifiez que le nom du type de fichiers approprié s'affiche à côté de **Type de fichier sélectionné**.
2. Entrez les extensions de fichier, une par ligne, dans la liste **Extensions de fichier**. Il n'est pas nécessaire d'ajouter le point (« . ») avant chaque extension.
3. Cliquez sur **OK** pour revenir à la page Modifier les types de fichiers. Les nouvelles extensions de fichier apparaissent dans la liste Personnaliser des extensions de fichiers.
4. Lorsque vos modifications sont terminées, cliquez sur **OK** dans la page Modifier les types de fichiers. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Utilisation d'expressions régulières

Une **expression régulière** est un modèle utilisé pour remplacer plusieurs chaînes ou groupes de caractères. Vous pouvez utiliser des expressions régulières dans des filtres d'accès limité ou pour définir des mots-clés ou des URL personnalisé(e)s. Filtering Service s'efforce ensuite de trouver une correspondance au modèle général plutôt qu'à un seul mot-clé ou à une seule URL spécifique.

Prenons l'exemple de cette simple expression régulière :

```
domaine.(com|org|net)
```

Ce modèle d'expression correspond aux URL :

- domaine.com
- domaine.org
- domaine.net

Les expressions régulières doivent être utilisées avec précaution. Elles sont un puissant outil de filtrage mais peuvent facilement conduire à un blocage excessif ou trop permissif. De même, les expressions régulières mal construites peuvent entraîner un filtrage excessif.

Important

L'utilisation d'expressions régulières comme critères de filtrage peut accroître la surcharge du processeur. Selon les tests, 100 expressions régulières augmentent de 20 % l'utilisation moyenne du processeur dans l'ordinateur Filtering Service.

Comme pour les mots-clés, lorsqu'une expression régulière contient des caractères non ASCII, la correspondance de l'expression est uniquement établie sur les parties chemin d'accès et requête de l'URL, pas sur le domaine (« www.domaine.com/**chemin?requête** »).

Websense prend en charge la syntaxe des expressions régulières Perl, à deux exceptions près. La partie de la syntaxe non prise en charge est a priori inutile pour les correspondances de chaînes détectées dans une URL.

La syntaxe des expressions régulières non prise en charge comprend :

```
(?{code})
??{code})
```

Pour plus d'informations sur les expressions régulières, consultez les sites :

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

Utilisation de la boîte à outils pour vérifier le comportement du filtrage

Dans TRITON - Web Security, le panneau de raccourcis droit comprend une **Boîte à outils** qui vous permet de vérifier rapidement la configuration de votre filtrage.

Cliquez sur le nom d'un outil pour y accéder. Cliquez de nouveau sur le nom pour afficher la liste des outils. Pour plus d'informations sur l'utilisation d'un outil, consultez :

- *Catégorie d'URL*, page 282
- *Vérifier la stratégie*, page 282
- *Tester le filtrage*, page 283
- *Accès à l'URL*, page 283
- *Analyser l'utilisateur*, page 283

Vous pouvez également cliquer sur **Portail de support** pour accéder au site Web du support technique de Websense dans un nouvel onglet ou une nouvelle fenêtre du navigateur. Notre Portail de support vous permet d'utiliser notre base de connaissances pour accéder à des articles, des conseils, des didacticiels, des vidéos et de la documentation sur votre produit.

Catégorie d'URL

Pour savoir comment un site est actuellement classé :

1. Cliquez sur **Catégorie d'URL** dans la boîte à outils.
2. Entrez une URL ou une adresse IP.
3. Cliquez sur **Ok**.

La catégorie actuelle du site s'affiche dans une fenêtre contextuelle. Si votre organisation a recatégorisé cette URL, la nouvelle catégorie s'affiche.

La catégorisation du site peut varier selon la version de la base de données principale utilisée (y compris des mises à jour en temps réel).

Vérifier la stratégie

Servez-vous de cet outil pour identifier les stratégies s'appliquant à un client spécifique. Les résultats ne concernent que l'heure et la date en cours.

1. Cliquez sur **Vérifier la stratégie** dans la boîte à outils.
2. Pour identifier un annuaire ou un client ordinateur, entrez :
   - Un nom d'utilisateur complet

     Pour localiser l'utilisateur dans l'annuaire, cliquez sur **Rechercher un utilisateur** (voir *Identification d'un utilisateur pour vérifier la stratégie ou tester le filtrage*, page 284).
   - Une adresse IP
3. Cliquez sur **Ok**.

Le nom d'une ou plusieurs stratégies s'affiche dans une fenêtre contextuelle. Plusieurs stratégies s'affichent lorsque aucune d'elles n'a été affectée à l'utilisateur alors que des stratégies ont été affectées à plusieurs groupes, domaines ou unités d'organisation dont l'utilisateur est membre.

Même lorsque plusieurs stratégies apparaissent, une seule s'applique à l'utilisateur à un moment donné (voir *Ordre du filtrage*, page 95).

Tester le filtrage

Pour savoir ce qu'il se passe lorsqu'un client spécifique demande un site particulier :

1. Cliquez sur **Tester le filtrage** dans la boîte à outils.
2. Pour identifier un annuaire ou un client ordinateur, entrez :
   - Un nom d'utilisateur complet

     Pour localiser l'utilisateur dans l'annuaire, cliquez sur **Rechercher un utilisateur** (voir *Identification d'un utilisateur pour vérifier la stratégie ou tester le filtrage*, page 284).
   - Une adresse IP
3. Entrez l'URL ou l'Adresse IP du site à vérifier.
4. Cliquez sur **Ok**.

La catégorie du site, l'action appliquée à cette catégorie et la raison de l'action apparaissent dans une fenêtre contextuelle.

Accès à l'URL

Pour savoir si des utilisateurs ont tenté d'accéder à un site au cours des deux dernières semaines, date du jour comprise :

1. Cliquez sur **Accès à l'URL** dans la boîte à outils.
2. Entrez une partie ou la totalité de l'URL ou de l'adresse IP du site à vérifier.
3. Cliquez sur **Ok**.

Un rapport d'investigation montre si des utilisateurs ont accédé à ce site et, dans l'affirmative, à quel moment.

Vous pouvez utiliser cet outil après réception d'une alerte de sécurité afin de voir si votre organisation a été exposée au phishing ou à des sites infectés par des virus.

Analyser l'utilisateur

Pour découvrir l'historique de l'activité Internet d'un utilisateur au cours des deux dernières semaines, date du jour non comprise :

1. Cliquez sur **Analyser l'utilisateur** dans la boîte à outils.
2. Saisissez un nom d'utilisateur complet ou partiel (si le filtrage par utilisateur est activé) ou l'adresse IP (pour les ordinateurs dans lesquels les utilisateurs ne sont pas identifiés).

   La recherche d'adresse IP ne présente de résultats que pour les noms d'utilisateur qui n'ont pas été journalisés.
3. Cliquez sur **Ok**.

L'historique de l'utilisation du client apparaît dans un rapport d'investigation.

Identification d’un utilisateur pour vérifier la stratégie ou tester le filtrage

Utilisez la page **Rechercher un utilisateur** pour identifier un client utilisateur (annuaire) pour l’outil Vérifier la stratégie ou Tester le filtrage.

La page s’ouvre avec l’option **Utilisateur** sélectionnée. Développez le dossier **Entrées de l’annuaire** pour parcourir votre annuaire, ou cliquez sur **Rechercher**. La fonction de recherche n’est disponible que si vous utilisez un service d’annuaire de type LDAP.

Pour rechercher un utilisateur dans l’annuaire :

1. Entrez une partie ou la totalité du **Nom** de l’utilisateur.
2. Développez l’arborescence **Entrées de l’annuaire** et localisez un contexte de recherche.

   Pour définir le contexte, vous devez cliquer sur un dossier (DC, OU ou CN). Le champ situé sous l’arborescence est alors renseigné.
3. Cliquez sur **Rechercher**. Les entrées correspondant à votre terme de recherche apparaissent sous **Résultats de la recherche**.
4. Cliquez sur un nom d’utilisateur pour sélectionner un utilisateur ou sur **Rechercher encore** pour entrer un nouveau terme de recherche ou un nouveau contexte.

   Pour parcourir à nouveau l’annuaire, cliquez sur **Annuler la recherche**.
5. Lorsque le nom d’utilisateur complet approprié s’affiche dans le champ **Utilisateur**, cliquez sur **Ok**.

Si vous utilisez l’outil Tester le filtrage, assurez-vous qu’une URL ou une adresse IP s’affiche dans le champ **URL** avant de cliquer sur **Ok**.

Pour identifier un client ordinateur plutôt qu’un utilisateur, cliquez sur **Adresse IP**.

14 Identification des utilisateurs

Pour appliquer des stratégies à des utilisateurs et des groupes, Websense doit pouvoir identifier l'utilisateur à l'origine d'une requête, en fonction de l'adresse IP d'origine. Plusieurs méthodes d'identification sont disponibles :

- Une application ou un périphérique d'intégration identifie et authentifie les utilisateurs, puis transmet les informations de cet utilisateur à Websense. Pour plus d'informations, consultez le Centre Installation et déploiement.
- Un agent d'identification transparente Websense fonctionne en arrière-plan pour communiquer avec un service d'annuaire et identifier les utilisateurs (voir *Identification transparente*).
- Websense demande aux utilisateurs leurs identifiants réseau, en les invitant à se connecter lorsqu'ils ouvrent un navigateur Web (voir *Authentification manuelle*, page 287).

Dans les environnements Websense Web Security Gateway Anywhere, le service hybride doit pouvoir identifier les utilisateurs pour appliquer les stratégies basées sur les utilisateurs et les groupes. Il n'utilise pas les informations fournies par User Service ou les agents d'identification transparente. À la place, les méthodes suivantes sont disponibles :

- Un composant appelé Websense Directory Agent collecte les informations qui servent à identifier les utilisateurs (voir *Identification des utilisateurs du filtrage hybride*, page 311).
- Websense Web Endpoint est installé dans les ordinateurs clients pour assurer une authentification transparente, imposer l'utilisation du filtrage hybride et transmettre les informations d'authentification au service hybride.
- Websense Authentication Service assure une authentification transparente par l'intermédiaire d'un ordinateur virtuel hébergé dans votre réseau et communiquant avec votre service d'annuaire.

Identification transparente

Rubriques connexes :

- *Authentification manuelle*, page 287
- *Configuration des méthodes d'identification des utilisateurs*, page 287

En général, **l'identification transparente** décrit la méthode dont se sert Websense pour identifier les utilisateurs de votre service d'annuaire sans leur demander d'informations de connexion. Cela comprend l'intégration dans Websense d'un périphérique ou d'une application fournissant les informations des utilisateurs à employer pour le filtrage, ou l'utilisation des agents d'identification transparente de Websense en option.

- Websense *DC Agent*, page 295 est utilisé avec un service d'annuaire de type Windows. Cet agent interroge régulièrement les contrôleurs de domaine sur les sessions de connexion des utilisateurs et les ordinateurs clients pour vérifier l'état des connexions. Il s'exécute dans un serveur Windows et peut être installé dans n'importe quel domaine du réseau.
- Websense *Logon Agent*, page 300 identifie les utilisateurs lorsqu'ils se connectent à des domaines Windows. L'agent s'exécute dans un serveur Linux ou Windows, mais son application de connexion associée s'exécute uniquement dans des ordinateurs Windows.
- Websense *RADIUS Agent*, page 303 peut être combiné aux services d'annuaire de type Windows ou LDAP. Cet agent fonctionne avec un serveur et un client RADIUS pour identifier les utilisateurs qui se connectent à partir d'emplacements distants.
- Websense *eDirectory Agent*, page 304 est utilisé avec Novell eDirectory. Cet agent utilise l'authentification Novell eDirectory pour mapper les utilisateurs avec les adresses IP.

Pour plus d'informations sur l'installation de chaque agent, consultez le Centre Installation et déploiement. L'agent peut être utilisé seul ou dans certaines combinaisons.

Les paramètres généraux d'identification des utilisateurs et les agents d'identification transparente spécifiques sont configurés dans TRITON - Web Security. Ouvrez la page **Paramètres > Général >Identification des utilisateurs**.

Pour obtenir des instructions détaillées sur la configuration, consultez la section *Configuration des méthodes d'identification des utilisateurs*, page 287.

Il arrive parfois que Websense ne puisse pas obtenir les informations des utilisateurs auprès d'un agent d'identification transparente. Cela peut se produire lorsque plusieurs utilisateurs emploient le même ordinateur, si l'utilisateur est un utilisateur invité ou anonyme, ou encore pour d'autres raisons. Dans ce cas, vous pouvez inviter l'utilisateur à se connecter par l'intermédiaire du navigateur (voir *Authentification manuelle*, page 287).

Identification transparente des utilisateurs distants

Dans certaines configurations, Websense peut identifier de manière transparente les utilisateurs qui se connectent à votre réseau à partir d'emplacements distants :

- Si vous avez déployé le serveur Websense Remote Filtering et le client Remote Filtering, Websense peut identifier les utilisateurs hors site qui se connectent à un domaine mis en cache à l'aide d'un compte de domaine. Pour plus d'informations, consultez la section *Filtrage des utilisateurs hors site*, page 237.
- Si vous avez déployé DC Agent, et que les utilisateurs distants se connectent directement à des domaines Windows nommés de votre réseau, DC Agent peut les identifier (voir *DC Agent*, page 295).
- Si vous utilisez un serveur RADIUS pour authentifier les utilisateurs qui se connectent à partir d'emplacements distants, RADIUS Agent peut les identifier de façon transparente de sorte que vous puissiez appliquer des stratégies de filtrage basées sur les utilisateurs ou les groupes (voir *RADIUS Agent*, page 303).

Authentification manuelle

Rubriques connexes :

- *Identification transparente*, page 285
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289
- *Authentification manuelle sécurisée*, page 292
- *Configuration des méthodes d'identification des utilisateurs*, page 287

L'identification transparente n'est pas toujours disponible ou souhaitable dans tous les environnements. Lorsque les organisations n'utilisent pas l'identification transparente, ou lorsque celle-ci n'est pas disponible, vous pouvez tout de même effectuer le filtrage en fonction des stratégies basées sur les utilisateurs et les groupes grâce à l'**authentification manuelle**.

L'authentification manuelle invite les utilisateurs à saisir un nom d'utilisateur et un mot de passe lors de leur première connexion à Internet via un navigateur. Websense confirme ensuite le mot de passe avec le service d'annuaire pris en charge, puis récupère les informations de stratégies liées à cet utilisateur.

Vous pouvez configurer Websense de manière à activer l'authentification manuelle chaque fois que l'identification transparente n'est pas disponible (voir *Configuration des méthodes d'identification des utilisateurs*, page 287, et *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214).

Vous pouvez également créer une liste d'ordinateurs spécifiques associés à des paramètres d'authentification personnalisée pour lesquels les utilisateurs sont invités à se connecter lorsqu'ils ouvrent un navigateur (voir *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289).

Lorsque l'authentification manuelle est activée, l'utilisateur peut recevoir une erreur HTTP et ne pas réussir à accéder à Internet dans les cas suivants :

- Il a saisi à trois reprises un mot de passe incorrect. Cela se produit lorsque le nom d'utilisateur ou le mot de passe n'est pas valide.
- Il clique sur **Annuler** pour contourner la demande d'authentification.

Lorsque l'authentification manuelle est activée, les utilisateurs qui ne peuvent pas s'identifier se voient refuser l'accès à Internet.

Configuration des méthodes d'identification des utilisateurs

Rubriques connexes :

- *Identification transparente*, page 285
- *Authentification manuelle*, page 287
- *Fonctionnement avec des utilisateurs et des groupes*, page 74

La page **Paramètres > Général >Identification utilisateur** permet de définir le moment et la manière dont Websense tente d'identifier les utilisateurs du réseau pour imposer les stratégies destinées aux groupes et aux utilisateurs.

- Configurez Policy Server pour qu'il communique avec les agents d'identification transparente.
- Vérifiez et actualisez les paramètres des agents d'identification transparente.
- Définissez une règle globale déterminant la réponse de Websense lorsque les utilisateurs ne peuvent pas être identifiés par un agent d'identification transparente ni par un périphérique d'intégration.
- Identifiez les ordinateurs de votre réseau auxquels les règles globales d'identification des utilisateurs ne s'appliquent pas, et précisez si leurs utilisateurs doivent être authentifiés et comment.

Si vous utilisez les agents d'identification transparente de Websense, ils sont répertoriés sous **Agents d'identification transparente** :

- **Serveur** présente l'adresse IP ou le nom de l'ordinateur qui héberge l'agent d'identification transparente.
- **Port** présente le port utilisé par Websense pour communiquer avec cet agent.
- **Type** indique si l'instance spécifiée est un agent DC Agent, Logon Agent, RADIUS Agent ou eDirectory Agent. (Consultez la section *Identification transparente*, page 285, pour la présentation de chaque type d'agent.)

Pour ajouter un agent, sélectionnez le type d'agent dans la liste déroulante **Ajouter un agent**. Cliquez sur l'un des liens suivants pour obtenir des instructions sur la configuration :

- *Configuration de DC Agent*, page 296
- *Configuration de Logon Agent*, page 301
- *Configuration de RADIUS Agent*, page 303
- *Configuration d'eDirectory Agent*, page 305

Pour supprimer une instance d'agent, cochez la case accolée aux informations de l'agent dans la liste, puis cliquez sur **Supprimer**.

Si vous utilisez une ou plusieurs instances de DC Agent, sous DC Agent Domains and Controllers (Domaines et contrôleurs DC Agent), cliquez sur **View Domain List (Afficher la liste des domaines)** pour obtenir des informations sur les contrôleurs de domaine actuellement interrogés par les agents. Pour plus d'informations, consultez la section *Vérification des domaines et contrôleurs de domaine interrogés par DC Agent*, page 299.

Sous **User Identification Exceptions (Exceptions à l'identification des utilisateurs)**, répertoriez les adresses IP des ordinateurs devant utiliser d'autres paramètres d'identification des utilisateurs que le reste de votre réseau.

Par exemple, si vous utilisez un agent d'identification transparente ou un produit d'intégration pour identifier vos utilisateurs et que vous avez activé l'authentification manuelle pour inviter les utilisateurs à saisir leurs informations d'identification lorsqu'ils ne peuvent pas être identifiés de manière transparente, vous pouvez identifier des ordinateurs spécifiques dans lesquels :

- Les utilisateurs qui ne peuvent pas être identifiés ne sont jamais invités à saisir leurs informations d'identification. En d'autres termes, lorsque l'identification transparente échoue, l'authentification manuelle n'est pas proposée et la stratégie du réseau ou de l'ordinateur, ou la stratégie Par défaut, s'applique.

- Les informations des utilisateurs sont toujours ignorées, même lorsqu'elles sont disponibles, et les utilisateurs sont toujours invités à saisir leurs identifiants.
- Les informations des utilisateurs sont toujours ignorées, même lorsqu'elles sont disponibles, et les utilisateurs ne sont jamais invités à saisir leurs identifiants (la stratégie de l'ordinateur ou du réseau, ou la stratégie Par défaut, est toujours appliquée).

Pour créer une exception, cliquez sur **Ajouter**, puis consultez la section *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289. Pour supprimer une exception, cochez la case accolée à la plage ou à l'adresse IP, puis cliquez sur **Supprimer**.

Sous **Options d'authentification supplémentaires**, définissez la réponse par défaut de Websense lorsque les utilisateurs ne sont pas identifiés de manière transparente (par un agent ou un périphérique d'intégration) :

- Cliquez sur **Appliquer la stratégie de l'ordinateur ou du réseau** pour ignorer les stratégies basées sur les utilisateurs et les groupes au profit des stratégies basées sur les ordinateurs et le réseau ou de la stratégie Par défaut.
- Cliquez sur **Inviter l'utilisateur à fournir des informations de connexion** pour obliger les utilisateurs à fournir leurs identifiants de connexion lorsqu'ils ouvrent un navigateur. Les stratégies destinées aux utilisateurs et aux groupes peuvent ensuite être appliquées (voir *Authentification manuelle*, page 287).
- Définissez le **Contexte de domaine par défaut** que Websense doit employer chaque fois qu'un utilisateur est invité à saisir ses identifiants de connexion. Il s'agit du domaine dans lequel les identifiants de connexion des utilisateurs sont valides.

  Si vous utilisez la liste Exceptions pour définir les ordinateurs avec lesquels les utilisateurs sont invités à saisir des identifiants de connexion, vous devez fournir un contexte de domaine par défaut, même si la règle globale consiste à appliquer une stratégie basée sur l'ordinateur ou le réseau.

Lorsque vos modifications sont terminées dans cette page, cliquez sur **OK** pour les mettre en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Définition de règles d'authentification pour des ordinateurs spécifiques

Rubriques connexes :

- *Configuration des méthodes d'identification des utilisateurs*, page 287
- *Authentification manuelle*, page 287
- *Authentification manuelle sécurisée*, page 292

L'authentification sélective vous permet de déterminer si les utilisateurs qui demandent un accès à Internet à partir d'un ordinateur client spécifique (identifié par son adresse IPv4 ou IPv6) sont invités à saisir leurs identifiants de connexion via le navigateur. Cette option peut être utilisée pour :

- Établir des règles d'authentification différentes pour un ordinateur situé dans une borne publique que celles des employés de l'organisation fournissant la borne de connexion
- Garantir que les utilisateurs d'un ordinateur de salle d'examen situé dans un cabinet médical soient toujours identifiés avant d'accéder à Internet

Les ordinateurs auxquels s'appliquent des paramètres particuliers d'identification sont répertoriés dans la page **Paramètres > Général > Identification des utilisateurs**. Cliquez sur **Exceptions** pour définir des paramètres d'identification spécifiques pour certains ordinateurs de votre réseau ou pour voir si des paramètres particuliers ont été définis pour un ordinateur spécifique.

Pour ajouter un ordinateur à la liste, cliquez sur **Ajouter**, puis passez à la section *Définition d'exceptions dans les paramètres d'identification des utilisateurs*, page 290, pour d'autres instructions.

Lorsque vous avez terminé d'ajouter des ordinateurs ou des plages réseau à la liste, cliquez sur **OK**. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Définition d'exceptions dans les paramètres d'identification des utilisateurs

Rubriques connexes :

- *Identification transparente*, page 285
- *Authentification manuelle*, page 287
- *Configuration des méthodes d'identification des utilisateurs*, page 287

La page **Identification des utilisateurs > Ajouter des adresses IP** vous permet d'identifier les ordinateurs auxquels des règles d'identification spécifiques doivent s'appliquer.

1. Entrez une **Adresse IP** ou une **Plage d'adresses IP** au format IPv4 ou IPv6 permettant d'identifier les clients auxquels une méthode d'authentification spécifique doit s'appliquer, puis cliquez sur la flèche droite pour les ajouter dans la liste **Sélectionné**.

   Si les mêmes règles doivent s'appliquer à plusieurs ordinateurs, ajoutez-les tous dans la liste.
2. Sélectionnez une entrée dans la liste déroulante **Identification des utilisateurs** pour indiquer si Websense doit tenter d'identifier les utilisateurs de ces ordinateurs de manière transparente.
   - Sélectionnez **Essayer d'identifier l'utilisateur de façon transparente** pour récupérer les informations des utilisateurs auprès d'un agent d'identification transparente ou d'un périphérique d'intégration.
   - Sélectionnez **Ignorer les informations de l'utilisateur** pour ne pas utiliser de méthode transparente pour l'identification des utilisateurs.
3. Indiquez si les utilisateurs doivent être invités à saisir leurs identifiants de connexion via le navigateur. Ce paramètre s'applique lorsque les informations des utilisateurs ne sont pas disponibles, soit parce qu'une autre identification a échoué, soit parce que les informations des utilisateurs ont été ignorées.
   - Sélectionnez **Appliquer la stratégie de l'ordinateur ou du réseau** pour que les utilisateurs ne soient jamais invités à fournir leurs identifiants de connexion.

Si l'option « Essayer d'identifier l'utilisateur de façon transparente » est également sélectionnée, les utilisateurs dont les identifiants de connexion peuvent être vérifiés de façon transparente sont filtrés par la stratégie d'utilisateurs appropriée.

- Sélectionnez **Inviter l'utilisateur à fournir des informations de connexion** pour obliger les utilisateurs à fournir leurs identifiants de connexion, puis spécifiez le **Contexte de domaine par défaut** à utiliser (le cas échéant).

  Si l'option « Essayer d'identifier l'utilisateur de façon transparente » est également sélectionnée, les utilisateurs reçoivent une invite du navigateur uniquement s'ils n'ont pas été identifiés de manière transparente.

4. Cliquez sur **OK** pour revenir à la page Identification des utilisateurs.
5. Lorsque la mise à jour de la liste Exceptions est terminée, 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)**.

Vérification des exceptions aux paramètres d'identification des utilisateurs

Rubriques connexes :

- *Identification transparente*, page 285
- *Authentification manuelle*, page 287
- *Configuration des méthodes d'identification des utilisateurs*, page 287

La page **Paramètres > Identification des utilisateurs > Modifier des adresses IP** permet de modifier les entrées de la liste Exceptions. Les modifications apportées dans cette page affectent tous les ordinateurs (identifiés par une adresse ou par une plage d'adresses IP) apparaissant dans la liste Sélectionné.

1. Sélectionnez une entrée dans la liste déroulante **Identification des utilisateurs** pour indiquer si Websense doit tenter d'identifier les utilisateurs de ces ordinateurs de manière transparente.
   - Sélectionnez **Essayer d'identifier l'utilisateur de façon transparente** pour récupérer les informations des utilisateurs auprès d'un agent d'identification transparente ou d'un périphérique d'intégration.
   - Sélectionnez **Ignorer les informations de l'utilisateur** pour ne pas utiliser de méthode transparente pour l'identification des utilisateurs.
2. Indiquez si les utilisateurs doivent être invités à saisir leurs identifiants de connexion via le navigateur. Ce paramètre s'applique lorsque les informations des utilisateurs ne sont pas disponibles, soit parce que l'identification transparente a échoué, soit parce qu'elle a été ignorée.
   - Sélectionnez **Appliquer la stratégie de l'ordinateur ou du réseau** pour que les utilisateurs ne soient jamais invités à fournir leurs identifiants de connexion.
   - Si l'option « Essayer d'identifier l'utilisateur de façon transparente » est également sélectionnée, les utilisateurs dont les identifiants de connexion peuvent être vérifiés de façon transparente sont filtrés par la stratégie d'utilisateurs appropriée.

- Sélectionnez **Inviter l'utilisateur à fournir des informations de connexion** pour obliger les utilisateurs à fournir leurs identifiants de connexion, puis spécifiez le **Contexte de domaine par défaut** à utiliser (le cas échéant).

  Si l'option « Essayer d'identifier l'utilisateur de façon transparente » est également sélectionnée, les utilisateurs reçoivent une invite du navigateur uniquement s'ils n'ont pas été identifiés de manière transparente.

3. Cliquez sur **OK** pour revenir à la page Identification des utilisateurs.
4. Lorsque la mise à jour de la liste Exceptions est terminée, 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)**.

Authentification manuelle sécurisée

Rubriques connexes :

- *Configuration des méthodes d'identification des utilisateurs*, page 287
- *Authentification manuelle*, page 287
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289
- *Activation de l'authentification manuelle sécurisée*, page 294

L'authentification manuelle sécurisée de Websense utilise le cryptage SSL (Secure Sockets Layer) pour protéger les données d'authentification qui circulent entre les ordinateurs client et Websense. Un serveur SSL intégré à Filtering Service assure le cryptage des noms d'utilisateur et des mots de passe transmis entre les ordinateurs clients et le service Filtering Service. Par défaut, l'authentification manuelle sécurisée est désactivée.

Remarque

L'authentification manuelle sécurisée ne peut pas être utilisée avec un logiciel de filtrage à distance. Le serveur Remote Filtering ne peut pas envoyer de pages de blocage aux clients s'il est associé à une instance de Filtering Service pour laquelle l'authentification manuelle sécurisée est activée.

Pour activer cette fonctionnalité, procédez comme suit :

1. Générez des certificats et des clés SSL, et stockez-les dans un emplacement accessible par Websense et Filtering Service (voir *Création de clés et de certificats*, page 293).
2. Activez l'authentification manuelle sécurisée (voir *Activation de l'authentification manuelle sécurisée*, page 294) et la communication sécurisée avec le service d'annuaire.
3. Importez les certificats dans le navigateur (voir *Acceptation du certificat dans le navigateur client*, page 294).

Création de clés et de certificats

Rubriques connexes :

- *Authentification manuelle*, page 287
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289
- *Authentification manuelle sécurisée*, page 292
- *Activation de l'authentification manuelle sécurisée*, page 294
- *Acceptation du certificat dans le navigateur client*, page 294

Tout certificat se compose d'une clé publique, utilisée pour crypter les données, et d'une clé privée, utilisée pour les décrypter. Les certificats sont publiés par une Autorité de certification (CA). Vous pouvez générer un certificat à partir d'un serveur de certificats interne ou obtenir un certificat client auprès d'une autorité de certification tierce, telle que VeriSign.

L'autorité de certification qui publie le certificat client doit être approuvée par Websense. En général, cela est déterminé par un paramètre du navigateur.

- Vous trouverez les réponses aux questions courantes relatives aux clés privées, aux requêtes CSR et aux certificats à l'adresse httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts.
- Pour plus d'informations sur la création de votre propre clé privée, requête CSR et certificat, consultez le site www.akadia.com/services/ssh_test_certificate.html.

De nombreux outils vous permettent de générer un certificat auto-signé, dont OpenSSL Toolkit (disponible sur le site openssl.org).

Quelle que soit la méthode choisie pour générer le certificat, utilisez la procédure suivante.

1. Générez une clé privée (**server.key**).
2. Générez une Requête de signature de certificat (CSR, Certificate Signing Request) avec la clé privée.

> **Important**
>
> Lorsque vous êtes invité(e) à saisir le NomCommun, entrez l'adresse IP de l'ordinateur Filtering Server. Si vous ignorez cette étape, les navigateurs clients afficheront une erreur de certificat de sécurité.

3. Servez-vous de la requête CSR pour générer un certificat auto-signé (**server.crt**).
4. Enregistrez les fichiers **server.crt** et **server.key** dans un emplacement accessible à Websense et dans lequel Filtering Service peut les lire.

Activation de l'authentification manuelle sécurisée

Rubriques connexes :
- *Authentification manuelle*, page 287
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289
- *Authentification manuelle sécurisée*, page 292
- *Création de clés et de certificats*, page 293
- *Acceptation du certificat dans le navigateur client*, page 294

1. Arrêtez Websense Filtering Service (voir *Arrêt et démarrage des services Websense*, page 375).
2. Dans l'ordinateur Filtering Service, localisez le répertoire d'installation de Websense (par défaut, **C:\Program Files\Websense\bin** ou **/opt/Websense/bin/**).
3. Localisez le fichier **eimserver.ini** et sauvegardez-le dans un autre répertoire.
4. Ouvrez le fichier INI original dans un éditeur de texte.
5. Localisez la section **[WebsenseServer]** et ajoutez la ligne suivante :
   ```
   SSLManualAuth=on
   ```
6. Au-dessous de la ligne précédente, ajoutez :
   ```
   SSLCertFileLoc=[chemin]
   ```
   Remplacez **[chemin]** par le chemin d'accès complet du certificat SSL, en incluant le nom du fichier (par exemple, C:\secmanauth\server.crt).
7. Ajoutez également :
   ```
   SSLKeyFileLoc=[chemin]
   ```
   Remplacez **[chemin]** par le chemin d'accès complet de la clé SSL, en incluant le nom du fichier (par exemple, C:\secmanauth\server.key).
8. Enregistrez et fermez le fichier **eimserver.ini**.
9. Démarrez Websense Filtering Service.

Après le démarrage, Filtering Service est à l'écoute des requêtes sur le port HTTP sécurisé par défaut (**15872**).

La procédure précédente assure une communication sécurisée entre l'ordinateur client et Websense. Pour sécuriser également la communication entre Websense et le service d'annuaire, assurez-vous que l'option **Utiliser SSL** est également sélectionnée à la page **Paramètres** > **Services d'annuaire**. Pour plus d'informations, consultez la section *Paramètres avancés de l'annuaire*, page 78.

Acceptation du certificat dans le navigateur client

Rubriques connexes :
- *Authentification manuelle*, page 287
- *Définition de règles d'authentification pour des ordinateurs spécifiques*, page 289
- *Authentification manuelle sécurisée*, page 292
- *Création de clés et de certificats*, page 293
- *Activation de l'authentification manuelle sécurisée*, page 294

Lors de votre première tentative d'accès à un site Web, le navigateur présente un avertissement sur le certificat de sécurité. Pour que ce message n'apparaisse plus ensuite, installez le certificat dans le magasin de certificats.

Microsoft Internet Explorer

1. Ouvrez le navigateur et accédez à un site Web.

   Un message d'avertissement s'affiche, signalant un problème avec le certificat de sécurité du site.
2. Cliquez sur **Continuer avec ce site Web (non conseillé)**.

   Si vous recevez une invite d'authentification, cliquez sur **Annuler**.
3. Cliquez sur la zone **Erreur de certificat** située à droite de la barre d'adresse (en haut de la fenêtre du navigateur), puis sur **Afficher les certificats**.
4. Dans l'onglet Général de la boîte de dialogue Certificat, cliquez sur **Installer le certificat**.
5. Sélectionnez **Sélectionner automatiquement le magasin de certificats selon le type de certificat**, puis cliquez sur **Suivant**.
6. Cliquez sur **Terminer**.
7. Lorsque vous êtes invité(e) à installer le certificat, cliquez sur **Oui**.

Les utilisateurs ne recevront plus d'avertissements de sécurité de certificat liés à Filtering Service sur cet ordinateur.

Mozilla Firefox

1. Ouvrez le navigateur et accédez à un site Web.

   Un message d'avertissement s'affiche.
2. Cliquez sur **Ou vous pouvez ajouter une exception**.
3. Cliquez sur **Ajouter une exception**.
4. Assurez-vous que l'option **Conserver définitivement cette exception** est bien activée, puis cliquez sur **Confirmer l'exception de sécurité**.

Les utilisateurs ne recevront plus d'avertissements de sécurité de certificat liés à Filtering Service sur cet ordinateur.

DC Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Configuration de DC Agent*, page 296

Websense DC Agent s'exécute sous Windows et détecte les utilisateurs du réseau Windows qui exécutent NetBIOS, WINS ou des services réseau DNS.

DC Agent et User Service rassemblent les données des utilisateurs du réseau et les envoient à Websense Filtering Service. Plusieurs variables déterminent la vitesse de transmission des données, dont la taille de votre réseau et le volume du trafic.

Pour activer l'identification transparente avec DC Agent :

1. Installez DC Agent. Pour plus d'informations, consultez le Centre Installation et déploiement.

   Pour pouvoir effectuer la détection des domaines (détection automatique des domaines et des contrôleurs de domaine) et interroger les ordinateurs (pour vérifier l'utilisateur connecté), DC Agent doit s'exécuter avec des autorisations **administrateur de domaine** ou **administrateur d'entreprise**. Si vous n'envisagez pas d'utiliser ces fonctionnalités, DC Agent peut s'exécuter comme n'importe quel utilisateur du réseau avec des autorisations en lecture sur le contrôleur de domaine. Notez que, lorsque la détection de domaine est désactivée, vous devez gérer manuellement la liste des domaines et contrôleurs de domaine pour chaque instance de DC Agent (voir *Fichier dc_config.txt*, page 299).
2. Configurez DC Agent pour qu'il communique avec les autres composants Websense et avec les contrôleurs de domaine de votre réseau (voir *Configuration de DC Agent*).
3. Utilisez TRITON - Web Security pour ajouter des utilisateurs et des groupes à filtrer (voir *Ajout d'un client*, page 81).

Websense peut inviter les utilisateurs à s'authentifier lorsque DC Agent ne peut pas les identifier de façon transparente. Pour plus d'informations, consultez la section *Authentification manuelle*, page 287.

Configuration de DC Agent

Rubriques connexes :

- *Identification transparente*
- *Authentification manuelle*
- *Configuration des méthodes d'identification des utilisateurs*
- *DC Agent*

La page **Identification des utilisateurs > DC Agent** permet de configurer une nouvelle instance de DC Agent et les paramètres globaux s'appliquant à toutes les instances de DC Agent.

Pour ajouter une nouvelle instance de DC Agent, fournissez d'abord les informations de base sur l'emplacement d'installation de l'agent et sur le mode de communication de Filtering Service avec cet agent. Ces paramètres peuvent être distincts pour chaque instance de l'agent.

1. Sous Configuration de base de l'agent, entrez l'**adresse IPv4 ou le nom d'hôte** de l'ordinateur dans lequel l'agent est installé.

Remarque

Les noms d'hôte doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.

Les noms d'hôte contenant des caractères ASCII étendus risquent de ne pas être résolus correctement. Si vous utilisez une version non anglaise de Websense, entrez une adresse IP plutôt qu'un nom d'ordinateur.

2. Entrez le numéro de **Port** que DC Agent doit utiliser pour communiquer avec les autres composants de Websense. La valeur par défaut est 30600.
3. Pour établir une connexion authentifiée entre Filtering Service et DC Agent, sélectionnez **Activer l'authentification**, puis entrez un **Mot de passe** de connexion.

Personnalisez ensuite la communication globale de DC Agent et les paramètres du dépannage, de l'interrogation du contrôleur de domaine et de l'interrogation des ordinateurs. Par défaut, les modifications apportées ici affectent toutes les instances de DC Agent.

Certains de ces paramètres peuvent toutefois être remplacés dans un fichier de configuration (voir le document technique Using DC Agent for Transparent User Identification (Utilisation de DC Agent pour l'identification transparente des utilisateurs)).

1. Sous Domain Discovery (Détection des domaines), activez ou désactivez la case à cocher **Enable automatic domain discovery (Activer la détection automatique des domaines)** pour indiquer si DC Agent doit rechercher automatiquement les domaines et les contrôleurs de domaine dans votre réseau.
2. Si vous activez la détection des domaines, définissez également :
   - La fréquence de **détection des domaines**. Par défaut, la détection des domaines intervient à intervalles de 24 heures.
   - Si **DC Agent** ou **User Service** est chargé d'effectuer la détection des domaines.

     Dans la plupart des environnements, il est préférable d'utiliser User Service pour la détection des domaines.

     Si DC Agent est utilisé pour la détection des domaines, le service doit s'exécuter avec des privilèges **administrateur de domaine** ou **administrateur d'entreprise**.
3. Lorsque User Service est installé dans un ordinateur Linux, la page comprend une section **Linux WINS Server Information (Informations sur Linux WINS Server)**. Un serveur WINS est requis pour résoudre les noms de domaine en adresses IP de contrôleur de domaine.

   Si vous n'avez pas encore fourni les informations WINS dans la page Paramètres > Services d'annuaire, saisissez :

   a. Le nom du compte d'un **administrateur** autorisé à accéder au service d'annuaire
   b. Le **Mot de passe** de ce compte
   c. Les informations du **Domaine** de ce compte
   d. L'adresse IP ou le nom d'hôte d'un serveur WINS présent dans votre réseau
4. Dans la section Domain Controller Polling (Interrogation du contrôleur de domaine) du champ Communication de DC Agent, cochez la case **Activer l'interrogation du contrôleur de domaine** afin que DC Agent puisse interroger les contrôleurs de domaine lors des sessions de connexion des utilisateurs.

   Pour interroger les contrôleurs de domaine, le service DC Agent n'a besoin que d'autorisations en lecture sur le contrôleur de domaine. La détection automatique des domaines (étapes 1 et 2) et l'interrogation des ordinateurs (étape 7) impliquent que le service s'exécute avec des autorisations élevées.

   Vous pouvez définir quels contrôleurs de domaine seront interrogés par chaque instance de DC Agent dans un fichier de configuration (voir *Fichier dc_config.txt*, page 299).

5. Utilisez le champ **Intervalle de requête** pour indiquer la fréquence (en secondes) selon laquelle DC Agent doit interroger les contrôleurs de domaine.

   Diminuer cet intervalle peut accroître la précision de la capture des sessions de connexion, mais augmente également le volume du trafic réseau. Augmenter cet intervalle allège le trafic réseau, mais peut également retarder ou empêcher la capture de certaines sessions de connexion. La valeur par défaut est 10 secondes.
6. Utilisez le champ **Délai d'attente de l'entrée utilisateur** pour définir la fréquence (en heures) selon laquelle DC Agent actualise les entrées des utilisateurs dans son mappage. Le délai par défaut est de 24 heures.
7. Sous Interrogation des ordinateurs, sélectionnez l'option **Activer l'interrogation des ordinateurs** afin que DC Agent interroge les ordinateurs pour les sessions de connexion des utilisateurs. Cela peut inclure des ordinateurs extérieurs aux domaines déjà interrogés par DC Agent.

   DC Agent utilise WMI (Windows Management Instruction) pour l'interrogation des ordinateurs. Si vous activez l'interrogation des ordinateurs, configurez le Pare-feu de Windows dans les ordinateurs clients pour autoriser une communication sur le port **135**.

   Si DC Agent effectue l'interrogation des ordinateurs, le service doit s'exécuter avec des privilèges **administrateur de domaine** ou **administrateur d'entreprise**.
8. Entrez un **Intervalle de vérification des correspondances d'utilisateur** pour définir la fréquence selon laquelle DC Agent contacte les ordinateurs clients afin de vérifier quels utilisateurs sont connectés. La valeur par défaut est 15 minutes.

   DC Agent compare les résultats de la requête et les paires nom d'utilisateur/adresse IP dans le mappage des utilisateurs qu'il envoie au service Filtering Service. Réduire cet intervalle peut accroître la précision des correspondances, mais augmente le trafic du réseau. Augmenter cet intervalle allège le trafic réseau, mais peut également réduire la précision.
9. Entrez un **Délai d'attente de l'entrée utilisateur** pour définir la fréquence selon laquelle DC Agent actualise les entrées obtenues via l'interrogation des ordinateurs dans son mappage des utilisateurs. Le délai par défaut est de 1 heure.

   DC Agent retire toutes les entrées nom d'utilisateur/adresse IP postérieures à ce délai, et qu'il ne peut pas vérifier par rapport aux utilisateurs actuellement connectés. Augmenter cet intervalle peut réduire la précision du mappage des utilisateurs, car les anciens noms d'utilisateur peuvent y demeurer pendant de plus longues périodes.

   Remarque

   Ne définissez pas un délai d'attente de l'entrée utilisateur plus court que l'intervalle de vérification des correspondances des utilisateurs, car des noms d'utilisateur pourraient être retirés du mappage avant de pouvoir être vérifiés.

10. Cliquez sur **OK** pour revenir à la page Identification des utilisateurs, 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)**.

Vérification des domaines et contrôleurs de domaine interrogés par DC Agent

Pour identifier les contrôleurs de domaine de votre réseau actuellement interrogés par chaque instance de DC Agent, utilisez la page **Identification des utilisateurs > DC Agent Domains and Controllers (Domaines et contrôleurs de domaine DC Agent)**.

> **Important**
>
> Si le texte de la page DC Agent Domains and Controllers (Domaines et contrôleurs de domaine DC Agent) indique que DC Agent n'interroge aucun contrôleur de domaine pour l'instant, consultez la section *Page des domaines et des contrôleurs de DC Agent vide*, page 457.

En général, la page présente les **Domaines** et **Contrôleurs de domaine** détectés par chacune des instances de **DC Agent** dans votre réseau.

Par défaut, DC Agent exécute son processus de **détection des domaines** (identification des domaines et des contrôleurs de domaine) au démarrage, puis toutes les 24 heures. Les informations relatives aux domaines et aux contrôleurs de domaine sont stockées dans un fichier nommé **dc_config.txt** (voir *Fichier dc_config.txt*, page 299).

Les informations affichées dans la page des domaines et contrôleurs de domaine DC Agent sont compilées à partir de chaque fichier dc_config.txt de votre déploiement.

- La liste comprend uniquement les domaines et les contrôleurs de domaine activement interrogés.
  - Si vous avez désactivé l'interrogation d'un contrôleur de domaine dans le fichier dc_config.txt, ce contrôleur de domaine n'apparaît pas.
  - De la même façon, si vous avez désactivé l'interrogation de tous les contrôleurs de domaine d'un domaine, ni le domaine ni ses contrôleurs n'apparaissent dans cette liste.
- Les informations s'affichent pour toutes les instances de DC Agent de votre réseau.
  - Lorsqu'un même contrôleur de domaine est interrogé par plusieurs instances de DC Agent, chacune de ces instances est répertoriée.
  - Pour configurer des instances de DC Agent distinctes pour qu'elles interrogent des domaines différents, actualisez le fichier dc_config.txt de chaque instance. Voir *Fichier dc_config.txt*, page 299.
- TRITON - Web Security vérifie les dernières informations des domaines et des contrôleurs de domaine chaque fois que vous accédez à la page des domaines et contrôleurs de domaine DC Agent. Par conséquent, si la détection des domaines est en cours d'exécution lorsque vous affichez cette page, vous devez la fermer, puis y revenir pour voir les mises à jour.

Fichier dc_config.txt

DC Agent fonctionne en identifiant les contrôleurs de domaine du réseau, puis en les interrogeant lors des sessions de connexion des utilisateurs. Par défaut, l'agent vérifie automatiquement les contrôleurs de domaine existants et détecte les nouveaux domaines ou contrôleurs de domaine ajoutés dans le réseau.

- Par défaut, DC Agent détecte les domaines (identification des domaines et des contrôleurs de domaine) au démarrage, puis toutes les 24 heures.
- Vous pouvez utiliser DC Agent ou User Service pour la détection des domaines.

Pour plus d'informations sur l'activation de la détection des domaines et la définition de l'intervalle de détection, consultez la section *Configuration de DC Agent*, page 296.

DC Agent stocke les informations relatives aux domaines et aux contrôleurs de domaine dans un fichier intitulé **dc_config.txt** (situé par défaut dans le répertoire C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin\ de chaque ordinateur DC Agent).

Pour changer les contrôleurs de domaine interrogés par DC Agent, modifiez le fichier dc_config.txt :

1. Accédez au répertoire **bin** de Websense (par défaut, C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin) dans l'ordinateur DC Agent.
2. Créez une copie de sauvegarde du fichier **dc_config.txt** dans un autre emplacement.
3. Ouvrez le fichier **dc_config.txt** original dans un éditeur de texte (tel que Notepad).
4. Vérifiez que tous vos domaines et contrôleurs de domaine sont répertoriés dans la liste. Par exemple :

   ```
   [WEST_DOMAIN]
   dcWEST1=on
   dcWEST2=on
   [EAST_DOMAIN]
   dcEAST1=on
   dcEAST2=on
   ```

5. Si certains contrôleurs de domaine de la liste ne doivent pas être interrogés par DC Agent, remplacez la valeur **on** par **off**. Par exemple :

   ```
   dcEAST2=off
   ```

   - Si vous configurez DC Agent pour qu'il n'interroge pas un contrôleur de domaine actif, l'agent ne peut pas identifier en transparence les utilisateurs qui se connectent à ce contrôleur de domaine.
   - Si la détection automatique des domaines de DC Agent détecte un contrôleur de domaine qui ne doit pas servir à identifier les utilisateurs, définissez son entrée sur **off** au lieu de la supprimer. Dans le cas contraire, le prochain processus de détection ajoutera à nouveau ce contrôleur.
6. Si des entrées de domaine ou de contrôleur de domaine n'apparaissent pas dans la liste, vous pouvez les ajouter manuellement. Avant d'ajouter ces entrées, exécutez la commande **net view /domain** dans l'ordinateur DC Agent afin de vérifier que l'agent peut voir le nouveau domaine.
7. Enregistrez vos modifications et fermez le fichier.
8. Redémarrez le service **Websense DC Agent**.

Logon Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Configuration de Logon Agent*, page 301

Websense Logon Agent identifie les utilisateurs en temps réel, lorsqu'ils se connectent aux domaines. Les risques de manquer une connexion d'utilisateur à cause d'un problème de délai de requête sont ainsi éliminés.

Logon Agent (également appelé Serveur d'authentification) peut résider dans un ordinateur Windows ou Linux. Cet agent fonctionne avec l'application Websense Logon (LogonApp.exe) dans les ordinateurs clients Windows pour identifier les utilisateurs lorsqu'ils se connectent aux domaines Windows.

Dans la plupart des cas, l'utilisation de DC Agent ou de Logon Agent suffit, mais vous pouvez les combiner. Dans ce cas, Logon Agent est prioritaire sur DC Agent. DC Agent communique uniquement les sessions de connexion à Filtering Service si Logon Agent en a manqué une, ce qui est peu probable.

Installez Logon Agent, puis déployez l'application de connexion dans les ordinateurs clients depuis un emplacement centralisé. Pour plus d'informations, consultez le document technique Using Logon Agent for Transparent User Identification (Utilisation de Logon Agent pour l'identification transparente des utilisateurs).

Après son installation, configurez l'agent pour qu'il communique avec les ordinateurs clients et avec Websense Filtering Service (voir *Configuration de Logon Agent*).

> **Remarque**
>
> Si vous utilisez Windows Active Directory (en mode natif) et que User Service est installé dans un ordinateur Linux, consultez la section *User Service sous Linux*, page 461, pour des instructions supplémentaires sur la configuration.

Configuration de Logon Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Authentification manuelle*, page 287
- *Configuration des méthodes d'identification des utilisateurs*, page 287
- *Logon Agent*, page 300

La page **Identification des utilisateurs > Logon Agent** permet de configurer une nouvelle instance de Logon Agent et les paramètres globaux s'appliquant à toutes les instances de Logon Agent.

Pour ajouter une nouvelle instance de Logon Agent :

1. Sous Configuration de base de l'agent, entrez l'**adresse IPv4 ou le nom d'hôte** de l'ordinateur Logon Agent.

   > **Remarque**
   >
   > Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.
   >
   > Les noms d'ordinateur contenant certains caractères ASCII étendus risquent de ne pas être résolus correctement. Si vous utilisez une version non anglaise de Websense, entrez une adresse IP plutôt qu'un nom d'ordinateur.

2. Entrez le numéro de **Port** que Logon Agent doit utiliser pour communiquer avec les autres composants de Websense (par défaut, 30602).
3. Pour établir une connexion authentifiée entre Filtering Service et Logon Agent, cochez la case **Activer l'authentification**, puis entrez un **Mot de passe** de connexion.

Personnalisez ensuite les paramètres globaux de communication de Logon Agent. Par défaut, les modifications apportées ici affectent toutes les instances de Logon Agent.

1. Sous Logon Application Communication (Communication de l'application de connexion), définissez le **Port de connexion** utilisé par l'application de connexion pour communiquer avec Logon Agent (par défaut, 15880).
2. Entrez le **Nombre maximum de connexions** que chaque instance de Logon Agent autorise (par défaut, 200).

   Si votre réseau est très vaste, vous pouvez augmenter la valeur de ce nombre. L'augmentation de cette valeur accroît le trafic réseau.

Pour configurer les paramètres par défaut qui déterminent comment la validité de l'entrée de l'utilisateur est vérifiée, vous devez commencer par décider si Logon Agent et l'application de connexion cliente fonctionnent en **mode persistant** ou en **mode non persistant** (par défaut).

Le mode non persistant est activé en incluant le paramètre /NOPERSIST au démarrage de **LogonApp.exe**. (Vous trouverez d'autres informations dans le fichier **LogonApp_ReadMe.txt**, inclus avec l'installation de Logon Agent.)

- En mode persistant, l'application de connexion contacte régulièrement Logon Agent pour communiquer les informations de connexion des utilisateurs.

  Si vous utilisez le mode persistant, définissez un **Intervalle de requête** pour déterminer la fréquence de communication des identifiants de connexion par l'application de connexion.

  > **Remarque**
  >
  > Si vous changez cette valeur, la modification ne prend pas effet avant la fin de l'intervalle précédemment défini. Par exemple, si vous remplacez un intervalle de 15 minutes par 5 minutes, l'intervalle de 15 minutes en cours doit s'écouler avant que l'interrogation ne commence toutes les 5 minutes.

- En mode non persistant, l'application de connexion n'envoie les informations de connexion des utilisateurs à Logon Agent qu'une fois par connexion.

  Si vous utilisez le mode non persistant, entrez un délai **Expiration des entrées utilisateur**. Lorsque ce délai est écoulé, l'entrée de l'utilisateur est retirée du mappage des utilisateurs.

Lorsque vos modifications de la configuration sont terminées, cliquez sur **OK** pour revenir à la page Paramètres > Identification des utilisateurs, puis de nouveau sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas enregistrées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

RADIUS Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Configuration de RADIUS Agent*, page 303

Websense RADIUS Agent vous permet d'appliquer des stratégies d'utilisateurs et de groupes à l'aide de l'authentification fournie par un serveur RADIUS. RADIUS Agent autorise l'identification transparente des utilisateurs qui accèdent à votre réseau par une connexion à distance, un VPN (Virtual Private Network), une ligne DSL ou une autre connexion à distance (selon votre configuration).

RADIUS Agent fonctionne avec le serveur RADIUS et le client RADIUS de votre réseau pour traiter et surveiller le trafic du protocole RADIUS (Remote Access Dial-In User Service). Vous pouvez ainsi affecter des stratégies de filtrage particulières aux utilisateurs ou aux groupes qui accèdent à votre réseau à distance, ainsi qu'aux utilisateurs locaux.

Lorsque vous installez RADIUS Agent, l'agent s'intègre aux composants Websense existants. Toutefois, RADIUS Agent, votre serveur RADIUS et votre client RADIUS doivent être configurés de façon adéquate (voir *Configuration de RADIUS Agent*, page 303).

Configuration de RADIUS Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Authentification manuelle*, page 287
- *Configuration des méthodes d'identification des utilisateurs*, page 287
- *RADIUS Agent*, page 303

La page **Identification des utilisateurs > RADIUS Agent** permet de configurer une nouvelle instance de RADIUS Agent et les paramètres globaux s'appliquant à toutes les instances de RADIUS Agent.

Pour ajouter une nouvelle instance de RADIUS Agent :

1. Sous Configuration de base de l'agent, entrez l'**adresse IPv4 ou le nom d'hôte** de l'ordinateur RADIUS Agent.

   Remarque

   Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.

   Les noms d'ordinateur contenant certains caractères ASCII étendus risquent de ne pas être résolus correctement. Dans les environnements non anglais, saisissez l'adresse IP à la place du nom.

2. Entrez le numéro de **Port** que RADIUS Agent doit utiliser pour communiquer avec les autres composants de Websense (par défaut, 30800).

3. Pour établir une connexion authentifiée entre Filtering Service et RADIUS Agent, cochez la case **Activer l'authentification**, puis entrez un **Mot de passe** de connexion.

Personnalisez ensuite les paramètres globaux de RADIUS Agent. Par défaut, les modifications apportées ici affectent toutes les instances de RADIUS Agent. Les paramètres signalés par un astérisque (*) peuvent toutefois être remplacés dans un fichier de configuration personnalisant le comportement de l'instance de cet agent (consultez le document technique Using RADIUS Agent for Transparent User Identification (Utilisation de RADIUS Agent pour l'identification transparente des utilisateurs)).

1. Sous Serveur RADIUS, entrez l'**adresse ou le nom du serveur RADIUS**. Si vous fournissez son adresse IP, utilisez le format IPv4.

   RADIUS Agent transmet les demandes d'authentification au serveur RADIUS et doit donc connaître l'identité de cet ordinateur.
2. Si votre réseau comprend un client RADIUS, saisissez l'**adresse ou le nom du client RADIUS**. Si vous fournissez son adresse IP, utilisez le format IPv4.

   Websense interroge cet ordinateur sur les sessions de connexion des utilisateurs.
3. Entrez le **Délai d'attente de l'entrée utilisateur** pour définir la fréquence selon laquelle RADIUS Agent actualise son mappage des utilisateurs. L'intervalle idéal est généralement celui proposé par défaut (24 heures).
4. Utilisez les paramètres **Ports d'authentification** et **Ports de gestion des comptes** pour définir les ports utilisés par RADIUS Agent pour envoyer et recevoir les requêtes d'authentification et de compte. Pour chaque type de communication, vous pouvez spécifier le port utilisé pour la communication entre :
   - RADIUS Agent et le serveur RADIUS (authentification, par défaut le port 1645 ; demande de comptes, par défaut le port 1646)
   - RADIUS Agent et le client RADIUS (authentification, par défaut le port 12345; demande de comptes, par défaut le port 12346)
5. Lorsque vos modifications de la configuration sont terminées, cliquez sur **OK** pour revenir à la page Paramètres > Identification des utilisateurs, puis de nouveau sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas enregistrées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Pour plus d'informations sur la configuration de la communication de votre client RADIUS et de votre serveur RADIUS avec Websense RADIUS Agent, consultez le document technique Using RADIUS Agent for Transparent User Identification (Utilisation de RADIUS Agent pour l'identification transparente des utilisateurs).

eDirectory Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Configuration d'eDirectory Agent*, page 305

Websense eDirectory Agent fonctionne avec Novell eDirectory pour identifier les utilisateurs de manière transparente de sorte que Websense puisse les filtrer en fonction des stratégies affectées aux utilisateurs, aux groupes, aux domaines ou aux unités d'organisation.

eDirectory Agent collecte les informations de session de connexion des utilisateurs auprès de Novell eDirectory, qui authentifie les utilisateurs se connectant au réseau. L'agent associe ensuite chaque utilisateur authentifié à une adresse IP et enregistre les paires nom d'utilisateur/adresse IP dans un mappage local des utilisateurs. eDirectory Agent transmet ensuite ces informations à Filtering Service.

Remarque

Plusieurs utilisateurs peuvent se connecter à un même serveur Novell eDirectory à partir d'un client Novell fonctionnant sous Windows. Dans ce cas, une même adresse IP est associée à plusieurs utilisateurs. Dans ce scénario, le mappage des utilisateurs d'eDirectory Agent ne conserve que la paire nom d'utilisateur/adresse IP du dernier utilisateur connecté à partir d'une adresse IP donnée.

Une même instance de Websense eDirectory Agent peut prendre en charge une instance principale de Novell eDirectory, plus n'importe quel nombre de répliques Novell eDirectory.

Configuration d'eDirectory Agent

Rubriques connexes :

- *Identification transparente*, page 285
- *Authentification manuelle*, page 287
- *Configuration des méthodes d'identification des utilisateurs*, page 287
- *eDirectory Agent*, page 304
- *Configuration d'eDirectory Agent pour l'utilisation de LDAP*, page 307

La page **Identification des utilisateurs > eDirectory Agent** permet de configurer une nouvelle instance d'eDirectory Agent et les paramètres globaux s'appliquant à toutes les instances d'eDirectory Agent.

Pour ajouter une nouvelle instance d'eDirectory Agent :

1. Sous Configuration de base de l'agent, entrez l'**adresse IPv4 ou le nom d'hôte** de l'ordinateur eDirectory Agent.

   Remarque

   Les noms d'ordinateur doivent commencer par un caractère alphabétique (a-z) et non par un caractère numérique ou spécial.

   Les noms d'ordinateur contenant certains caractères ASCII étendus risquent de ne pas être résolus correctement. Dans les environnements non anglais, saisissez l'adresse IP à la place du nom.

2. Entrez le numéro de **Port** que eDirectory Agent doit utiliser pour communiquer avec les autres composants de Websense (par défaut, 30700).

3. Pour établir une connexion authentifiée entre Filtering Service et eDirectory Agent, sélectionnez **Activer l'authentification**, puis entrez un **Mot de passe** de connexion.

Personnalisez ensuite les paramètres globaux de communication d'eDirectory Agent :

1. Sous Serveur eDirectory, spécifiez la **Base de recherche** (contexte racine) qu'eDirectory Agent doit utiliser comme point de départ lorsqu'il recherche des informations d'utilisateurs dans l'annuaire.
2. Entrez les informations du compte d'administration qu'eDirectory Agent doit utiliser pour communiquer avec l'annuaire :
   a. Entrez le **Nom distinctif de l'administrateur** d'un compte d'administration Novell eDirectory.
   b. Entrez le **Mot de passe** utilisé par ce compte.
   c. Entrez un **Délai d'attente de l'entrée utilisateur** pour définir le délai de conservation des entrées dans le mappage des utilisateurs de l'agent.

      Cet intervalle doit être environ 30 % plus long qu'une session de connexion d'utilisateur typique. Il évite que des entrées d'utilisateur ne soient retirées du mappage avant que ces utilisateurs n'aient terminé leur navigation.

      L'intervalle idéal est généralement celui proposé par défaut (24 heures).

> **Remarque**
>
> Dans certains environnements, au lieu d'utiliser le délai d'attente de l'entrée de l'utilisateur pour déterminer la fréquence selon laquelle eDirectory Agent actualise son mappage des utilisateurs, il peut être approprié de demander régulièrement à eDirectory Server les mises à jour des connexions des utilisateurs. Voir *Activation des requêtes complètes du serveur eDirectory*, page 308.

3. Ajoutez l'instance principale d'eDirectory Server et les répliques éventuelles dans la liste **Répliques eDirectory**. Pour ajouter une instance principale d'eDirectory Server dans la liste, cliquez sur **Ajouter** et suivez les instructions de la section *Ajout d'une réplique de serveur eDirectory*, page 306.

Lorsque vos modifications de la configuration sont terminées, cliquez sur **OK** pour revenir à la page Paramètres > Identification des utilisateurs, puis de nouveau sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas enregistrées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout d'une réplique de serveur eDirectory

Une même instance de Websense eDirectory Agent peut prendre en charge une instance principale de Novell eDirectory, plus n'importe quel nombre de répliques Novell eDirectory s'exécutant dans des ordinateurs distincts.

eDirectory Agent doit pouvoir communiquer avec chaque ordinateur exécutant une réplique du service d'annuaire. L'agent obtient ainsi les informations de connexion les plus récentes aussi rapidement que possible et n'attend pas qu'une réplication d'eDirectory ne se produise.

Novell eDirectory réplique l'attribut qui identifie de façon unique les utilisateurs connectés seulement toutes les 5 minutes. Malgré ce délai de réplication, eDirectory Agent récupère les nouvelles sessions de connexion dès qu'un utilisateur se connecte à une réplique eDirectory.

Pour configurer l'installation d'eDirectory Agent pour une communication avec eDirectory :

1. Saisissez l'**Adresse IP du serveur** de l'instance principale ou de la réplique de Novell eDirectory.
2. Entrez le numéro de **Port** qu'eDirectory Agent utilise pour communiquer avec l'ordinateur eDirectory. Les valeurs valides sont **389** (par défaut) et **636** (port SSL).
3. Cliquez sur **OK** pour revenir à la page eDirectory Agent. La nouvelle entrée apparaît dans la liste Répliques eDirectory.
4. Répétez éventuellement ce processus pour d'autres serveurs eDirectory.
5. Cliquez sur **OK** pour revenir à la page Paramètres >Identification des utilisateurs, puis de nouveau sur **OK** pour mettre vos modifications en cache.
6. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.
7. Arrêtez et redémarrez eDirectory Agent pour que l'agent puisse commencer à communiquer avec la nouvelle réplique. Pour obtenir des instructions, consultez la section *Arrêt et démarrage des services Websense*, page 375.

Configuration d'eDirectory Agent pour l'utilisation de LDAP

Websense eDirectory Agent peut utiliser le protocole NCP (Netware Core Protocol) ou LDAP (Lightweight Directory Access Protocol) pour obtenir les informations de connexion des utilisateurs auprès de Novell eDirectory. Par défaut, eDirectory Agent utilise NCP sous Windows. Sous Linux, eDirectory Agent doit utiliser LDAP.

Si vous exécutez eDirectory Agent sous Windows et que vous souhaitez que l'agent utilise LDAP pour interroger Novell eDirectory, définissez l'agent pour qu'il utilise LDAP au lieu de NCP. En général, NCP assure un mécanisme de requête plus efficace.

Pour qu'eDirectory Agent utilise LDAP sous Windows :

1. Assurez-vous de disposer d'au moins une réplique Novell eDirectory contenant tous les objets de l'annuaire pour surveiller et filtrer votre réseau.
2. Arrêtez le service Websense eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 375).
3. Localisez le répertoire d'installation d'eDirectory Agent (par défaut, **\Program Files\Websense\bin**), puis ouvrez le fichier **wsedir.ini** dans un éditeur de texte.
4. Modifiez l'entrée **QueryMethod** comme suit :

   ```
   QueryMethod=0
   ```

   Ce paramètre indique à l'agent d'utiliser LDAP pour interroger Novell eDirectory. (La valeur par défaut est 1, pour NCP.)
5. Enregistrez et fermez le fichier.
6. Redémarrez le service Websense eDirectory Agent.

Activation des requêtes complètes du serveur eDirectory

Dans les petits réseaux, vous pouvez configurer Websense eDirectory Agent pour qu'il interroge, à intervalles réguliers, le serveur eDirectory pour tous les utilisateurs connectés. L'agent peut ainsi détecter les utilisateurs nouvellement connectés et ceux qui se sont déconnectés depuis la dernière requête, et mettre à jour son mappage local des utilisateurs en conséquence.

Important

Configurer eDirectory Agent pour qu'il utilise des requêtes complètes n'est pas conseillé dans les grands réseaux. En effet, le temps nécessaire pour renvoyer les résultats des requêtes dépend du nombre d'utilisateurs connectés. Plus le nombre d'utilisateurs connectés est important, plus les performances sont ralenties.

Lorsque vous activez les requêtes complètes pour eDirectory Agent, le **délai d'attente de l'entrée de l'utilisateur** n'est pas employé car les utilisateurs qui se sont déconnectés sont identifiés par la requête. Par défaut, la requête intervient toutes les 30 secondes.

L'activation de cette fonction accroît le temps de traitement d'eDirectory Agent de deux manières :

- Du fait du temps nécessaire pour récupérer les noms des utilisateurs connectés à chaque nouvelle requête
- Du fait du temps nécessaire pour traiter les informations relatives aux noms des utilisateurs, pour supprimer les entrées obsolètes du mappage local des utilisateurs et pour ajouter les nouvelles entrées en fonction de la dernière requête

eDirectory Agent examine le mappage local des utilisateurs dans son intégralité après chaque requête au lieu d'identifier uniquement les nouvelles connexions. Le temps requis par ce processus dépend du nombre d'utilisateurs renvoyés par chaque requête. Ce processus peut donc affecter les délais de réponse d'eDirectory Agent et du serveur Novell eDirectory.

Pour activer les requêtes complètes :

1. Dans l'ordinateur eDirectory Agent, localisez le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
2. Localisez le fichier **wsedir.ini** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
3. Ouvrez le fichier **wsedir.ini** dans un éditeur de texte (tel que Notepad ou vi).
4. Localisez la section **[eDirAgent]**, puis l'entrée suivante :

   `QueryMethod=<N>`

   Prenez note de la valeur de QueryMethod pour le cas où vous souhaiteriez ensuite rétablir le paramètre par défaut.
5. Modifiez la valeur de **QueryMethod** comme suit :
   - Si la valeur actuelle est 0 (communication avec l'annuaire via LDAP), remplacez-la par **2**.

- Si la valeur actuelle est 1 (communication avec l'annuaire via NCP), remplacez-la par **3**.

> **Remarque**
> Si la modification de cette valeur de requête ralentit les performances du système, rétablissez la valeur précédente de l'entrée QueryMethod.

6. Si l'intervalle de requête par défaut (30 secondes) ne convient pas à votre environnement, modifiez la valeur de **PollInterval** de façon appropriée.

   Notez que l'intervalle est défini en **millisecondes**.
7. Enregistrez et fermez le fichier.
8. Redémarrez le service Websense eDirectory Agent (voir *Arrêt et démarrage des services Websense*, page 375).

Configuration d'un agent pour ignorer certains noms d'utilisateur

Vous pouvez configurer un agent d'identification transparente de sorte qu'il ignore les noms de connexion non associés à de véritables utilisateurs. Cette fonction est souvent exploitée pour gérer la manière dont certains services Windows contactent les contrôleurs de domaine du réseau.

Par exemple, **utilisateur1** se connecte au réseau et est identifié par le contrôleur de domaine en tant que **ordinateurA/utilisateur1**. Cet utilisateur est filtré par une stratégie Websense affectée à **utilisateur1**. Si un service démarre dans l'ordinateur de l'utilisateur avec l'identité **ordinateurA/NomService** pour contacter le contrôleur de domaine, des problèmes de filtrage peuvent survenir. Websense traite **ordinateurA/NomService** comme un nouvel utilisateur auquel aucune stratégie n'a été attribuée et filtre cet utilisateur en fonction de la stratégie de l'ordinateur ou de la stratégie **Par défaut**.

Pour résoudre ce problème :

1. Arrêtez le service de l'agent (voir *Arrêt et démarrage des services Websense*, page 375).
2. Accédez au répertoire **\Websense\bin** et ouvrez le fichier **ignore.txt** dans un éditeur de texte.
3. Entrez chaque nom d'utilisateur sur une ligne distincte. N'utilisez pas de caractère générique comme « * ».

   ```
   maran01
   WindowsServiceName
   ```

   Websense ignore ces noms d'utilisateur, quel que soit l'ordinateur auquel ils sont associés.

   Pour indiquer à Websense d'ignorer un nom d'utilisateur dans un domaine spécifique, utilisez le format **nom d'utilisateur, domaine**.

   ```
   aperez, engineering1
   ```

4. Lorsque vous avez terminé, enregistrez et fermez le fichier.
5. Redémarrez le service de l’agent.

L’agent ignore les noms d’utilisateur spécifiés et Websense ne prend plus ces noms en compte dans le filtrage.

Identification des utilisateurs du filtrage hybride

Rubriques connexes :

- *Websense Directory Agent*, page 319
- *Lorsque les utilisateurs ne sont pas identifiés*, page 321
- *Priorité et dérogation d'authentification*, page 313
- *Fonctionnement des clients du filtrage hybride*, page 86

Pour configurer la manière dont les utilisateurs sont identifiés par le service hybride et tester et configurer les connexions des utilisateurs au service, sélectionnez **Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs)**. Au besoin, vous pouvez configurer plusieurs options d'authentification ou d'identification pour vos utilisateurs hybrides.

Pour garantir l'application de la stratégie par utilisateur ou par groupe appropriée aux utilisateurs du filtrage hybride, qu'ils soient situés dans un emplacement filtré ou hors site, Websense Web Security Gateway Anywhere propose des options d'identification transparente des utilisateurs du filtrage hybride :

- **Websense Web Endpoint** est installé dans les ordinateurs clients pour assurer une authentification transparente, imposer l'utilisation du filtrage hybride et transmettre les informations d'authentification au service hybride. Voir *Présentation du déploiement de Web Endpoint*, page 314.
- **Websense Authentication Service** assure une authentification transparente sans client par l'intermédiaire d'une passerelle hébergée dans votre réseau. Voir *Déploiement de Websense Authentication Service*, page 317.

Si vous ne déployez ni Web Endpoint, ni Authentication Service, le service hybride peut identifier les utilisateurs de manière transparente ou manuelle lorsqu'ils se connectent au filtrage hybride.

- Les utilisateurs ne peuvent être identifiés en transparence via l'identification NTLM que s'ils sont connectés à partir d'une adresse IP connue, définie en tant qu'**emplacement filtré** (voir *Définition des emplacements filtrés*, page 205). Notez que l'identification NTLM n'est pas disponible pour les utilisateurs hors site.
- Le service hybride peut être configuré de manière à générer automatiquement des mots de passe pour tous les utilisateurs dont Directory Agent collecte les informations (voir *Configuration de l'accès des utilisateurs au filtrage hybride*, page 214).
- Si vous n'activez aucune forme d'authentification transparente :
  - Les utilisateurs hors site qui n'utilisent ni Web Endpoint ni Authentication Service sont invités à saisir une adresse électronique et un mot de passe lorsqu'ils ouvrent un navigateur et se connectent à Internet.
  - Les autres utilisateurs du filtrage hybride sont filtrés en fonction de leur adresse IP lorsque Web Endpoint, le service d'authentification ou l'identification NTLM ne sont pas disponibles.

Indiquez comment le service hybride doit identifier les utilisateurs qui demandent un accès à Internet. Ces options servent également de stratégie de repli en cas de défaillance d'Endpoint ou de Authentication Service.

- Cochez la case **Always authenticate users on first access (Authentifier systématiquement les utilisateurs lors du premier accès)** pour activer l'identification NTLM transparente ou l'authentification manuelle lorsque les utilisateurs se connectent pour la première fois au filtrage hybride.

  Si vous ne sélectionnez pas cette option et qu'aucune autre méthode d'authentification n'est disponible pour les utilisateurs situés dans des emplacements filtrés, ces utilisateurs sont filtrés par la stratégie de leur adresse IP.

  Internet Explorer et Firefox peuvent servir à l'identification transparente des utilisateurs. Les autres navigateurs invitent les utilisateurs à saisir leurs identifiants de connexion.

  Si Directory Agent envoie des données au service hybride, il est recommandé de choisir NTLM pour identifier les utilisateurs.

- Cochez la case **Use NTLM to identify users when possible (Utiliser NTLM pour identifier les utilisateurs lorsque cela est possible)** pour exploiter les informations d'annuaire collectées par Directory Agent pour identifier les utilisateurs en transparence, lorsque cela est possible.

  Lorsque cette option est sélectionnée, le service hybride exploite NTLM pour identifier l'utilisateur lorsque le client prend en charge cette méthode d'identification, ou invite l'utilisateur à saisir ses informations d'authentification lorsque ce n'est pas le cas.

  > **Remarque**
  >
  > Lorsque NTLM sert à identifier les utilisateurs, **ne choisissez pas** l'auto-enregistrement (configuré dans la page User Access (Accès utilisateur) sous Registered Domains (Domaines enregistrés)).

- Cochez la case Use secured form authentication **to identify users (Utiliser le formulaire d'authentification sécurisée pour identifier les utilisateurs)** pour présenter un formulaire de connexion sécurisée à l'utilisateur final. Lorsque l'utilisateur saisit son adresse électronique et son mot de passe de filtrage hybride, les informations d'identification sont envoyées par connexion sécurisée pour authentification.

  Si vous sélectionnez cette option, définissez la fréquence à laquelle les informations d'identification des utilisateurs doivent être à nouveau validées pour des raisons de sécurité sous Session Timeout (Expiration de la session). Les options par défaut sont 1, 7, 14 ou 30 jours. Le même délai d'expiration s'applique à Authentication Service, lorsque ce dernier est activé.

  > **Remarque**
  >
  > Il est possible d'étendre les options d'expiration de la session à 3 mois, 6 mois et 12 mois. Pour activer cette fonctionnalité étendue, contactez le Support technique.

  Si l'utilisateur ne s'est pas encore enregistré pour le service, il peut le faire à ce stade en cliquant sur l'option **Register (S'enregistrer)** dans le formulaire de connexion. Pour utiliser cette option, vous devez activer l'auto-enregistrement (configuré dans la page User Access (Accès utilisateur) sous Registered Domains (Domaines enregistrés)). Demandez aux utilisateurs de ne **pas** employer le même mot de passe pour le filtrage hybride et pour la connexion au réseau.

  Si vous ne sélectionnez ni l'option NTLM ni le formulaire d'authentification sécurisée, mais que vous activez l'option **Always authenticate users on first access (Authentifier systématiquement les utilisateurs lors du premier accès)**,

les utilisateurs qui ne peuvent pas s'identifier par un autre moyen obtiennent une invite de connexion chaque fois qu'ils accèdent à Internet. L'authentification de base sert à identifier les utilisateurs qui obtiennent une invite de connexion.

- Indiquez si une page d'accueil doit s'afficher ou non lorsque les utilisateurs, qui n'ont pas été identifiés via NTLM ou qui n'emploient pas le formulaire d'authentification sécurisée, ouvrent un navigateur pour se connecter à Internet. La page d'accueil :
  - Propose une sélection simple de moteurs de recherche courants pour aider l'utilisateur à démarrer
  - Est principalement utilisée par ceux qui se connectent au service hybride à partir d'un emplacement non filtré (par exemple lorsqu'ils travaillent chez eux ou sont en déplacement)

Lorsque vous avez terminé, 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)**.

Après avoir défini le filtrage hybride et configuré les navigateurs des utilisateurs pour qu'ils accèdent au fichier PAC, vous pouvez exploiter les liens fournis sous **Verify End User Configuration (Vérifier la configuration de l'utilisateur)** pour vérifier que les ordinateurs des utilisateurs ont accès à Internet et sont correctement configurés pour se connecter au service hybride.

Si votre compte de filtrage hybride n'a pas été vérifié (ce qui signifie qu'aucune adresse électronique n'a été saisie dans la page Paramètres > Général > Compte), les URL ne s'affichent pas.

Priorité et dérogation d'authentification

La page **Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs)** vous permet de sélectionner plusieurs options d'authentification pour vos utilisateurs. Les options sont classées par ordre de priorité comme suit :

- Lorsqu'il est installé dans un ordinateur client, Web Endpoint est systématiquement utilisé.
- Lorsque Web Endpoint n'est pas installé ou échoue, Authentication Service est utilisé dans les cas suivants :
  - Il a été déployé dans votre réseau, et
  - Il a été sélectionné dans la page Hybrid User Identification (Identification hybride des utilisateurs) pour un utilisateur filtré par le service hybride.
- Lorsque ni Web Endpoint ni Authentication Service ne sont disponibles, l'utilisateur est authentifié par le biais d'un formulaire d'authentification sécurisée, si :
  - Il a été sélectionné dans la page Hybrid User Identification (Identification hybride des utilisateurs), et
  - L'agent utilisateur ou l'application qui demande l'authentification prend en charge l'authentification à base de formulaire via une page HTML.
- Les applications qui ne reconnaissent pas l'authentification à base de formulaire utilisent soit l'identification NTLM, soit l'authentification de base. L'authentification de base est systématiquement utilisée lorsque l'option **Always authenticate users on first access (Authentifier systématiquement les utilisateurs lors du premier accès)** est sélectionnée et qu'aucune autre option n'est sélectionnée ou disponible.

Vous pouvez également imposer une option d'authentification spécifique à certains utilisateurs, par exemple à tous les utilisateurs d'une filiale, en déployant une URL de fichier PAC au format suivant :

```
http://hybrid-web.global.blackspider.com:8082/proxy.pac?a=X
```

Le paramètre a= contrôle l'option d'authentification, tandis que le paramètre X peut prendre l'une des valeurs suivantes :

Paramètre	Description
a=n	L'identification NTLM ou l'authentification de base est utilisée, selon les paramètres de stratégie et les possibilités du navigateur ou de l'application.
a=t	L'authentification est effectuée via Authentication Service. Si l'application ou l'agent utilisateur n'utilise pas Authentication Service, l'identification NTLM ou l'authentification de base est utilisée. Lorsqu'un utilisateur distant ne peut pas se connecter à Authentication Service, il a la possibilité de réessayer ou de se connecter via ses identifiants Websense.
a=f	L'authentification passe par un formulaire sécurisé.

Lorsque vous voulez que certains de vos utilisateurs s'identifient via Authentication Service et d'autres via l'authentification à base de formulaire sécurisé, il est conseillé de déployer des fichiers PAC comprenant le paramètre « a= ». En effet, ces deux méthodes utilisent des ports distincts dans le service hybride.

Présentation du déploiement de Web Endpoint

Websense Web Endpoint est un petit logiciel installé dans un ordinateur client. Il impose l'utilisation du service hybride pour le filtrage Web et transmet les informations d'authentification aux proxy hybrides, autorisant ainsi une authentification transparente et sécurisée.

Des versions 32 et 64 bits de Web Endpoint sont disponibles pour les systèmes d'exploitation suivants :

- Windows XP avec Service Pack 2 ou version ultérieure
- Windows Vista avec Service Pack 1 ou version ultérieure
- Windows 7

Pour déployer Web Endpoint dans des clients Windows, vous pouvez :

- Télécharger les fichiers d'installation, puis utiliser un Objet de stratégie de groupe Microsoft (GPO) ou un outil de distribution similaire pour déployer les fichiers dans les ordinateurs clients sélectionnés
- Télécharger ou copier les fichiers d'installation dans un ordinateur client, puis installer manuellement le logiciel Web Endpoint
- Déployer Web Endpoint dans certains ou tous les utilisateurs du filtrage hybride directement à partir du service hybride. Chaque utilisateur est alors invité à installer le logiciel Web Endpoint dans son ordinateur.

  Si l'utilisateur n'installe pas le logiciel Endpoint, il doit s'authentifier via les options que vous avez sélectionnées dans la page User Identification (Identification des utilisateurs). S'il est configuré, Websense Authentication Service est utilisé. Sinon,

le service hybride revient aux options d'identification ou d'authentification que vous avez sélectionnées ou, pour finir, à l'authentification de base. L'utilisateur est de nouveau invité à installer le logiciel Endpoint au démarrage de sa prochaine session de navigation.

Voir *Déploiement manuel de Web Endpoint pour Windows*, page 316.

Si vous utilisez TRITON - Data Security et que vous souhaitez déployer à la fois Web Endpoint et Data Endpoint dans les ordinateurs clients, vous devez utiliser le générateur de package fourni avec Data Security pour créer un package de déploiement pour Web Endpoint et Data Endpoint. Reportez-vous à la rubrique Installing and Deploying Websense Endpoints (Installation et déploiement des logiciels Websense Endpoint) du Centre Installation et déploiement.

Un certain nombre de protections protègent Endpoint contre les utilisations abusives et devraient éviter toute désinstallation ou suppression d'Endpoint par les utilisateurs finaux, y compris lorsqu'ils disposent de droits d'administrateurs locaux.

- Les fichiers et les dossiers Endpoint sont protégés contre la suppression et le changement de nom.
- Le processus Endpoint redémarre automatiquement lorsqu'il est interrompu ou arrêté.
- Un mot de passe est nécessaire pour désinstaller Endpoint ou arrêter le service Endpoint.
- Les paramètres de registre Endpoint ne peuvent pas être modifiés ni supprimés.
- La commande Service Control de suppression du service Endpoint est bloquée.

Vous devez définir le mot de passe d'anti-altération à utiliser pour arrêter ou désinstaller le service Endpoint avant de pouvoir télécharger le fichier installation ou d'activer le déploiement à partir du service hybride. Ce mot de passe est automatiquement lié à tous les déploiements d'Endpoint.

Important

Pour des raisons de sécurité, Websense ne conserve pas de copie de votre mot de passe d'anti-altération. Si vous oubliez ce mot de passe, vous pouvez le réinitialiser via la page Hybrid User Identification (Identification hybride des utilisateurs) en saisissant, puis en confirmant un nouveau mot de passe. Tous les logiciels Endpoint installés sont alors mis à jour et utilisent le nouveau mot de passe lors de leur prochaine connexion à Internet.

Pour activer le déploiement de Web Endpoint :

1. Dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs), cochez la case **Enable installation and update of Web Endpoint on client machines (Activer l'installation et la mise à jour de Web Endpoint dans les ordinateurs clients)**.

   L'activation de cette option vous permet de configurer le déploiement de Web Endpoint et les paramètres de mise à jour automatique. Si vous désactivez ensuite cette option, tous les clients Endpoint installés continuent à fonctionner jusqu'à leur désinstallation, mais ne bénéficient plus des mises à jour automatiques.
2. Saisissez, puis confirmez votre mot de passe d'anti-altération. Ce mot de passe doit comporter entre 4 et 25 caractères.
3. Choisissez une méthode de déploiement :

- Si vous voulez installer Web Endpoint manuellement dans des ordinateurs individuels ou par le biais de votre méthode de distribution favorite, cliquez sur **Deploy Web Endpoint Manually (Déployer Web Endpoint manuellement)**.

  Remarquez la commande GPO affichée à l'écran. Si vous envisagez d'utiliser un objet GPO pour distribuer Endpoint, servez-vous de cette commande dans votre script de déploiement. Voir *Déploiement manuel de Web Endpoint pour Windows*, page 316.

  Cliquez sur **View Web Endpoint Files (Afficher les fichiers Web Endpoint)** pour afficher les versions Endpoint qui conviennent à vos ordinateurs clients. Sélectionnez un système d'exploitation client, puis cliquez sur la version d'Endpoint à télécharger. Vous pouvez également consulter un fichier PDF présentant les notes de publication de chaque version en cliquant sur le lien de la version appropriée. Cliquez sur **Fermer** lorsque vous avez terminé.
- Pour déployer directement Endpoint à partir du service hybride, cochez la case **Deploy Web Endpoint from hybrid service proxies (Déployer Web Endpoint à partir des proxy du service hybride)**.

  Indiquez si Endpoint doit être déployé vers **tous les utilisateurs** filtrés par le service hybride ou vers les **utilisateurs hors site** uniquement.

  Vous pouvez faire en sorte qu'un message personnalisé soit présenté aux utilisateurs au début du processus de téléchargement et d'installation d'Endpoint. Ce message peut rassurer les utilisateurs en leur indiquant que le téléchargement est approuvé par la société et éventuellement leur fournir des informations nécessaires. Pour personnaliser ce message, cliquez sur **Paramètres avancés**, puis saisissez le nom de votre organisation et le texte à afficher. Cliquez sur **View Sample Page (Afficher l'exemple de page)** pour obtenir un aperçu de ce que verra l'utilisateur.

  L'exemple de page contient également le texte par défaut présenté systématiquement à l'utilisateur au début du téléchargement.

4. Cochez la case **Automatically update endpoint installations when a new version is released (Mettre automatiquement à jour les installations Endpoint lorsqu'une nouvelle version est disponible)** si vous voulez être certain que tous les logiciels Endpoint installés dans vos ordinateurs clients disposent de la version la plus récente dès sa mise à disposition via le service hybride.
5. 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)**.

Déploiement manuel de Web Endpoint pour Windows

Déploiement via un objet GPO

Pour déployer Web Endpoint via un Objet de stratégie de groupe (GPO) :

1. Créez un dossier partagé dans le contrôleur de domaine et définissez ses autorisations sur lecture seule.
2. Servez-vous d'un éditeur de texte pour créer un fichier de commandes (.bat) dans ce dossier partagé (par exemple **installwebep.bat**).
3. Entrez la commande msiexec suivante dans le fichier de commandes et enregistrez ce dernier.
4. Saisissez la **commande GPO** affichée dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs) de TRITON - Web Security.

5. Enregistrez et fermez le fichier.
6. Ouvrez la Console de gestion des stratégies de groupe (GPMC) et créez un nouvel objet GPO (ou ouvrez un objet existant) pour l'unité d'organisation dans laquelle résident les comptes de vos ordinateurs. Pour créer un nouvel objet GPO :
   a. Dans l'arborescence de la console, cliquez du bouton droit sur Objets de stratégie de groupe dans la forêt et le domaine dans lesquels vous souhaitez créer un objet de stratégie de groupe (GPO).
   b. Cliquez sur **Nouveau**.
   c. Dans la boîte de dialogue Nouvel objet GPO, entrez le nom du nouvel objet, puis cliquez sur **OK**.
7. Sélectionnez **Configuration ordinateur > Paramètres Windows > Scripts**, puis double-cliquez sur **Démarrage** dans le volet droit.
8. Cliquez sur **Ajouter**.
9. Dans le champ Nom du script, saisissez le chemin réseau complet et le nom du fichier de commandes que vous avez créé à l'étape 2, puis cliquez sur **OK** et fermez la console GPMC.
10. Exécutez la commande **gpupdate /force** à l'invite de commande pour actualiser la stratégie de groupe.

L'application s'installe au démarrage. Il est possible que le client ne soit pas entièrement fonctionnel avant d'avoir redémarré.

Déploiement dans un seul ordinateur

1. Copiez le fichier d'installation du client Endpoint dans un dossier temporaire de l'ordinateur client, puis décompressez-le.
2. Ouvrez une fenêtre d'invite de commande et naviguez jusqu'à l'emplacement des fichiers Endpoint décompressés.
3. Entrez la commande suivante :

   ```
   msiexec /package "Websense Endpoint.msi" /norestart
   WSCONTEXT=xxxx
   ```

   Remplacez « xxxx » par le code de configuration unique indiqué dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs) de TRITON - Web Security. Ce code fait partie de la chaîne **commande GPO**.

Déploiement de Websense Authentication Service

Websense Authentication Service est un ordinateur virtuel réseau qui authentifie l'identité, les attributs et les rôles des utilisateurs à l'aide des annuaires de l'entreprise. Toutes les communications entre les composants sont sécurisées.

Lorsque Authentication Service est installé dans votre réseau, les clients qui se connectent au proxy hybride à partir d'un emplacement filtré sont redirigés vers ce service. Dès qu'Authentication Service a authentifié un utilisateur grâce à votre service d'annuaire, cet utilisateur est redirigé vers le proxy et la stratégie appropriée s'applique. Les clients qui se sont déjà authentifiés une première fois n'ont plus besoin de le faire lors de leurs prochaines sessions de navigation Web.

Les utilisateurs hors site doivent saisir leur adresse électronique et leur mot de passe réseau chaque fois qu'ils se connectent au proxy hybride. Ces informations d'authentification sont vérifiées par Authentication Service et la stratégie appropriée s'applique ensuite pour cette session.

Pour plus d'informations, consultez le Guide d'installation et de configuration d'Authentication Service.

Pour télécharger et déployer Websense Authentication Service :

1. Dans la page **Paramètres > Hybrid Configuration (Configuration hybride) > Hybrid User Identification (Identification hybride des utilisateurs)**, cliquez sur **Authentication Service Files (Fichiers de Authentication Service)** pour afficher les téléchargements d'Authentication Service disponibles.

   Cliquez sur le nom d'un fichier pour télécharger cette version. Vous pouvez également consulter un fichier PDF présentant les notes de publication de chaque version en cliquant sur le lien de la version appropriée. Cliquez sur **Fermer** lorsque vous avez terminé.
2. Installez Authentication Service selon les instructions du Guide d'installation et de configuration d'Authentication Service.
3. Dans la page **Paramètres > Hybrid Configuration (Configuration hybride) > User Access (Accès utilisateur)**, téléchargez, puis installez le certificat SSL hybride afin que l'authentification transparente soit garantie auprès des sites HTTPS. Lorsque le certificat n'est pas installé pour les utilisateurs du service d'authentification, ces derniers doivent s'authentifier manuellement ou via l'identification NTLM, en fonction des paramètres définis dans la page Hybrid User Identification (Identification des utilisateurs du service hybride). Voir *Activation des pages de notification HTTPS*, page 218.
4. Après avoir installé et configuré Authentication Service et installé le certificat SSL dans les clients, copiez l'URL des métadonnées depuis la page Configuration > Fédération de la console Authentication Service, puis copiez-la dans le champ Metadata URL (URL des métadonnées) de la page Hybrid User Identification (Identification hybride des utilisateurs).
5. Pour tester le bon fonctionnement d'Authentication Service, configurez un client de sorte qu'il utilise l'une des URL de fichier PAC temporaire affichée sous Test Authentication Service (Tester Authentication Service).
   - Pour accéder au fichier PAC via le port 8082, utilisez l'URL **Fichier PAC (port 8082)**.
   - Pour accéder au fichier PAC via le port 80, utilisez l'URL **Fichier PAC (port 80)**.

   L'utilisateur de l'ordinateur client doit alors pouvoir accéder aux sites Web autorisés par sa stratégie sans saisir d'informations d'identification.

   Si vous obtenez une page d'erreur lors de la tentative d'accès au fichier PAC, assurez-vous d'avoir suivi toutes les étapes de la procédure du *Guide d'installation et de configuration d'Authentication Service*.
6. Cochez la case **Enable Authentication Service (Activer Authentication Service)** pour activer ce service dans tous les ordinateurs clients. Vérifiez que le client utilisé pour tester l'implémentation à l'étape 6 revient au fichier PAC standard.
7. Sous Session Timeout (Expiration de la session), définissez la fréquence à laquelle les informations d'identification des utilisateurs doivent être à nouveau validées pour des raisons de sécurité. Les options par défaut sont 1, 7, 14 ou 30 jours.

   Remarque

   Il est possible d'étendre les options d'expiration de la session à 3 mois, 6 mois et 12 mois. Pour activer cette fonctionnalité étendue, contactez le Support technique.
8. 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)**.

Websense Directory Agent

Dans les environnements Websense Web Security Gateway Anywhere, un composant d'interopérabilité intitulé **Websense Directory Agent** est requis si vous souhaitez activer le filtrage basé sur les utilisateurs, les groupes ou les domaines (unités d'organisation) via le service hybride.

Directory Agent doit être installé dans un ordinateur qui lui permette de communiquer avec :

- Votre service d'annuaire de type LDAP pris en charge (Windows Active Directory [Mode natif], Oracle Directory Server ou Novell eDirectory)

  Si votre organisation exploite Windows Active Directory en mode mixte, les données des utilisateurs et des groupes ne peuvent pas être récupérées et envoyées au service hybride.

- Websense Sync Service

Directory Agent peut être installé dans le même ordinateur que les autres composants Websense, y compris Sync Service et User Service.

Après le déploiement, servez-vous de TRITON - Web Security pour configurer Directory Agent pour la collecte des données à partir de votre service d'annuaire (voir *Envoi de données d'utilisateur et de groupe au service hybride*, page 220). Une fois configuré, Directory Agent récupère les données des utilisateurs et des groupes auprès de votre service d'annuaire et les envoie à Sync Service au format LDIF.

À intervalles planifiés (voir *Planification de la communication avec le filtrage hybride*, page 227), Sync Service envoie les informations des utilisateurs et des groupes collectées par Directory Agent au service hybride. Avant de les envoyer, Sync Service compresse les fichiers volumineux.

Directory Agent et User Service

Rubriques connexes :

- *Identification des utilisateurs du filtrage hybride*, page 311
- *Fonctionnement avec des utilisateurs et des groupes*, page 74
- *Services d'annuaire*, page 75
- *Envoi de données d'utilisateur et de groupe au service hybride*, page 220

Bien que Directory Agent collecte les informations de l'annuaire de manière autonome, il dépend toutefois fortement de User Service. Au moment de l'installation, Directory Agent doit se connecter à une instance de Policy Server associée à une instance de User Service. Directory Agent peut être configuré pour communiquer uniquement avec l'annuaire que cette instance de User Service doit utiliser.

En d'autres termes, dans un déploiement distribué, si vous utilisez plusieurs instances de Policy Server, chacune associée à une instance de User Service, et que les instances de User Service se connectent à des serveurs d'annuaire distincts, vous devez associer Directory Agent et l'instance de Policy Server à laquelle User Service se connecte à l'annuaire que vous souhaitez utiliser pour identifier les utilisateurs du filtrage hybride.

- Vous pouvez avoir plusieurs instances de Directory Agent.

- Chaque instance de Directory Agent doit être associée à une instance de Policy Server distincte.
- Toutes les instances de Directory Agent doivent se connecter à une même instance de Sync Service. (Le déploiement ne peut avoir qu'une seule instance de Sync Service.)

  Vous devez configurer manuellement la connexion à Sync Service de toutes les instances de Directory Agent supplémentaires. (La communication de l'instance de Directory Agent qui se connecte à l'instance de Policy Server en tant que Sync Service est configurée automatiquement.) Pour ce faire :

  1. Lorsque vous vous connectez à TRITON - Web Security, sélectionnez l'instance de Policy Server appropriée pour l'instance de Directory Agent que vous souhaitez configurer.
  2. Ouvrez la page Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées).
  3. Sous Synchronize User Data (Synchroniser les données des utilisateurs), vérifiez le **Nom ou l'adresse IP** de l'ordinateur Sync Service et le **Port** utilisé pour la communication avec Sync Service (par défaut, 55832).
  4. Pour vérifier que Directory Agent peut envoyer les données au service de synchronisation, cliquez sur **Test Connection (Tester la connexion)**. Ce test peut prendre une minute ou davantage de temps.
     - Lorsque la connexion est établie, un message confirme le succès de l'opération.
     - Si la connexion ne peut pas être établie, vérifiez l'adresse IP ou le nom d'hôte de l'ordinateur Sync Service, ainsi que le port de communication. Assurez-vous également que l'ordinateur Sync Service soit opérationnel, que le service de synchronisation s'exécute et que votre pare-feu réseau autorise les connexions au port de Sync Service.
  5. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

Directory Agent ne peut pas être configuré tant qu'il n'existe pas de configuration de User Service prise en charge. Les modifications apportées à la configuration de User Service peuvent également impliquer la mise à jour de votre configuration de Directory Agent.

- La configuration de User Service doit être effectuée dans la page Paramètres > Général > Directory Services (Services d'annuaire) (voir *Fonctionnement avec des utilisateurs et des groupes*, page 74).
- La configuration de Directory Agent doit être effectuée dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées) (voir *Envoi de données d'utilisateur et de groupe au service hybride*, page 220).

Vous pouvez configurer Directory Agent de sorte qu'il utilise un autre contexte racine que User Service et qu'il traite les données de l'annuaire différemment de ce dernier. De même, avec Windows Active Directory, si User Service est configuré pour communiquer avec plusieurs serveurs de catalogue global, Directory Agent peut communiquer avec l'ensemble de ces derniers.

Notez que, si vous avez plusieurs instances de Directory Agent, chacune d'elles doit utiliser un contexte racine unique, sans chevauchement.

Lorsque les utilisateurs ne sont pas identifiés

Rubriques connexes :

- *Identification des utilisateurs du filtrage hybride*, page 311
- *Fonctionnement des clients du filtrage hybride*, page 86

Si vous choisissez de ne pas déployer Directory Agent, Web Endpoint ni Authentication Service, ou si vous désactivez l'identification des utilisateurs, seuls 3 types de stratégies peuvent être appliqués aux utilisateurs :

- La stratégie appliquée à l'adresse IP externe à partir de laquelle l'utilisateur se connecte

  Cette adresse IP doit être définie en tant qu'emplacement filtré.
- La stratégie Par défaut de votre organisation, lorsque la demande provient d'un emplacement non filtré ou lorsque aucune stratégie d'ordinateur ou réseau n'a été appliquée à l'emplacement filtré.
- La stratégie Par défaut du filtrage hybride, lorsque la connexion de l'utilisateur ne peut pas être associée à votre organisation

  Cette situation, plutôt rare, ne peut se produire qu'en cas de problème de configuration lié à votre compte de filtrage hybride.

Les stratégies d'utilisateurs et de groupes ne peuvent pas être appliquées aux utilisateurs auto-enregistrés. Ces derniers sont systématiquement filtrés par la stratégie Par défaut (voir *Auto-enregistrement des utilisateurs hors site*, page 243).

15 Administration déléguée et génération de rapports

L'administration déléguée est un moyen efficace de répartir entre plusieurs personnes la charge de la configuration de la sécurité Web, de la gestion des accès Internet, de la génération de rapports sur l'activité Internet et de l'audit de la conformité. Par exemple :

- Laissez les différents responsables définir les stratégies et exécuter les rapports sur les utilisateurs de leurs équipes.
- Accordez des autorisations de gestion des stratégies aux administrateurs locaux des bureaux régionaux ou des campus, ainsi qu'un accès restreint aux options de configuration locale, tout en limitant l'accès aux rapports pour protéger la confidentialité de vos utilisateurs.
- Assurez-vous que le service des ressources humaines puissent exécuter les rapports de l'activité Internet pour certains ou la totalité des clients, identifiés par leur nom d'utilisateur ou leur adresse IP.
- Autorisez les auditeurs à afficher l'ensemble des écrans de gestion des stratégies et de configuration dans TRITON - Web Security sans les autoriser à enregistrer de modifications.

Les sections suivantes présentent les principaux concepts de l'administration déléguée, puis donnent des instructions spécifiques en matière de configuration et d'implémentation.

- *Principes fondamentaux de l'administration déléguée*, page 323
- *Préparation de l'administration déléguée*, page 330
- *Gestion des rôles d'administration déléguée*, page 335
- *Mise à jour des rôles d'administration déléguée*, page 344
- *Exécution des tâches d'administration déléguée*, page 346
- *Activation des comptes réseau*, page 351

Principes fondamentaux de l'administration déléguée

Rubriques connexes :

- *Rôles d'administration déléguée*, page 324
- *Administrateurs délégués*, page 325
- *Autorisations d'administration déléguée et de génération de rapports*, page 326
- *Administrateurs attribués à plusieurs rôles*, page 329
- *Accès de plusieurs administrateurs à TRITON - Web Security*, page 329

Avant de configurer l'administration déléguée pour votre organisation, vous devez comprendre 3 concepts clés :

- Les **Rôles** sont des conteneurs regroupant des **administrateurs** et des clients. Il existe 3 types de rôles. Voir *Rôles d'administration déléguée*, page 324.
- Les **Administrateurs** sont des individus ou des groupes chargés de configurer les paramètres de TRITON - Web Security, de gérer les stratégies associées aux clients, d'exécuter des rapports sur l'activité Internet ou de pratiquer des audits du système. Le jeu de responsabilités d'un administrateur dépend du **rôle** et des **autorisations** qui lui ont été attribués. Voir *Administrateurs délégués*, page 325.
- Les **Autorisations** déterminent les responsabilités (par exemple la création de stratégies ou l'exécution de rapports) d'un **administrateur** au sein d'un **rôle**. Les autorisations disponibles dépendent du type de rôle attribué à l'administrateur. Voir *Autorisations d'administration déléguée et de génération de rapports*, page 326.

Rôles d'administration déléguée

Un **rôle** regroupe des clients (utilisateurs, groupes, domaines (unités d'organisation), ordinateurs et réseaux) et un ou plusieurs administrateurs.

- Les clients associés à un rôle d'administration déléguée sont appelés **clients gérés**.
- Les administrateurs peuvent exécuter différentes tâches (par exemple gérer des stratégies ou générer des rapports) pour les clients gérés qui font partie de leur rôle, en fonction de leurs **autorisations**.

TRITON - Web Security comprend un rôle prédéfini : Super administrateur. Bien qu'il ne s'affiche pas, le rôle **admin** (compte Administrateur de sécurité globale) est membre de ce rôle. Le compte admin ne peut pas être délégué et ses autorisations ne sont pas modifiables.

Important

Vous ne pouvez pas supprimer le rôle de Super administrateur ni le compte admin.

Les administrateurs affectés au rôle Super administrateur peuvent créer des rôles, affecter des administrateurs et des clients gérés à des rôles, et identifier les autorisations des administrateurs au sein de ce rôle. Les Administrateurs de sécurité globale peuvent ajouter des administrateurs au rôle Super administrateur.

Les Super administrateurs peuvent créer deux types de rôle d'administration déléguée et de génération de rapports :

- **Gestion des stratégies et génération de rapports** : les stratégies des utilisateurs sont gérées par les administrateurs du rôle. Les administrateurs du rôle peuvent éventuellement aussi générer des rapports.
- **Rapports d'investigation** : les administrateurs peuvent générer des rapports d'investigation présentant l'activité Internet des clients gérés présents dans leur rôle uniquement. Les stratégies des clients sont gérées dans un ou plusieurs autres rôles.

Vous pouvez définir autant de rôles supplémentaires que nécessaire pour votre organisation. Par exemple :

- Vous pouvez créer un rôle pour chaque département, en désignant son responsable comme administrateur et ses membres comme clients gérés.
- Dans une organisation distribuée géographiquement, vous pouvez créer un rôle pour chaque site géographique et attribuer tous les utilisateurs de ce site en tant que clients gérés de ce rôle. Un ou plusieurs individus de ce même site peuvent ensuite être nommés administrateurs.

Administrateurs délégués

Les administrateurs sont les personnes autorisées à accéder à TRITON - Web Security. Selon les autorisations qui leur sont attribuées, ils peuvent effectuer les opérations suivantes :

- Se connecter et afficher certains éléments du tableau de bord Système, sans pouvoir exécuter d'autres actions
- Accéder à toutes les fonctionnalités de configuration et de gestion de TRITON - Web Security, sans pouvoir enregistrer de modifications
- Générer des rapports sur des groupes de clients spécifiques ou sur tous les clients
- Gérer les stratégies de groupes de clients spécifiques
- Disposer d'un accès complet à la configuration de toutes les fonctionnalités de TRITON - Web Security

Les autorisations disponibles dépendent du type de rôle de l'administrateur (Super administrateur, gestion des stratégies et génération de rapports ou rapports d'investigation). Voir *Rôles d'administration déléguée*, page 324.

Les administrateurs de sécurité globale (par exemple **admin**) définissent les comptes d'administrateur dans les paramètres de TRITON. Il peut s'agir de comptes de connexion réseau (définis dans un service d'annuaire pris en charge) ou de comptes locaux, exclusivement utilisés pour accéder à TRITON. Une fois qu'un compte a été défini, l'Administrateur de sécurité globale lui attribue un niveau d'accès à un ou plusieurs modules TRITON.

Les différents niveaux d'accès Web Security pouvant être attribués aux administrateurs sont les suivants :

- **Gestion des accès et des comptes**, correspondant aux autorisations des Super administrateurs inconditionnels (voir *Autorisations d'administration déléguée et de génération de rapports*, page 326)
- **Accès**, qui permet à l'administrateur de se connecter et d'afficher certaines parties des pages État > Tableau de bord et Alertes uniquement. Les Super administrateurs peuvent ajouter ces administrateurs à des rôles afin de leur accorder un certain niveau d'accès à la gestion des stratégies, à la génération de rapports, ou aux deux.

Tout compte d'administrateur autorisé à accéder au module Web Security apparaît dans la page Administration déléguée > View Administrator Accounts (Afficher les comptes d'administrateur). Ces comptes sont également répertoriés dans la page Administration déléguée > Modifier le rôle > Ajouter des administrateurs.

Seuls les administrateurs auxquels un accès à Web Security a déjà été accordé via les paramètres de TRITON peuvent être ajoutés à des rôles.

Autorisations d'administration déléguée et de génération de rapports

Les autorisations disponibles pour un administrateur varient selon si l'administrateur a été affecté au rôle de Super administrateur, de gestion des stratégies et de génération de rapports, ou de rapports d'investigation.

Autorisations du Super administrateur

Le rôle de Super administrateur peut contenir deux types d'administrateurs : Super administrateurs inconditionnels et Super administrateurs conditionnels.

Lorsque vous créez un compte d'administrateur de sécurité globale dans la page Paramètres > Administrateurs de TRITON ou lorsque vous sélectionnez l'accès **Web Security > Grant (Accorder) et la possibilité de modifier les autorisations d'accès des autres comptes**, le compte est automatiquement ajouté au rôle Super administrateur dans TRITON - Web Security, avec des autorisations inconditionnelles.

Les Super administrateurs inconditionnels peuvent :

- Accéder à la totalité des paramètres de configuration du système pour les solutions de sécurité Web Websense (gérés dans l'onglet Paramètres)
- Ajouter ou supprimer des administrateurs dans le rôle Super administrateur
- Créer ou modifier leVerrouillage du filtre qui bloque certaines catégories et certains protocoles pour tous les utilisateurs gérés par les rôles d'administration déléguée. Voir *Création d'un verrouillage du filtre*, page 332.
- Gérer les stratégies des clients du rôle Super administrateur, notamment la stratégie Par défaut appliquée à tous les clients non affectés à une autre stratégie dans un autre rôle
- Créer et générer des rapports sur tous les clients, quel que soit le rôle auquel ils sont affectés
- Accéder à Real-Time Monitor
- Consulter le journal d'audit, qui enregistre les accès de l'administrateur et les actions effectuées au sein de TRITON - Web Security
- (*Web Security Gateway* [*Anywhere*]) Ouvrir Content Gateway Manager via un bouton de la page Paramètres > Général > Content Gateway Access (Accès à Content Gateway) et se connecter automatiquement, sans avoir à fournir d'identifiants de connexion

Lorsqu'un Super administrateur inconditionnel ajoute d'autres administrateurs au rôle Super administrateur (via la page Gestion des stratégies > Administration déléguée dans TRITON - Web Security), des autorisations conditionnelles sont attribuées à ces nouveaux administrateurs.

Contrairement aux Super administrateurs inconditionnels, dont les autorisations ne sont pas modifiables, une certaine combinaison d'autorisations de gestion des stratégies, de génération de rapports et d'accès peuvent être attribuées aux Super administrateurs conditionnels.

- Les autorisations **Full policy (Stratégie complète)** permettent aux Super administrateurs conditionnels d'effectuer les opérations suivantes :
  - Créer et modifier les rôles d'administration déléguée, les composants du filtrage, les filtres, les stratégies et les exceptions, et appliquer des stratégies aux clients non gérés par d'autres rôles

- Accéder aux paramètres de téléchargement des bases de données, du service d'annuaire, d'identification des utilisateurs et de configuration de Network Agent. Les Super administrateurs conditionnels autorisés à générer des rapports peuvent également accéder aux paramètres de configuration des outils de rapports.
- Créer et modifier les rôles d'administration déléguée, mais pas supprimer les rôles, les administrateurs ou les clients gérés qui leur sont attribués

- Les autorisations **Exceptions only (Exceptions uniquement)** permettent aux Super administrateurs conditionnels de créer et de modifier des exceptions. (Les exceptions autorisent ou bloquent des URL pour les utilisateurs spécifiés, quelle que soit la stratégie de filtrage régissant habituellement leur accès à Internet.)

  Les pages de stratégies, de filtres, de composants de filtre, du verrouillage de filtres et toutes les pages Paramètres sont masquées pour les Super administrateurs qui disposent d'autorisations d'exceptions uniquement.
- Les autorisations **Reporting (Génération de rapports)** permettent aux Super administrateurs conditionnels d'effectuer les opérations suivantes :
  - Accéder aux graphiques du Tableau de bord Web Security
  - Générer des rapports d'investigation et de présentation sur tous les utilisateurs

  Si un administrateur est uniquement autorisé à générer des rapports, les options Créer une stratégie, Recatégoriser une URL et Débloquer une URL de la liste Tâches courantes ne s'affichent pas. De plus, l'option Vérifier la stratégie ne s'affiche pas dans la Boîte à outils.
- **Les autorisations Real-Time Monitor** permettent aux Super administrateurs de surveiller l'ensemble de l'activité du filtrage Internet pour chaque instance de Policy Server associée à TRITON - Web Security.
- Les autorisations **Accès direct à Content Gateway** permettent aux Super administrateurs de se connecter automatiquement à Content Gateway Manager par le biais d'un bouton de la page Paramètres > Général > Content Gateway Access (Accès à Content Gateway) dans TRITON - Web Security.

Un seul administrateur à la fois peut se connecter à un rôle disposant des autorisations **stratégie complète** ou **exceptions uniquement**. Par conséquent, lorsqu'un administrateur se connecte au rôle Super administrateur pour effectuer des tâches de stratégie ou de configuration, les autres Super administrateurs ne peuvent se connecter à ce rôle qu'avec des autorisations de génération de rapports, d'auditeur ou de surveillance de l'état. Les Super administrateurs ont également la possibilité de sélectionner un autre rôle à gérer.

Pour changer de rôle après votre connexion, sélectionnez-en un dans la liste déroulante **Rôle** de la barre d'outils Web Security.

Autorisations Gestion des stratégies et génération de rapports

Les administrateurs délégués appartenant aux rôles gestion des stratégies et génération de rapports peuvent se voir affecter toute combinaison des autorisations suivantes :

- Les autorisations **Full policy (stratégie complète)** permettent aux administrateurs délégués de créer et de gérer les composants des filtres (notamment les catégories personnalisées et les URL recatégorisées), les filtres (catégorie, protocole et accès limité), les stratégies et les exceptions (listes noire et blanche) de leurs clients gérés.

  Les filtres créés par les administrateurs délégués sont limités par le Verrouillage du filtre, qui peut désigner certains protocoles et catégories en tant que **bloqués et verrouillés**. Les administrateurs délégués ne peuvent pas autoriser ces catégories et protocoles.

Un seul administrateur à la fois peut se connecter à un rôle disposant d'autorisations sur les stratégies. Par conséquent, lorsqu'un administrateur se connecte à un rôle pour effectuer des tâches de stratégie, les autres administrateurs du rôle peuvent uniquement se connecter avec des autorisations d'audit (lecture seule), de génération de rapports ou Real-Time Monitor. Les administrateurs affectés à plusieurs rôles ont également la possibilité de sélectionner un autre rôle à gérer.

Pour changer de rôle après votre connexion, sélectionnez-en un dans la liste déroulante **Rôle** de la bannière.

- Les autorisations **Exceptions only (Exceptions uniquement)** permettent aux administrateurs délégués de créer et de gérer des exceptions pour les clients gérés de leur rôle. (Les exceptions autorisent ou bloquent des URL pour les utilisateurs spécifiés, quelle que soit la stratégie de filtrage régissant habituellement leur accès à Internet.)

  Les stratégies, les filtres et les composants de filtres sont masqués pour les administrateurs délégués qui disposent d'autorisations d'exceptions uniquement.

- Des autorisations de génération de rapports peuvent être accordées dans l'une des deux catégories générales : rapport sur **tous les clients** ou rapport sur les **clients gérés uniquement** du rôle.
  - Tout administrateur délégué disposant d'autorisations de génération de rapports peut être autorisé à accéder au Tableau de bord de Web Security, aux rapports d'investigation et aux pages de paramètres qui permettent de gérer Log Server et la base de données d'activité.
  - Les administrateurs délégués autorisés à générer des rapports sur tous les clients peuvent également accéder aux rapports de présentation.
- Les autorisations **Real-Time Monitor** permettent aux administrateurs de surveiller l'ensemble de l'activité du filtrage Internet pour chaque instance de Policy Server associée à TRITON - Web Security.

Autorisations Rapports d'investigation

Les administrateurs appartenant aux rôlesrapports d'investigation peuvent créer des rapports d'investigation pour les clients gérés dans leur rôle. (Les stratégies des clients sont gérées dans d'autres rôles.) Ils peuvent également exploiter les outils Catégorie d'URL, Accès à l'URL et Analyser l'utilisateur.

Ces administrateurs n'ont pas accès aux rapports de présentation ni à Real-Time Monitor, mais peuvent éventuellement être autorisés à consulter les graphiques du Tableau de bord Web Security.

Auditeurs

Tout Super administrateur conditionnel ou administrateur délégué peut se voir attribuer des autorisations d'**Auditeur**. Un auditeur peut voir toutes les fonctionnalités et fonctions de TRITON - Web Security non disponibles pour les autres administrateurs, mais ne peut pas enregistrer de modifications.

À la place des boutons OK et Annuler, qui permettent aux autres administrateurs de mettre les modifications en cache ou de les annuler, les Auditeurs disposent d'un seul bouton de retour en arrière. Le bouton Save and Deploy (Enregistrer et déployer) est désactivé pour eux.

Administrateurs attribués à plusieurs rôles

Rubriques connexes :

- *Rôles d'administration déléguée*, page 324
- *Administrateurs délégués*, page 325
- *Autorisations d'administration déléguée et de génération de rapports*, page 326

Selon les besoins de votre organisation, le même administrateur peut être attribué à plusieurs rôles. Lors de leur connexion, les administrateurs attribués à plusieurs rôles doivent choisir un unique rôle à gérer.

Après la connexion, vos autorisations sont les suivantes :

- **Gestion des stratégies** :
  - **Full policy (stratégie complète)** : vous pouvez ajouter et modifier des filtres et des stratégies pour le rôle sélectionné lors de la connexion, et appliquer des stratégies aux clients gérés par ce rôle.
  - **Exceptions only (exceptions uniquement)** : vous pouvez créer et gérer des exceptions pour le rôle sélectionné lors de la connexion, et appliquer des exceptions aux clients gérés par ce rôle.
- **Génération de rapports** : vous disposez des autorisations de génération de rapports combinées de tous vos rôles. Supposons par exemple que trois rôles vous soient attribués, avec les autorisations de génération de rapports suivantes :
  - Rôle 1 : pas de génération de rapports
  - Rôle 2 : rapports d'investigation uniquement
  - Rôle 3 : rapports sur tous les clients, accès complet à toutes les fonctions de génération de rapports

  Dans ce cas, quel que soit le rôle choisi au moment de la connexion, vous êtes autorisé(e) à consulter les graphiques du Tableau de bord Web Security et à générer des rapports sur tous les clients, à l'aide de toutes les fonctions de rapports.

  Si vous êtes connecté(e) pour la génération de rapports uniquement, le champ Rôle de la barre de la bannière précise si vous disposez d'une autorisation Génération de rapports complète (rapports sur tous les clients) ou Génération de rapports limitée (rapports sur les clients gérés uniquement).

Accès de plusieurs administrateurs à TRITON - Web Security

Les administrateurs de **différents** rôles peuvent accéder simultanément à TRITON - Web Security pour exécuter leurs tâches autorisées. Comme ils gèrent des clients différents, ils peuvent créer et appliquer des stratégies sans provoquer de conflits.

La situation est différente lorsque plusieurs administrateurs disposant d'autorisations de stratégie au sein du **même** rôle tentent de se connecter simultanément. **Un seul administrateur à la fois** peut se connecter au rôle partagé avec des autorisations de stratégie complète ou d'exceptions uniquement. Lorsqu'un second administrateur tente de se connecter avec les mêmes autorisations alors qu'un autre est déjà connecté, il peut choisir d'effectuer les opérations suivantes :

- Se connecter en lecture seule (ce qui correspond à des autorisations d'auditeur temporaire)

Lorsque cette option est sélectionnée, la liste déroutante Rôle propose « Nom du rôle - [Lecture seule] » en tant que rôle actuel et la possibilité de basculer vers le rôle « Nom du rôle » (sans aucune modification possible). Cela permet ensuite d'accéder au rôle avec des autorisations de stratégie lorsque ce rôle n'est plus verrouillé.

- Se connecter pour la génération de rapports uniquement, s'il dispose des autorisations appropriées
- Se connecter à un rôle différent, s'il est attribué à d'autres rôles
- Se connecter pour afficher uniquement les pages d'état jusqu'à ce que le rôle redevienne disponible (accès État limité)
- Se reconnecter ultérieurement, après la déconnexion du premier administrateur

Les administrateurs qui n'utilisent pas leurs autorisations de stratégie peuvent effectuer l'une des opérations suivantes pour déverrouiller le rôle et autoriser un autre administrateur à se connecter pour gérer les stratégies :

- Dans le cas de l'autorisation de génération de rapports, sélectionnez **Libérer les autorisations de stratégie** dans la liste déroulante **Rôle**.

  Lorsque cette option est activée, les fonctionnalités de gestion des stratégies sont masquées pour l'administrateur connecté, mais les fonctionnalités de génération de rapports demeurent actives.
- Pour la surveillance des performances du système, sélectionnez **Status Monitor (Moniteur d'état)** dans la liste déroulante **Rôle**.

  En mode Status Monitor (Moniteur d'état), les administrateurs peuvent accéder aux pages État > Tableau de bord et Alertes, ainsi qu'à Real-Time Monitor (le cas échéant). Leur session n'expire pas.

  Lorsque des administrateurs tentent de se connecter en mode Status Monitor (Moniteur d'état) à une autre page que Tableau de bord, Alertes ou Real-Time Monitor, ils sont de nouveaux invités à se connecter.

Préparation de l'administration déléguée

Rubriques connexes :

- *Principes fondamentaux de l'administration déléguée*, page 323
- *Création d'un verrouillage du filtre*, page 332
- *Préparation des administrateurs délégués*, page 334
- *Gestion des rôles d'administration déléguée*, page 335

Avant de créer des rôles d'administration déléguée, le Super administrateur doit effectuer deux tâches clés de planification et de configuration :

- Vérifiez et modifiez le Verrouillage du filtre, qui bloque les catégories et les protocoles spécifiés pour les clients gérés de tous les rôles d'administration déléguée. Le Verrouillage du filtre bloquant et verrouillant par défaut plusieurs catégories, il est important de vérifier que les paramètres par défaut conviennent à votre organisation. (Voir *Création d'un verrouillage du filtre*, page 332.)

- Les restrictions du Verrouillage du filtre sont automatiquement imposées à tous les filtres créés ou copiés dans un rôle d'administration déléguée, et ne sont pas modifiables par l'administrateur délégué.
- Les administrateurs délégués peuvent appliquer n'importe quelle action de filtrage aux catégories et aux protocoles **non** bloqués et verrouillés par le Verrouillage du filtre.
- Les modifications apportées au Verrouillage du filtre sont implémentées pour tous les clients gérés dès l'enregistrement des modifications. Les administrateurs délégués connectés à TRITON - Web Security lorsque les modifications prennent effet ne voient pas les changements avant leur prochaine connexion.
- Les restrictions du Verrouillage du filtre ne s'appliquent pas aux clients gérés par le rôle Super administrateur.

◆ Identifiez les stratégies et filtres de Super administrateur devant être copiés dans chaque nouveau rôle que vous envisagez de créer, puis modifiez les stratégies existantes en fonction de vos besoins.

- Par défaut, chaque rôle est créé avec une seule stratégie Par défaut, créée à partir du filtre de catégories et de protocoles Par défaut (**pas** la stratégie Par défaut), actuellement configurée pour le rôle Super administrateur.
- Vous pouvez également copier tous les objets de stratégie (stratégies, filtres, catégories personnalisées et URL personnalisées) du rôle Super administrateur dans le nouveau rôle. L'administrateur délégué commence alors avec un jeu complet de stratégies et de composants de stratégie.
  - Les copies de stratégies et de filtres d'un rôle d'administration déléguée sont soumises au Verrouillage du filtre et ne sont donc pas identiques aux stratégies et aux filtres équivalents du rôle Super administrateur.
  - Lorsque la stratégie non limitée est copiée, les noms de stratégie **et** de filtres sont modifiés de manière à indiquer que la stratégie est soumise au Verrouillage du filtre et n'autorise plus toutes les requêtes.

  Selon le volume d'informations concerné, copier les objets de stratégie Super administrateur dans un nouveau rôle peut prendre beaucoup de temps.

Dès que ces étapes de planification sont terminées, chacun des composants d'administration déléguée suivants doit être mis en vigueur :

1. Un Administrateur de sécurité globale crée des comptes d'administrateur dans la page Paramètres > Administrateurs de TRITON et leur accorde le niveau d'accès approprié à Web Security.
2. Un Super administrateur crée des rôles d'administration déléguée dans la page Gestion des stratégies > Administration déléguée, puis ajoute des administrateurs et des clients gérés à ces rôles. Voir *Gestion des rôles d'administration déléguée*, page 335.
3. Le Super administrateur prévient les administrateurs délégués qu'un accès administratif à TRITON - Web Security leur a été accordé et leur détaille leur niveau d'autorisations. Voir *Préparation des administrateurs délégués*, page 334.

Création d'un verrouillage du filtre

Rubriques connexes :

- *Verrouillage de catégories*, page 332
- *Verrouillage de protocoles*, page 333

La page **Gestion des stratégies > Verrouillage du filtre** vous permet de définir des catégories et protocoles bloqués pour tous les clients gérés des rôles d'administration déléguée. Tout élément (catégorie ou protocole) bloqué dans le Verrouillage du filtre est considéré comme **bloqué et verrouillé**.

- Cliquez sur le bouton **Catégories** pour bloquer et verrouiller des catégories ou des éléments de catégorie spécifiques (mots-clés et types de fichiers). Voir *Verrouillage de catégories*, page 332.
- Cliquez sur le bouton **Protocoles** pour bloquer et verrouiller des protocoles, ou définir les protocoles systématiquement consignés dans le journal. Voir *Verrouillage de protocoles*, page 333.

Verrouillage de catégories

Rubriques connexes :

- *Création d'un verrouillage du filtre*, page 332
- *Verrouillage de protocoles*, page 333

La page **Gestion des stratégies > Verrouillage du filtre > Catégories** permet de sélectionner des catégories à bloquer et à verrouiller pour tous les membres des rôles d'administration déléguée. Vous pouvez également bloquer et verrouiller des mots-clés et des types de fichiers pour une catégorie.

1. Sélectionnez une catégorie dans l'arborescence.

   Les rôles d'administration déléguée n'ont pas accès aux catégories personnalisées créées par les Super administrateurs. Les catégories personnalisées n'apparaissent donc pas dans cette arborescence.
2. Définissez les restrictions de cette catégorie dans le champ qui apparaît à côté de l'arborescence des catégories.

Option	Description
Verrouiller la catégorie	Bloque et verrouille l'accès aux sites de cette catégorie
Verrouiller des mots-clés	Bloque et verrouille l'accès en fonction des mots-clés définis pour cette catégorie dans chaque rôle

Option	Description
Verrouiller des types de fichiers	Bloque et verrouille les types de fichiers sélectionnés pour les sites de cette catégorie Assurez-vous de cocher la case de chaque type de fichier à bloquer et à verrouiller. Les types de fichiers personnalisés créés par le Super administrateur sont inclus dans cette liste, car ils sont disponibles pour les rôles d'administration déléguée.
Appliquer aux sous-catégories	Applique les mêmes paramètres à toutes les sous-catégories de cette catégorie

Au besoin, vous pouvez bloquer et verrouiller des éléments sélectionnés pour toutes les catégories en même temps. Sélectionnez **Toutes les catégories** dans l'arborescence, puis les éléments à bloquer pour toutes les catégories. Cliquez ensuite sur **Appliquer aux sous-catégories**.

3. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Verrouillage du filtre. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Verrouillage de protocoles

Rubriques connexes :

- *Création d'un verrouillage du filtre*, page 332
- *Verrouillage de catégories*, page 332

La page **Gestion des stratégies > Verrouillage du filtre > Protocoles** permet de bloquer et de verrouiller l'accès ou de verrouiller la journalisation des protocoles sélectionnés pour tous les clients gérés par les rôles d'administration déléguée.

Remarque

La journalisation des protocoles est associée aux alertes d'utilisation des protocoles. Vous ne pouvez pas générer d'alertes d'utilisation d'un protocole si ce dernier n'est pas défini pour la journalisation dans au moins un filtre de protocoles. L'activation de l'option **Verrouiller la journalisation du protocole** via le verrouillage du filtre permet de s'assurer que des alertes d'utilisation pourront être générées pour ce protocole. Voir *Configuration des alertes d'utilisation de protocole*, page 382.

1. Sélectionnez un protocole dans l'arborescence.

   Les rôles d'administration déléguée ont accès aux protocoles personnalisés créés par le Super administrateur. Les protocoles personnalisés apparaissent donc dans cette arborescence.

2. Définissez les restrictions de ce protocole dans le champ qui apparaît à côté de l'arborescence des protocoles.

Option	Description
Verrouiller le protocole	Bloque et verrouille l'accès aux applications et aux sites Web qui utilisent ce protocole
Verrouiller la journalisation du protocole	Journalise les informations liées à l'accès à ce protocole et empêche les administrateurs délégués de désactiver cette journalisation
Appliquer au groupe	Applique les mêmes paramètres à tous les protocoles du groupe

Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Verrouillage du filtre. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Préparation des administrateurs délégués

Rubriques connexes :

- *Principes fondamentaux de l'administration déléguée*, page 323
- *Préparation de l'administration déléguée*, page 330
- *Exécution des tâches d'administration déléguée*, page 346

Après avoir attribué des individus en tant qu'administrateurs dans un rôle d'administration, assurez-vous de leur fournir les informations suivantes :

- L'URL permettant de se connecter à TRITON - Web Security. Par défaut :

  ```
  https://<emplacement de TRITON>:9443/triton/
  ```

  Remplacez l'emplacement par l'adresse IP ou le nom d'hôte de l'ordinateur exécutant TRITON - Web Security.
- L'instance de Policy Server à sélectionner après la connexion, le cas échéant. Dans un environnement qui regroupe plusieurs instances de Policy Server, les administrateurs peuvent sélectionner celle à utiliser dans la barre d'outils Web Security. Ils doivent dans ce cas choisir le serveur Policy Server configuré pour communiquer avec le service d'annuaire qui authentifie leurs clients gérés.
- S'ils doivent utiliser leur compte de connexion réseau ou un compte Websense local pour se connecter à TRITON - Web Security. Si des administrateurs se connectent avec des comptes locaux, fournissez-leur un nom d'utilisateur et un mot de passe.
- Leurs autorisations : créer et appliquer des stratégies aux clients du rôle, générer des rapports, créer des stratégies et générer des rapports, ou auditer les tâches d'administration sans implémenter de modification.

  Conseillez aux administrateurs qui disposent à la fois des autorisations de stratégie et de génération de rapports de tenir compte des activités qu'ils prévoient d'effectuer au cours de leur session. S'ils prévoient uniquement de générer des rapports, conseillez-leur d'accéder au champ **Rôle** dans la bannière et de choisir

Libérer les autorisations de stratégie. Cette option libère les autorisations de stratégie pour le rôle, ce qui permet à un autre administrateur d'accéder à TRITON - Web Security et de gérer une stratégie pour ce rôle.

- Comment trouver la liste des clients gérés par leur rôle. Les administrateurs peuvent ouvrir la page Gestion des stratégies > Administration déléguée et cliquer sur le nom de leur rôle pour afficher la page Modifier le rôle, qui présente la liste de leurs clients gérés.
- Les limites imposées par le Verrouillage du filtre, lorsque des catégories ou des protocoles ont été bloqués et verrouillés.
- Les tâches généralement effectuées par les administrateurs. Voir *Exécution des tâches d'administration déléguée*, page 346.

N'oubliez pas d'avertir les administrateurs délégués lorsque vous ajoutez ou modifiez des protocoles et des types de fichiers personnalisés. Ces composants s'affichant automatiquement dans les filtres et les stratégies de tous les rôles, il est donc important que ces administrateurs sachent que des modifications ont été apportées.

Gestion des rôles d'administration déléguée

Rubriques connexes :

- *Principes fondamentaux de l'administration déléguée*, page 323
- *Préparation de l'administration déléguée*, page 330
- *Gestion des conflits entre rôles*, page 343

La page **Gestion des stratégies > Administration déléguée** propose des options différentes selon si elle est affichée par un Super administrateur ou par un administrateur délégué.

Les Super administrateurs voient la liste de tous les rôles actuellement définis et disposent des options suivantes.

Option	Description
Ajouter	Cliquez sur cette option pour ajouter un nouveau rôle. Voir *Ajout de rôles*, page 336.
Rôle	Cliquez sur le nom d'un rôle pour l'afficher ou le configurer. Voir *Modification des rôles*, page 337.
Supprimer	Cochez la case accolée au nom d'un rôle, puis cliquez sur le bouton pour supprimer le(s) rôle(s) sélectionné(s). Cette option n'est disponible que pour les Super administrateurs inconditionnels. Pour plus d'informations sur la gestion des clients après la suppression d'un rôle, consultez la section *Suppression de rôles*, page 345.
Avancé	Cliquez sur cette option pour accéder à la fonction Gérer la priorité des rôles.

Option	Description
Gérer la priorité des rôles	Cliquez sur cette option pour définir les paramètres de stratégie du rôle devant être utilisés lorsque le même client est membre de plusieurs groupes gérés par des rôles différents. Voir *Gestion des conflits entre rôles*, page 343.
View Administrator Accounts (Afficher les comptes d'administrateur)	Cliquez sur cette option pour afficher les comptes d'administrateur, locaux et réseau, qui disposent d'un accès à TRITON - Web Security et vérifier leur niveau d'autorisations et leur affectation à des rôles. Voir *Vérification des comptes d'administrateur*, page 351.

Les administrateurs délégués ne voient que les rôles dont ils sont administrateurs et disposent d'options limitées.

Option	Description
Rôle	Cliquez sur cette option pour afficher les clients attribués au rôle et les autorisations de génération de rapports spécifiques accordées. Voir *Modification des rôles*, page 337.

Ajout de rôles

Rubriques connexes :

- *Préparation de l'administration déléguée*, page 330
- *Gestion des rôles d'administration déléguée*, page 335
- *Modification des rôles*, page 337

La page **Administration déléguée** > **Ajouter un rôle** permet d'entrer le nom et la description du nouveau rôle.

1. Entrez le **Nom** du nouveau rôle.

   Le nom doit comprendre entre 1 et 50 caractères et ne peut inclure aucun des caractères suivants :

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

   Les noms de rôle peuvent comprendre des espaces et des tirets.

2. Entrez la **Description** du nouveau rôle.

   Cette description peut comprendre jusqu'à 255 caractères. Les restrictions de caractères qui s'appliquent aux noms de rôle s'appliquent également aux descriptions, à deux exceptions près : les descriptions peuvent inclure des points (.) et des virgules (,).

3. Définissez le **Type de rôle** :

   - Un rôle **Gestion des stratégies et génération de rapports** permet aux administrateurs de créer des filtres et des stratégies et de les appliquer aux clients gérés. Les administrateurs de ces rôles peuvent également être autorisés à générer des rapports sur les clients gérés ou sur tous les clients.

Si vous sélectionnez ce type de rôle, choisissez également éventuellement de **Copy all Super Administrator policies, filters, and filter components to the new role (Copier l'ensemble des stratégies, filtres et composants de filtre du Super administrateur dans le nouveau rôle)**. Si vous sélectionnez cette option, le processus de création du rôle peut prendre quelques minutes.

Si vous ne copiez pas toutes les stratégies du Super administrateur dans le rôle, une stratégie Par défaut est créée pour ce rôle et impose les filtres de catégories et de protocoles par défaut du Super administrateur.

- Le rôle **Rapports d'investigation** permet aux administrateurs de générer des rapports sur leurs clients gérés uniquement, à l'aide de l'outil des rapports d'investigation. Les clients gérés par un rôle de rapports d'investigation peuvent également être ajoutés dans un rôle de gestion des stratégies et de génération de rapports.

4. Cliquez sur **OK** pour afficher la page **Modifier le rôle** et définir les caractéristiques de ce rôle. Voir *Modification des rôles*, page 337.
   - Si vous avez créé un rôle de gestion des stratégies et de génération de rapports, le nouveau rôle s'affiche dans la liste déroulante Rôle de la barre d'outils Web Security dès votre prochaine connexion.
   - Si vous avez créé un rôle de rapports d'investigation, le nom de ce rôle ne s'affiche pas dans la liste déroulante des rôles. Cela est dû au fait que les autorisations de génération de rapports sont cumulatives (voir *Administrateurs attribués à plusieurs rôles*, page 329).

Modification des rôles

Rubriques connexes :

- *Gestion des rôles d'administration déléguée*, page 335
- *Ajout de rôles*, page 336
- *Gestion des conflits entre rôles*, page 343

Les administrateurs délégués peuvent utiliser la page **Administration déléguée** > **Modifier le rôle** pour consulter la liste des clients gérés par leur rôle, et les autorisations de génération de rapports spécifiques accordées.

Les Super administrateurs peuvent utiliser cette page pour sélectionner les administrateurs et les clients d'un rôle, et définir les autorisations des administrateurs, tel que décrit ci-dessous. Seuls les Super administrateurs inconditionnels peuvent supprimer des administrateurs et des clients dans un rôle.

1. Modifiez le **Nom** et la **Description** du rôle, selon vos besoins.

   Le nom du rôle Super administrateur ne peut pas être modifié.

2. Ajoutez ou supprimez des administrateurs dans ce rôle (Super administrateurs uniquement).

Élément	Description
Nom d'utilisateur	Nom d'utilisateur de l'administrateur
Type de compte	Indique si l'utilisateur est défini dans le service d'annuaire réseau (Annuaire) ou est unique dans la console TRITON (Local)

Élément	Description
Génération de rapports	Autorise l'administrateur à utiliser les outils de génération de rapports
Real-Time Monitor	Autorise l'administrateur à surveiller toute l'activité du filtrage Internet pour n'importe quelle instance de Policy Server
Stratégie	Autorise l'administrateur à créer des filtres et des stratégies, et à appliquer les stratégies aux clients gérés par son rôle Dans le rôle Super administrateur, les administrateurs disposant d'une autorisation de stratégie peuvent également gérer certains paramètres de configuration de Websense. Voir *Autorisations du Super administrateur*, page 326.
Auditeur	Autorise l'administrateur à afficher l'ensemble des fonctionnalités et fonctions à la disposition des autres administrateurs du rôle, sans possibilité d'enregistrer des modifications. Les cases à cocher des autres autorisations sont désactivées lorsque les autorisations Auditeur sont sélectionnées.
Ajouter	Ouvre la page **Ajouter des administrateurs**. Voir *Ajout d'administrateurs*, page 340.
Supprimer	Retire les administrateurs sélectionnés du rôle • Cette option n'est disponible que pour les Super administrateurs inconditionnels. • Les comptes de Super administrateur inconditionnel ne peuvent être supprimés que dans la page Paramètres > Administrateurs de TRITON.

3. Ajoutez et supprimez des **Clients gérés** pour le rôle.

   Seuls les Super administrateurs peuvent apporter des modifications. Les administrateurs délégués peuvent consulter les clients attribués à leur rôle.

Élément	Description
<Nom>	Affiche le nom de chaque client attribué explicitement au rôle. Les administrateurs du rôle doivent ajouter les clients dans la page Clients avant que des stratégies ne puissent être appliquées. Voir *Exécution des tâches d'administration déléguée*, page 346.
Ajouter	Ouvre la page **Ajouter des clients gérés**. Voir *Ajout de clients gérés*, page 342.
Supprimer	Disponible uniquement pour les Super administrateurs inconditionnels, ce bouton retire du rôle tous les clients cochés dans la liste des clients gérés. Certains clients ne peuvent pas être retirés directement de la liste des clients gérés. Pour plus d'informations, consultez la section *Suppression de clients gérés*, page 345.

4. Utilisez la zone **Autorisations de génération de rapports** pour sélectionner les fonctions disponibles aux administrateurs de ce rôle qui disposent d'un droit d'accès à la génération de rapports.

a. Choisissez le niveau général des autorisations de génération de rapports :

Option	Description
Rapport sur tous les clients	Sélectionnez cette option pour autoriser les administrateurs à générer des rapports sur tous les utilisateurs du réseau. Servez-vous des options restantes de la zone Autorisations de génération de rapports pour définir des autorisations spécifiques pour les administrateurs de ce rôle.
Rapport sur les clients gérés uniquement	Sélectionnez cette option pour limiter les administrateurs à la génération de rapports sur les clients gérés attribués à ce rôle. Sélectionnez ensuite les fonctions de rapports d'investigation auxquels ces administrateurs peuvent accéder. Les administrateurs limités à la génération de rapports sur les clients gérés ne peuvent pas accéder aux rapports de présentation ni aux rapports basés sur les utilisateurs dans le Tableau de bord Web Security.

b. Cochez la case de chaque fonction de génération de rapports que les administrateurs du rôle peuvent utiliser.

Option	Description
Accéder aux rapports de présentation	Permet d'accéder aux fonctions des rapports de présentation. Cette option n'est disponible que si les administrateurs peuvent générer des rapports sur tous les clients. Voir *Rapports de présentation*, page 131.
Accès au Tableau de bord de Web Security	Active l'affichage des graphiques présentant l'activité Internet dans les tableaux de bord Risques, Usage et Système. Voir *Tableau de bord de Web Security*, page 33. Si cette option est désactivée, les administrateurs ne peuvent afficher que les sections Alertes d'état et Value Estimates (Estimations de l'utilité) (si affichées) du tableau de bord Système.
Accès au tableau de bord Menaces	Permet aux administrateurs d'accéder aux graphiques, au tableau récapitulatif et aux détails des événements liés au contenu malveillant avancé détecté dans votre réseau. Voir *Tableau de bord Threats (Menaces)*, page 35.
Accéder aux données d'analyse du tableau de bord Menaces	Avec Websense Web Security Gateway ou Gateway Anywhere, permet aux administrateurs d'afficher les fichiers associés à l'activité des menaces et de consulter des informations sur les tentatives d'envoi de fichiers. Voir *Configuration du stockage des données d'analyse*, page 420.
Accéder aux rapports d'investigation	Permet d'accéder aux fonctions de base des rapports d'investigation. Lorsque cette option est activée, d'autres fonctions de rapports d'investigation peuvent également être sélectionnées. Voir *Rapports d'investigation*, page 152.

Option	Description
Afficher les noms d'utilisateur dans les rapports d'investigation	Permet aux administrateurs de ce rôle d'afficher les noms d'utilisateur, s'ils sont connectés. Voir *Configuration du mode de journalisation des requêtes filtrées*, page 398. Désactivez cette option pour n'afficher que les codes d'identification générés par le système à la place des noms. Cette option n'est disponible que si les administrateurs sont autorisés à accéder aux rapports d'investigation.
Enregistrer les rapports d'investigation comme favoris	Permet aux administrateurs de ce rôle de créer des rapports d'investigation favoris. Voir *Rapports d'investigation favoris*, page 169. Cette option n'est disponible que si les administrateurs sont autorisés à accéder aux rapports d'investigation.
Planifier les rapports d'investigation	Permet aux administrateurs de ce rôle de planifier l'exécution ultérieure ou périodique de rapports d'investigation. Voir *Planification des rapports d'investigation*, page 172. Cette option n'est disponible que si les administrateurs sont autorisés à enregistrer les rapports d'investigation comme favoris.
Gérer Log Server et la base de données d'activité	Permet aux administrateurs d'accéder aux pages Paramètres > Génération de rapports > Log Server et Base de données d'activité. Voir *Configuration de Log Server*, page 400, et *Paramètres d'administration de la base de données d'activité*, page 408.

5. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Administration déléguée. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout d'administrateurs

Rubriques connexes :

- *Administrateurs délégués*, page 325
- *Modification des rôles*, page 337

Les Super administrateurs peuvent utiliser la page **Administration déléguée > Modifier le rôle** > **Ajouter des administrateurs** pour désigner les administrateurs d'un rôle.

Remarque

Des administrateurs peuvent être ajoutés à plusieurs rôles. Ces administrateurs doivent alors choisir un rôle lors de leur connexion. Dans ce cas, l'administrateur dispose d'autorisations de génération de rapports combinées pour tous les rôles.

Les administrateurs délégués exercent un contrôle important sur les activités Internet de leurs clients gérés. Pour être certain que ce contrôle soit géré de façon responsable et selon les stratégies d'utilisation acceptées par l'organisation, les Super administrateurs peuvent utiliser la page Journal d'audit pour surveiller les modifications apportées par les administrateurs. Voir *Affichage et exportation du journal d'audit*, page 373.

1. Si vous envisagez de définir des comptes réseau en tant qu'administrateurs délégués, assurez-vous d'être connecté à l'instance de Policy Server dont la configuration Paramètres > Général > Directory Service (Service d'annuaire) (voir *Services d'annuaire*, page 75) correspond à la configuration Paramètres > User Directory (Annuaire des utilisateurs) dans TRITON.

   Si vous ajoutez uniquement des comptes locaux comme administrateurs, vous pouvez vous connecter à n'importe quel serveur Policy Server.
2. Sous **Comptes locaux**, cochez la case d'un ou plusieurs utilisateurs, puis cliquez sur la flèche droite pour déplacer les utilisateurs sélectionnés vers la liste **Sélectionné**.
3. Sous **Comptes réseau**, cochez la case d'un ou plusieurs utilisateurs, puis cliquez sur la flèche droite (>) pour les déplacer vers la liste **Sélectionné**.

> **Remarque**
>
> Les groupes LDAP personnalisés ne peuvent pas être ajoutés en tant qu'administrateurs.

4. Définissez les **Autorisations** des administrateurs de ce rôle.

Option	Description
Administrateur : Gestion des stratégies	Permet aux administrateurs de ce rôle d'appliquer des stratégies à leurs clients gérés. Cette option permet également d'accéder à certains paramètres de configuration de Websense.
Administrateur : Génération de rapports	Permet aux administrateurs d'accéder aux outils de génération de rapports. Utilisez la page Modifier le rôle pour définir les fonctions de rapport autorisées de façon spécifique.
Administrateur : Real-Time Monitor	Permet aux administrateurs de surveiller le trafic du filtrage Internet en temps réel. Voir *Real-Time Monitor*, page 178.
Auditeur	Permet à l'administrateur d'afficher l'ensemble des fonctionnalités et fonctions à la disposition des autres administrateurs du rôle, sans possibilité d'enregistrer des modifications.

5. Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier le rôle.
6. Dans la page Modifier le rôle, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout de clients gérés

Rubriques connexes :

- *Gestion des rôles d'administration déléguée*, page 335
- *Modification des rôles*, page 337

Les clients gérés sont des utilisateurs et des ordinateurs attribués à un rôle, et dont les stratégies sont définies par les administrateurs de ce rôle. Les clients de l'annuaire (utilisateurs, groupes et domaines [unités d'organisation]), les ordinateurs (adresses IPv4 ou IPv6 individuelles) et les réseaux (plages d'adresses IPv4 ou IPv6) peuvent tous être définis en tant que clients gérés.

Les Super administrateurs peuvent utiliser la page **Administration déléguée** > **Modifier le rôle** > **Ajouter des clients gérés** pour ajouter autant de clients que nécessaire dans un rôle. Chaque client ne peut être attribué qu'à un seul rôle de gestion des stratégies et de génération de rapports.

Si vous attribuez une plage réseau en tant que client géré dans un rôle, vous ne pouvez pas attribuer les adresses IP individuelles de cette plage à un autre rôle. De plus, vous ne pouvez pas attribuer de façon spécifique un utilisateur, un groupe ou un domaine (unité d'organisation) à deux rôles différents. Vous pouvez cependant attribuer un utilisateur à un rôle, puis attribuer un groupe ou un domaine (unité d'organisation) dont cet utilisateur est membre à un autre rôle.

Remarque

Si un groupe est un client géré dans un rôle et que l'administrateur de ce rôle applique une stratégie à chaque membre du groupe, les utilisateurs individuels de ce groupe ne peuvent pas être attribués à un autre rôle ultérieurement.

Lorsque vous ajoutez des clients gérés, tenez compte des types de clients à inclure.

- Si vous ajoutez des adresses IP à un rôle, ses administrateurs peuvent générer des rapports sur **toute** l'activité des ordinateurs spécifiés, quelle que soit la personne connectée.
- Si vous ajoutez des utilisateurs à un rôle, les administrateurs peuvent générer des rapports sur toute l'activité de ces utilisateurs, quel que soit l'ordinateur sur lequel cette activité est détectée.

Les administrateurs ne sont pas automatiquement inclus en tant que clients gérés dans les rôles qu'ils administrent, car cela leur permettrait de définir leur propre stratégie. Pour autoriser des administrateurs à consulter leur propre utilisation d'Internet, activez la fonction de génération de rapports sur leur propre activité (voir *Rapports sur activité propre*, page 425).

Si votre organisation a déployé plusieurs serveurs Policy Server et que ces derniers communiquent avec des annuaires différents, assurez-vous de sélectionner le serveur Policy Server connecté à l'annuaire contenant les clients que vous souhaitez ajouter.

Remarque

Les meilleures pratiques montrent qu'il est préférable que tous les clients du même rôle appartiennent au même annuaire.

1. Sélectionnez des clients pour le rôle :
   - Sous **Annuaire**, cochez la case d'un ou plusieurs utilisateurs.

     Si votre environnement utilise Active Directory (en mode natif) ou un autre service d'annuaire de type LDAP, vous pouvez rechercher dans l'annuaire des noms d'utilisateur, de groupe ou de domaine (unité d'organisation) spécifiques. Voir *Recherche dans le service d'annuaire*, page 82.
   - Sous **Ordinateur**, saisissez l'adresse IP à ajouter dans ce rôle au format IPv4 ou IPv6.
   - Sous **Réseau**, saisissez la première et la dernière adresse IP d'une plage au format IPv4 ou IPv6.
2. Cliquez sur la flèche droite (>) accolée au type de client pour déplacer les clients sélectionnés vers la liste **Sélectionné**.
3. Lorsque vos modifications sont terminées, cliquez sur **OK** pour revenir à la page Modifier le rôle.
4. Dans la page Modifier le rôle, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Gestion des conflits entre rôles

Rubriques connexes :

- *Gestion des rôles d'administration déléguée*, page 335
- *Ajout de clients gérés*, page 342

Dans les services d'annuaire, le même utilisateur peut appartenir à plusieurs groupes. Par conséquent, un même utilisateur peut être membre de groupes gérés par des rôles d'administration déléguée différents. Il en est de même pour les domaines (unités d'organisation).

De plus, un utilisateur peut être géré par un seul rôle et appartenir à un groupe ou un domaine (unité d'organisation) géré par un rôle différent. Si les administrateurs de ces deux rôles sont connectés simultanément, l'administrateur responsable de l'utilisateur peut lui appliquer une stratégie alors même que l'administrateur responsable du groupe applique une stratégie aux membres individuels du groupe.

La page **Administration déléguée > Gérer la priorité des rôles** permet d'indiquer à Websense le comportement qu'il doit adopter lorsque des stratégies différentes s'appliquent simultanément aux mêmes utilisateurs. En cas de conflit, Websense applique alors la stratégie de filtrage du rôle apparaissant en premier dans cette liste.

1. Sélectionnez un rôle quelconque dans la liste, à l'exception du rôle Super administrateur.

   Remarque

   Le rôle Super administrateur est toujours le premier dans cette liste. Il ne peut pas être déplacé.

2. Cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier sa position dans la liste.

3. Répétez les étapes 1 et 2 jusqu'à ce que tous les rôles aient la priorité désirée.
4. Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache et revenir à la page Administration déléguée. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Mise à jour des rôles d'administration déléguée

Rubriques connexes :
- *Suppression de rôles*, page 345
- *Suppression de clients gérés*, page 345

Les stratégies et les clients gérés sont généralement ajoutés à un rôle lors de la création de ce dernier.

- Les administrateurs délégués qui disposent d'autorisations de stratégie peuvent modifier les stratégies existantes et créer de nouvelles stratégies dans le rôle qu'ils gèrent.
- Lorsque de nouveaux membres rejoignent l'organisation, un Super administrateur peut les ajouter dans des rôles existants (voir *Modification des rôles*, page 337).

À tout moment, les Super administrateurs peuvent également déplacer des clients (voir *Déplacements de clients vers des rôles*, page 86) et des stratégies (*Copie de filtres et de stratégies vers des rôles*, page 252) du rôle Super administrateur vers un rôle d'administration déléguée existant.

- Lorsqu'un client est déplacé vers un rôle d'administration déléguée, la stratégie appliquée au rôle de Super administrateur est également copiée. Au cours du processus de copie, les filtres sont mis à jour de manière à imposer les restrictions éventuelles du Verrouillage du filtre.

  Dans le rôle cible, la mention « (Copié) » est ajoutée à la fin du nom du filtre ou de la stratégie. Les administrateurs de ce rôle peuvent identifier rapidement le nouvel élément et le mettre à jour de façon appropriée.

  Encouragez les administrateurs du rôle à renommer les filtres et les stratégies et à les modifier selon leurs besoins afin de simplifier la compréhension de leurs paramètres et de minimiser les doublons. Ces modifications peuvent simplifier la maintenance ultérieure.

  Une fois le client déplacé vers le nouveau rôle, seul un administrateur de ce rôle peut en modifier la stratégie ou les filtres qu'il impose. Les modifications apportées à la stratégie ou aux filtres d'origine dans le rôle Super administrateur n'affectent pas les copies de la stratégie ou des filtres dans les rôles d'administration déléguée.
- Lorsque vous copiez directement des filtres et des stratégies, les contraintes imposées lors de la copie de filtres et de stratégies dans le cadre d'un déplacement de client s'appliquent également.
  - Les restrictions du Verrouillage du filtre sont implémentées pendant la copie.
  - Les filtres de catégories et de protocoles Autoriser tout sont renommés et deviennent modifiables, mais restent soumis au Verrouillage du filtre.

- Les filtres et les stratégies copiés sont identifiés dans le rôle par la mention (Copié) qui apparaît dans leur nom.

Le cas échéant, pensez à modifier les descriptions de la stratégie avant de démarrer la copie de manière à les rendre significatives pour les administrateurs des rôles visés.

Suppression de rôles

Dans la page **Administration déléguée**, les Super administrateurs inconditionnels peuvent supprimer tous les rôles devenus obsolètes.

La suppression d'un rôle retire également tous les clients que les administrateurs du rôle ont ajoutés à la page Clients. Une fois le rôle supprimé, si ces clients appartiennent à des réseaux, des groupes ou des domaines gérés par d'autres rôles, ils sont gérés par la stratégie appropriée appliquée à ces derniers (voir *Ordre du filtrage*, page 95). Sinon, ils sont gérés par la stratégie Par défaut du Super administrateur.

1. Dans la page **Administration déléguée**, cochez la case accolée à chaque rôle à supprimer.

> **Remarque**
> Vous ne pouvez pas supprimer le rôle Super administrateur.

2. Cliquez sur **Supprimer**.
3. Confirmez l'opération pour supprimer les rôles sélectionnés de la page Administration déléguée. Les modifications ne sont pas définitives tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

   Le rôle supprimé est retiré de la liste déroulante Rôle dans la bannière dès votre prochaine connexion à TRITON - Web Security.

Suppression de clients gérés

Les clients ne peuvent pas être supprimés directement de la liste des clients gérés (Administration déléguée > Modifier le rôle) dans les cas suivants :

- L'administrateur a appliqué une stratégie au client.
- L'administrateur a appliqué une stratégie à un ou plusieurs membres d'un réseau, d'un groupe ou d'un domaine (unité d'organisation).

Des problèmes peuvent également survenir si le Super administrateur est connecté à un autre serveur Policy Server que celui qui communique avec le service d'annuaire contenant les clients à supprimer. Dans ce cas, le serveur Policy Server actif et le service d'annuaire ne reconnaissent pas les clients.

Un Super administrateur inconditionnel peut vérifier que les clients appropriés peuvent être supprimés, comme suit.

1. Ouvrez la liste **Policy Server** dans la barre d'outils Web Security et vérifiez que vous êtes connecté au serveur Policy Server qui communique avec l'annuaire approprié. Vous devez vous connecter avec des autorisations de Super administrateur inconditionnel.
2. Ouvrez la liste **Rôle** dans la barre d'outils Web Security et sélectionnez le rôle duquel les clients gérés doivent être retirés.

3. Ouvrez la page **Gestion des stratégies > Clients** pour voir la liste de tous les clients auxquels l'administrateur délégué a explicitement attribué une stratégie.

   Cela peut comprendre les clients spécifiquement identifiés dans la liste des clients gérés du rôle et les clients membres de réseaux, de groupes, de domaines ou d'unités d'organisation présents dans la liste des clients gérés.
4. Supprimez les clients appropriés.
5. Cliquez sur **OK** pour mettre vos modifications en cache.
6. Ouvrez la liste **Rôle** dans la bannière et sélectionnez le rôle **Super administrateur**.
7. Ouvrez la page **Gestion des stratégies > Administration déléguée > Modifier le rôle**.
8. Supprimez les clients appropriés de la liste des clients gérés, puis cliquez sur **OK** pour confirmer l'opération.
9. Dans la page Modifier le rôle, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Gestion des clients des Super administrateurs

Les clients qui ne sont pas attribués de façon spécifique à un rôle d'administration déléguée sont gérés par les Super administrateurs. Il n'existe pas de liste de Clients gérés pour le rôle Super administrateur.

Pour appliquer des stratégies à ces clients, ajoutez-les à la page Gestion des stratégies > Clients. Voir *Ajout d'un client*, page 81. Les clients qui n'ont pas été attribués à une stratégie spécifique sont gérés par la stratégie Par défaut du Super administrateur.

Il peut arriver que vous ne puissiez pas ajouter de clients dans la page Clients. Cela peut se produire lorsque le client est membre d'un réseau, d'un groupe ou d'un domaine (unité d'organisation) attribué à un autre rôle. Si l'administrateur de cet autre rôle a appliqué une stratégie à des membres individuels du réseau ou du groupe, ces clients ne peuvent pas être ajoutés au rôle Super administrateur.

Exécution des tâches d'administration déléguée

Les administrateurs délégués qui disposent d'autorisations de **stratégie** peuvent effectuer les tâches suivantes.

- *Affichage de votre compte d'utilisateur*, page 347
- *Affichage de la définition de votre rôle*, page 348
- *Ajout de clients dans la page Clients*, page 348
- *Création de stratégies et de filtres*, page 349
- *Application de stratégies à des clients*, page 350

Des autorisations de **génération de rapports** peuvent être accordées à un niveau granulaire. Les autorisations de génération de rapports spécifiques accordées à votre rôle déterminent les tâches disponibles pour les administrateurs autorisés à générer des rapports parmi les tâches suivantes. Voir *Génération de rapports*, page 351.

Affichage de votre compte d'utilisateur

Rubriques connexes :

- *Exécution des tâches d'administration déléguée*, page 346
- *Affichage de la définition de votre rôle*, page 348
- *Ajout de clients dans la page Clients*, page 348
- *Création de stratégies et de filtres*, page 349
- *Application de stratégies à des clients*, page 350

Si vous vous connectez à TRITON - Web Security avec des identifiants réseau, les modifications du mot de passe sont gérées via le service d'annuaire de votre réseau. Au besoin, demandez l'aide de votre administrateur système.

Si un nom d'utilisateur local et un mot de passe vous ont été attribués, vous pouvez consulter les informations relatives à votre compte et modifier votre mot de passe dans la console TRITON.

1. Cliquez sur **Paramètres TRITON** dans la barre d'outils de TRITON, juste au-dessous de la bannière.

   La page Mon compte s'affiche.
2. Pour modifier votre mot de passe, commencez par entrer votre mot de passe actuel, puis saisissez et confirmez le nouveau mot de passe.
   - Ce mot de passe doit comporter entre 4 et 255 caractères.
   - Des mots de passe renforcés sont conseillés : au moins 8 caractères, comprenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial (tiret, trait de soulignement ou espace).

   Cliquez sur **OK** pour enregistrer et implémenter vos modifications.
3. Pour afficher la liste des rôles que vous pouvez administrer, ouvrez la page Policy Management (Gestion des stratégies Web Security) > Administration déléguée > View Administrator Accounts (Afficher les comptes d'administrateur) dans TRITON - Web Security.
   - Si vous avez été affecté à la gestion d'un seul rôle, son nom s'affiche dans la liste.
   - Si vous avez été affecté à la gestion de plusieurs rôles, cliquez sur l'option **Afficher** accolée à votre nom d'utilisateur pour en voir la liste.
4. Lorsque vous avez terminé, cliquez sur **Fermer** pour revenir à la page Administration déléguée.

Affichage de la définition de votre rôle

Rubriques connexes :

- *Exécution des tâches d'administration déléguée*, page 346
- *Affichage de votre compte d'utilisateur*, page 347
- *Ajout de clients dans la page Clients*, page 348
- *Création de stratégies et de filtres*, page 349
- *Application de stratégies à des clients*, page 350

Ouvrez la page Administration déléguée et cliquez sur le nom de votre rôle pour afficher la page Modifier le rôle qui présente la liste des clients gérés du rôle. Cette page présente également les fonctions de rapports disponibles pour les administrateurs autorisés à générer des rapports dans ce rôle.

Les administrateurs qui ne disposent que des autorisations de génération de rapports ne peuvent pas consulter cette page. Ces administrateurs ne peuvent consulter que les fonctions de génération de rapports spécifiées.

Ajout de clients dans la page Clients

Rubriques connexes :

- *Exécution des tâches d'administration déléguée*, page 346
- *Affichage de votre compte d'utilisateur*, page 347
- *Affichage de la définition de votre rôle*, page 348
- *Création de stratégies et de filtres*, page 349
- *Application de stratégies à des clients*, page 350

Les Super administrateurs attribuent des clients gérés à un rôle, mais les administrateurs délégués doivent les ajouter dans la page Clients avant de leur appliquer des stratégies. Pour obtenir des instructions, consultez la section *Ajout d'un client*, page 81.

Lorsque des clients sont ajoutés à une liste de clients gérés, ils sont immédiatement filtrés par la stratégie de ce rôle.

- Les clients auparavant attribués à une stratégie du rôle Super administrateur sont gérés par une copie de cette stratégie dans le nouveau rôle. Le processus Déplacer vers le rôle copie automatiquement la stratégie applicable.
- Les clients qui n'étaient pas attribués à une stratégie auparavant sont filtrés par la stratégie Par défaut du nouveau rôle. À l'origine, cette stratégie Par défaut applique obligatoirement le filtre de catégories et de protocoles Par défaut copié à partir du rôle Super administrateur.

Tous les clients apparaissant dans la liste de la page Administration déléguée > Modifier le rôle de votre rôle peuvent être ajoutés à la page Clients et attribués à une stratégie. Pour les groupes, domaines (unités d'organisation) et réseaux attribués au rôle, vous pouvez également ajouter :

- Des utilisateurs individuels membres du groupe ou du domaine/unité d'organisation
- Des ordinateurs individuels membres du réseau

Comme un utilisateur peut faire partie de plusieurs groupes, domaines ou unités d'organisation, l'ajout d'individus à partir d'un regroupement plus important de clients peut éventuellement créer des conflits lorsque différents rôles gèrent les groupes, les domaines ou les unités d'organisation présentant des membres communs. Si des administrateurs de rôles différents accèdent à TRITON - Web Security en même temps, ils peuvent ajouter le même client (membre individuel d'un groupe, par exemple) à leur page Clients. Dans ce cas, le filtrage Internet de ce client est régi par la priorité établie pour chaque rôle. Voir *Gestion des conflits entre rôles*, page 343.

Création de stratégies et de filtres

Rubriques connexes :

- *Exécution des tâches d'administration déléguée*, page 346
- *Affichage de votre compte d'utilisateur*, page 347
- *Affichage de la définition de votre rôle*, page 348
- *Ajout de clients dans la page Clients*, page 348
- *Application de stratégies à des clients*, page 350

Lorsque votre rôle a été créé, il a automatiquement hérité des filtres de catégories et de protocoles Par défaut du rôle Super administrateur. La stratégie Par défaut propre au rôle qui a été créée impose les filtres de catégories et de protocoles Par défaut hérités. (Cette stratégie Par défaut propre au rôle s'applique automatiquement à tous les clients ajoutés au rôle jusqu'à ce qu'une autre stratégie soit affectée.)

Le Super administrateur peut également avoir copié d'autres stratégies et filtres dans votre rôle.

Outre les stratégies et les filtres, vous héritez également des protocoles et des types de fichiers personnalisés créés par le Super administrateur.

Vous pouvez modifier les stratégies et les filtres hérités. Les modifications que vous apportez n'affectent que votre rôle. Toutes les modifications apportées ensuite par le Super administrateur aux stratégies et aux filtres d'origine n'affectent pas votre rôle.

Remarque

Les modifications apportées par le Super administrateur aux protocoles et aux types de fichiers affectent automatiquement les filtres et les stratégies de votre rôle.

Lorsqu'un Super administrateur vous signale des modifications de ces composants, vérifiez vos filtres et vos stratégies pour vous assurer qu'ils sont correctement gérés.

Vous pouvez également créer autant de filtres et de stratégies que nécessaire. Les filtres et les stratégies créés par un administrateur délégué ne sont disponibles qu'aux administrateurs connectés à votre rôle. Pour plus d'informations sur la création de stratégies, consultez la section *Fonctionnement des stratégies*, page 91. Pour plus d'informations sur la création de filtres, consultez la section *Fonctionnement des filtres*, page 59.

Vous pouvez modifier les composants de filtre pour votre rôle, avec certaines restrictions.

- **Catégories :** ajoutez des catégories personnalisées et modifiez la base de données principale et les catégories personnalisées, en définissant des URL recatégorisées et des mots-clés à utiliser au sein de leur rôle. Modifiez l'action et l'option de filtrage avancé appliquées par défaut dans les filtres de catégories qu'elles créent. (Les modifications apportées à l'action par défaut d'une catégorie ne sont implémentées que si la catégorie n'est pas verrouillée par le Verrouillage du filtre.)
- **Protocoles :** modifiez l'action et les options de filtrage avancé appliquées par défaut dans les filtres de protocoles qu'ils créent. (Les modifications apportées à l'action par défaut d'un protocole ne sont implémentées que si le protocole n'est pas verrouillé par le Verrouillage du filtre.) Les administrateurs délégués ne peuvent pas ajouter ni supprimer de définitions de protocole.
- **Types de fichiers :** affichez les extensions de fichier affectées à chaque type de fichiers. Les administrateurs délégués ne peuvent pas ajouter de types de fichiers ni modifier les extensions affectées à un type de fichiers.

Pour plus d'informations, consultez la section *Construction de composants de filtres*, page 253.

Si un Super administrateur a implémenté des restrictions de Verrouillage du filtre, certains protocoles ou catégories peuvent être automatiquement bloqués et ne plus être modifiables dans les filtres que vous créez et modifiez.

Application de stratégies à des clients

Rubriques connexes :

- *Exécution des tâches d'administration déléguée*, page 346
- *Affichage de votre compte d'utilisateur*, page 347
- *Affichage de la définition de votre rôle*, page 348
- *Ajout de clients dans la page Clients*, page 348
- *Création de stratégies et de filtres*, page 349

Après avoir créé une stratégie, vous pouvez l'appliquer directement aux clients qui ont déjà été ajoutés à la page Clients en cliquant sur le bouton **Appliquer aux clients**. Voir *Attribution d'une stratégie aux clients*, page 95.

Vous pouvez également ouvrir la page Clients et ajouter les clients devant être régis par cette stratégie. Voir *Fonctionnement des clients*, page 72.

Génération de rapports

Si vous disposez d'autorisations de génération de rapports, les options de rapports spécifiques disponibles sont définies par le Super administrateur. Pour voir quelles fonctions vous pouvez utiliser, ouvrez la page Administration déléguée et cliquez sur le nom du rôle. La page Modifier le rôle présente les fonctions de rapports pour lesquelles vous disposez d'autorisations. Voir :

- *Rapports de présentation*, page 131
- *Rapports d'investigation*, page 152
- *Real-Time Monitor*, page 178

Vérification des comptes d'administrateur

Utilisez la page **Administration déléguée > View Administrator Accounts (Afficher les comptes d'administrateur)** pour :

- Afficher la liste des comptes locaux et réseau auxquels un administrateur de sécurité globale a attribué un accès à Web Security
- Vérifier le niveau d'autorisations affecté à chaque compte
- Afficher la liste des rôles associés à chaque compte

  Lorsqu'un compte à été ajouté à un seul rôle en tant qu'administrateur, ce rôle s'affiche à droite du nom du compte. Si le compte permet de gérer plusieurs rôles, cliquez sur **Afficher** pour afficher les rôles répertoriés.

Les administrateurs délégués ne peuvent consulter que les informations relatives à leur propre compte et non celles de tous les comptes.

Lorsque la vérification des comptes d'administrateur est terminée, cliquez sur **Fermer** pour revenir à la page Administration déléguée.

Activation des comptes réseau

Les Administrateurs de sécurité globale peuvent utiliser la page **Paramètres > User Directory (Annuaire des utilisateurs)** de TRITON pour saisir les informations du service d'annuaire nécessaires pour que les administrateurs puissent se connecter à TRITON - Web Security avec leurs identifiants de connexion réseau.

Cette tâche est effectuée **en plus de** la configuration définie par les Super administrateurs de Web Security et vise à spécifier le service d'annuaire servant à identifier les clients (utilisateurs et groupes).

Remarque

Les informations du service d'annuaire des clients sont configurées à la page Paramètres > Services d'annuaire (voir *Services d'annuaire*, page 75).

Les identifiants réseau des administrateurs de TRITON doivent être authentifiés par rapport au contenu d'un seul service d'annuaire. Si votre réseau comprend plusieurs services d'annuaire, une relation approuvée doit exister entre l'annuaire défini dans les Paramètres de TRITON et les autres services.

S'il n'est pas possible de définir un seul service d'annuaire pour la console TRITON Unified Security Center, envisagez plutôt la création de comptes locaux pour vos administrateurs.

Des instructions spécifiques sur la définition de l'annuaire utilisé pour authentifier les connexions des administrateurs sont disponibles dans l'Aide des Paramètres de TRITON.

16 Administration du serveur Web Security

Rubriques connexes :

- *Composants du produit Websense Web Security*, page 354
- *Fonctionnement de la Base de données des stratégies*, page 360
- *Fonctionnement de Policy Server*, page 360
- *Fonctionnement de Filtering Service*, page 365
- *Intégration à une solution SIEM tierce*, page 371
- *Fonctionnement de Content Gateway*, page 372
- *Affichage et exportation du journal d'audit*, page 373
- *Arrêt et démarrage des services Websense*, page 375
- *Alertes*, page 377
- *Sauvegarde et restauration de vos données Websense*, page 386

Le filtrage de l'utilisation d'Internet requiert une interaction entre plusieurs composants de Websense Web Security :

- Les demandes d'accès à Internet des utilisateurs sont reçues par Network Agent, Content Gateway ou un produit ou un dispositif tiers intégré (intégration).
- Les requêtes sont envoyées à Websense Filtering Service pour être traitées.
- Filtering Service communique avec le serveur Policy Server et Policy Broker pour appliquer la stratégie appropriée en réponse à la requête.

Une même Base de données de stratégies gère les informations des clients, des filtres, des stratégies et de la configuration générale, qu'il existe un ou plusieurs serveurs Policy Server.

Chaque instance de TRITON - Web Security est associée à cette Base de données de stratégies et permet de configurer toutes les instances de Policy Server associées à cette base de données.

La configuration des stratégies effectuée dans TRITON - Web Security étant stockée dans la base de données centrale, les informations des stratégies sont automatiquement accessibles à tous les serveurs Policy Server associés à cette base de données de stratégies.

Composants du produit Websense Web Security

Rubriques connexes :

- *Fonctionnement de la Base de données des stratégies*, page 360
- *Fonctionnement de Policy Server*, page 360
- *Fonctionnement de Filtering Service*, page 365
- *Policy Server, Filtering Service et State Server*, page 368
- *Arrêt et démarrage des services Websense*, page 375
- *Vérification de l'état actuel du système*, page 385

Le logiciel Websense Web Security est constitué de plusieurs composants qui travaillent ensemble pour assurer la sécurité Internet, l'identification des utilisateurs et la génération des rapports. Pour vous aider à mieux comprendre et à mieux gérer votre environnement, cette section présente chaque composant.

Pour obtenir la liste des composants et leur description, consultez les sections suivantes :

- *Composants du filtrage et de la gestion*, page 354
- *Composants de la génération de rapports*, page 357
- *Composants de l'identification des utilisateurs*, page 358
- *Composants d'interopérabilité*, page 359

Lorsque le logiciel Websense est intégré à Citrix, Microsoft Forefront TMG ou à un proxy ou un cache de proxy qui utilise ICAP, un composant d'intégration supplémentaire (service d'intégration, plug-in de filtrage ou serveur ICAP) est également installé.

Composants du filtrage et de la gestion

Composant	Description
Base de données des stratégies	Stocke les paramètres et les informations des stratégies de Websense. Installée automatiquement avec Policy Broker.
Policy Broker	Gère les requêtes provenant des composants de Websense pour les informations des stratégies et de la configuration générale

Composant	Description
Policy Server	• Identifie et surveille l'emplacement et l'état des autres composants de Websense • Stocke les informations de configuration spécifiques à une seule instance de Policy Server • Communique les données de configuration au service Filtering Service, qui filtre les requêtes Internet Configurez les paramètres de Policy Server dans TRITON - Web Security (voir *Fonctionnement de Policy Server*, page 360). Les paramètres des stratégies et la plupart des paramètres de configuration sont partagés entre les serveurs Policy Server qui partagent une même base de données de stratégies (voir *Fonctionnement d'un environnement à plusieurs serveurs Policy Server*, page 363).
Filtering Service	Assure le filtrage Internet avec Network Agent ou un produit d'intégration tiers. Lorsqu'un utilisateur demande un site, Filtering Service reçoit sa requête et détermine la stratégie à appliquer. • Filtering Service doit s'exécuter pour que les requêtes Internet soient filtrées et journalisées. • Chaque instance de Filtering Service télécharge sa propre copie de la base de données principale Websense. Configurez le comportement du filtrage et de Filtering Service dans TRITON - Web Security (voir *Filtres de l'utilisation Internet*, page 49, et *Configuration des paramètres de filtrage de Websense*, page 67).
Network Agent	• Étend les fonctions de filtrage et de journalisation • Autorise la gestion des protocoles • Autorise le filtrage dans un environnement autonome Pour plus d'informations, consultez la section *Configuration du réseau*, page 427.
Base de données principale	• Comprend plus de 36 millions de sites Web, classés dans plus de 90 catégories et sous-catégories • Contient plus de 100 définitions de protocole à utiliser dans le filtrage de protocoles Téléchargez la base de données principale Websense pour activer le filtrage Internet et veillez à ce que cette base de données reste à jour. Si la Base de données principale date de plus de 2 jours, aucun filtrage n'est effectué. Pour plus d'informations, consultez la section *Base de données principale Websense*, page 27.
Infrastructure TRITON	Plate-forme prenant en charge et unifiant les modules TRITON - Web Security, Data Security et Email Security Gère une base de données interne des paramètres globaux appliqués à tous les modules TRITON

Composant	Description
TRITON - Web Security	Sert d'interface de configuration, de gestion et de génération de rapports dans Websense Utilisez TRITON - Web Security pour définir et personnaliser les stratégies d'accès à Internet, configurer les composants du logiciel Websense, générer des rapports sur l'activité du filtrage Internet, etc. TRITON - Web Security est constitué des services suivants : • Websense - TRITON Web Security • Websense Web Reporting Tools • Websense Explorer Report Scheduler • Websense Information Service for Explorer • Websense Reporter Scheduler Pour plus d'informations, consultez la section *Utilisation de TRITON - Web Security*, page 18.
Usage Monitor	• Autorise les alertes basées sur l'utilisation d'Internet • Fournit des informations sur l'utilisation d'Internet à Real-Time Monitor Usage Monitor surveille les accès aux catégories d'URL (affichées dans Real-Time Monitor) et aux protocoles, et génère des messages d'alerte en fonction du comportement d'alerte configuré. Pour plus d'informations, consultez *Alertes*, page 377, et *Real-Time Monitor*, page 178.
Content Gateway	• Fournit un proxy et une plate-forme de mise en cache robustes • Peut analyser le contenu des sites Web et des fichiers en temps réel pour catégoriser les sites précédemment non catégorisés • Autorise la gestion des protocoles • Analyse le code HTML pour rechercher des risques pour la sécurité (par exemple, le phishing, la redirection d'URL, les exploits Web et l'antiblocage par proxy) • Analyse le contenu des fichiers pour attribuer une catégorie de menaces (par exemple virus, Chevaux de Troie ou vers) • Découpe le contenu actif de certaines pages Web Voir *Options d'analyse et contournement du décryptage SSL*, page 181.
Client Remote Filtering	• Réside dans les ordinateurs clients situés hors du pare-feu réseau • Identifie les ordinateurs en tant que clients à filtrer et communique avec le serveur Remote Filtering Pour plus d'informations, consultez la section *Filtrage des utilisateurs hors site*, page 237.
Serveur Remote Filtering	• Autorise le filtrage des clients situés hors du pare-feu réseau • Communique avec Filtering Service pour assurer la gestion des accès Internet des ordinateurs distants Pour plus d'informations, consultez la section *Filtrage des utilisateurs hors site*, page 237.
State Server	Dans les environnements comprenant plusieurs instances de Filtering Service, surveille les sessions de temps contingenté, de confirmation, d'accès par mot de passe et de remplacement de compte des clients pour vérifier que les durées de session sont allouées correctement Pour activer cette fonctionnalité, déployez une instance de State Server par instance de Policy Server.

Pour plus d'informations sur les autres composants, consultez les sections suivantes :

- *Composants de la génération de rapports*, page 357
- *Composants de l'identification des utilisateurs*, page 358
- *Composants d'interopérabilité*, page 359

Composants de la génération de rapports

Composant	Description
Log Server	Journalise les données des requêtes Internet, dont : • La source de la requête • La catégorie ou le protocole associé(e) à la requête • Si la requête a été autorisée ou bloquée • Si le blocage par mot-clé, le blocage de type de fichiers, l'attribution de temps contingenté, des niveaux de bande passante ou la protection par mot de passe ont été appliqués Avec Network Agent et certains produits d'intégration, Log Server stocke également des informations sur la quantité de bande passante utilisée. Log Server est un composant Windows uniquement dont l'installation est nécessaire pour activer la plupart des fonctionnalités de génération de rapports de TRITON - Web Security. Après l'installation de Log Server, configurez Filtering Service pour transmettre les données de journalisation à l'emplacement approprié (voir *Configuration du mode de journalisation des requêtes filtrées*, page 398).
Base de données d'activité	Stocke les données des requêtes Internet collectées par Log Server en vue de leur utilisation dans les outils de génération de rapports de Websense
Real-Time Monitor	Présente l'activité du filtrage des URL en cours, notamment : • Source de la requête (nom d'utilisateur ou adresse IP) • URL (complète ou domaine uniquement) • Catégorie (Base de données principale, URL personnalisée ou dynamique, selon l'analyse de Content Gateway) • Si la requête a été autorisée ou bloquée • Date et heure de la requête Real-Time Monitor comprend 3 services : • Client Websense RTM • Serveur Websense RTM • Base de données Websense RTM Voir *Real-Time Monitor*, page 178.
Multiplexer	Lorsqu'il est activé, ce composant transmet les données de journalisation de Filtering Service à : • Une solution SIEM spécifiée • Log Server Utilisé uniquement lorsque Websense est intégré à un produit SIEM pris en charge. Pour activer l'intégration SIEM, installez une seule instance de Multiplexer par serveur Policy Server.

Pour plus d'informations sur les autres composants, consultez les sections suivantes :

- *Composants du filtrage et de la gestion*, page 354
- *Composants de l'identification des utilisateurs*, page 358
- *Composants d'interopérabilité*, page 359

Composants de l'identification des utilisateurs

Composant	Description
User Service	• Communique avec votre service d'annuaire • Transmet les informations liées aux utilisateurs, y compris les relations utilisateur/groupe et utilisateur/domaine, à Policy Server et Filtering Service en vue de leur application dans les stratégies de filtrage Si vous avez installé et configuré un agent d'identification transparente Websense (voir *Identification transparente*, page 285), User Service simplifie l'interprétation des informations relatives à l'ouverture de session des utilisateurs, et exploite ces informations pour fournir des associations nom d'utilisateur/adresse IP à Filtering Service. Lorsque vous ajoutez des utilisateurs et des groupes en tant que clients Websense (voir *Ajout d'un client*, page 81), User Service fournit à TRITON - Web Security les informations de nom et de chemin provenant du service d'annuaire. Pour plus d'informations sur la configuration des accès aux services d'annuaire, consultez la section *Services d'annuaire*, page 75.
DC Agent	• Autorise l'identification transparente des utilisateurs dans un service d'annuaire basé sur Windows • Communique avec User Service pour fournir à Websense des informations actualisées sur l'ouverture de session des utilisateurs à employer lors du filtrage Pour plus d'informations, consultez la section *DC Agent*, page 295.
Logon Agent	• Assure une identification transparente des utilisateurs sans précédent dans les réseaux Linux et Windows • Ne dépend pas d'un service d'annuaire ou d'un autre intermédiaire pour la capture des sessions de connexion des utilisateurs • Détecte les sessions de connexion des utilisateurs en temps réel Logon Agent communique avec l'application de connexion des ordinateurs clients pour faire en sorte que les sessions de connexion individuelles soient capturées et traitées directement par Websense. Pour plus d'informations, consultez la section *Logon Agent*, page 300.
eDirectory Agent	• Fonctionne avec Novell eDirectory pour identifier les utilisateurs de façon transparente • Collecte les informations des sessions de connexion des utilisateurs auprès de Novell eDirectory, qui authentifie les utilisateurs qui se connectent au réseau • Associe chaque utilisateur authentifié à une adresse IP, puis travaille avec User Service pour fournir les informations à Filtering Service Pour plus d'informations, consultez la section *eDirectory Agent*, page 304.

Composant	Description
RADIUS Agent	Autorise l'identification transparente des utilisateurs qui accèdent au réseau par une connexion distante, un VPN (Virtual Private Network), une ligne DSL ou une autre connexion à distance Pour plus d'informations, consultez la section *RADIUS Agent*, page 303.

Pour plus d'informations sur les autres composants, consultez les sections suivantes :

- *Composants du filtrage et de la gestion*, page 354
- *Composants de la génération de rapports*, page 357
- *Composants d'interopérabilité*, page 359

Composants d'interopérabilité

Composant	Description
Directory Agent	Dans les déploiements Websense Web Security Gateway Anywhere, ce composant collecte les informations relatives aux utilisateurs et aux groupes auprès d'un service d'annuaire pris en charge, en vue de leur utilisation lors du filtrage effectué par le service hybride.
Plug-in de filtrage	Lorsque le logiciel Websense est intégré à certains pare-feu, proxy, caches ou produits similaires, un plug-in de filtrage peut être installé pour autoriser la communication entre Filtering Service et le dispositif d'intégration.
Linking Service	Dans les déploiements Websense Web Security Gateway Anywhere ou dans les environnements qui combinent des données Websense et des solutions Web Security, de composant permet au logiciel chargé de la sécurité des données d'accéder aux informations de catégorisation de la Base de données principale et aux informations relatives aux utilisateurs et aux groupes collectés par User Service.
Sync Service	Dans les déploiements Websense Web Security Gateway Anywhere : • Envoie les mises à jour des stratégies et les informations sur les utilisateurs et les groupes au service hybride • Reçoit les données de rapports issues du service hybride

Pour plus d'informations sur les autres composants, consultez les sections suivantes :

- *Composants du filtrage et de la gestion*, page 354
- *Composants de la génération de rapports*, page 357
- *Composants de l'identification des utilisateurs*, page 358

Fonctionnement de la Base de données des stratégies

Rubriques connexes :

- *Fonctionnement de Policy Server*, page 360
- *Fonctionnement de Filtering Service*, page 365
- *Policy Server, Filtering Service et State Server*, page 368

La Base de données des stratégies Websense stocke les données des stratégies (y compris les paramètres des clients, des filtres, des composants de filtre et de l'administration déléguée) et les paramètres globaux configurés dans TRITON - Web Security. Les paramètres propres à une seule instance de Policy Server (par exemple ses connexions à Filtering Service et à Network Agent) sont stockés séparément.

Dans les environnements à plusieurs serveurs Policy Server, une seule base de données de stratégies gère les données des stratégies et de la configuration générale pour toutes les instances de Policy Server.

1. Au démarrage, chaque composant Websense demande les informations de configuration applicables dans la base de données de stratégies via le composant Policy Broker.
2. Les composants qui s'exécutent vérifient fréquemment la présence de modifications dans la base de données des stratégies.
3. La base de données des stratégies est actualisée chaque fois que des administrateurs modifient TRITON - Web Security et cliquent sur Save and Deploy (Enregistrer et déployer).
4. Lorsque la base de données des stratégies a été modifiée, chaque composant demande et reçoit les modifications affectant son fonctionnement.

Sauvegardez régulièrement la base de données des stratégies pour protéger les informations de stratégie et de configuration importantes. Pour plus d'informations, consultez la section *Sauvegarde et restauration de vos données Websense*, page 386.

Fonctionnement de Policy Server

Rubriques connexes :

- *Vérification des connexions à Policy Server*, page 361
- *Ajout ou modification des instances de Policy Server*, page 362
- *Fonctionnement d'un environnement à plusieurs serveurs Policy Server*, page 363
- *Modification de l'adresse IP de Policy Server*, page 363
- *Fonctionnement de Filtering Service*, page 365
- *Policy Server, Filtering Service et State Server*, page 368

Policy Server communique avec Filtering Service pour imposer les stratégies, et il est chargé d'identifier les autres composants du logiciel Websense et de surveiller leur emplacement et leur état.

Lorsque vous vous connectez à TRITON - Web Security, vous êtes connecté(e) à l'interface graphique de Policy Server.

- Vous ne pouvez pas vous connecter à TRITON - Web Security s'il n'est pas configuré pour communiquer avec Policy Server.
- Si votre installation Websense comprend plusieurs des instances de Policy Server, vous pouvez passer d'une instance à l'autre après vous être connecté à TRITON - Web Security.
- Vous pouvez ajouter ou supprimer des instances de Policy Server dans TRITON - Web Security.

La communication entre TRITON - Web Security et une instance de Policy Server est établie lors de l'installation de TRITON - Web Security.

La plupart des environnements ne requièrent qu'un seul serveur Policy Server. Un même serveur Policy Server peut communiquer avec plusieurs instances de Filtering Service et Network Agent pour l'équilibrage de la charge. Toutefois, dans les très grandes organisations (plus de 10 000 utilisateurs), l'installation de plusieurs instances de Policy Server peut s'avérer judicieuse. Si vous installez d'autres serveurs Policy Server, ajoutez chaque instance dans TRITON - Web Security (voir *Vérification des connexions à Policy Server*, page 361).

Vérification des connexions à Policy Server

La page **Paramètres > Général > Policy Servers (Serveurs Policy Server)** vous permet de vérifier les informations relatives à toutes les instances de Policy Server associées à TRITON - Web Security.

Si vous utilisez plusieurs instances de Policy Server partageant une même clé d'abonnement, vous pouvez désigner l'une d'elles en tant qu'instance de Policy Server principale et les autres en tant qu'instances de Policy Server secondaires. Vous pourrez ainsi gagner du temps lors de la configuration des connexions à Policy Server.

Pour afficher les instances de Policy Server secondaires associées à une instance de Policy Server principale dans la liste, cliquez sur le symbole « + » accolé au nom ou à l'adresse IP de l'instance de Policy Server.

Pour chaque instance de Policy Server répertoriée, le tableau présente une brève description et son port de communication. Les entrées des instances de Policy Server principales comprennent également la clé d'abonnement associée à l'instance et ses instances secondaires, ainsi que le niveau d'abonnement (par exemple, Web Security ou Web Security Gateway) de cette clé.

- Cliquez sur **Ajouter** pour associer une autre instance de Policy Server à cette instance de TRITON - Web Security. Voir *Ajout ou modification des instances de Policy Server*, page 362.
- Cliquez sur l'adresse IP ou le nom d'une instance de Policy Server pour modifier ses informations de configuration. Voir *Ajout ou modification des instances de Policy Server*, page 362.

  TRITON - Web Security est associé à une seule instance de Policy Server lors de l'installation. Cette instance devient le serveur Policy Server de base de l'installation TRITON - Web Security, et son adresse IP et sa description ne sont pas modifiables.

Vous pouvez toutefois modifier la clé d'abonnement associée à l'instance de base de Policy Server.

- Cochez une ou plusieurs entrées de Policy Server, puis cliquez sur **Supprimer** pour retirer la connexion reliant TRITON - Web Security à l'instance de Policy Server sélectionnée.

  Le fait de cliquer sur Supprimer retire l'instance de Policy Server dans TRITON - Web Security, mais ne désinstalle pas, ni n'arrête le service Websense Policy Server. Vous ne pouvez pas supprimer l'instance de base de Policy Server.

Après l'ajout ou la modification d'une connexion à Policy Server, cliquez sur **OK** dans la page Policy Servers (Serveurs Policy Server) 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)**.

Ajout ou modification des instances de Policy Server

La page Paramètres > Général > **Ajouter un serveur Policy Server** ou **Edit Policy Server (Modifier un serveur Policy Server)** vous permet d'associer une nouvelle instance de Policy Server à TRITON - Web Security ou d'actualiser les informations de configuration d'une instance de Policy Server existante.

1. Saisissez ou modifiez l'**adresse IP ou le nom** et le **Port** de communication de l'instance de Policy Server. Le port par défaut est le **55806**.
2. Entrez ou actualisez la **Description** de l'instance de Policy Server sélectionnée.

   Vous ne pouvez pas modifier la description de l'instance de base de Policy Server.
3. Indiquez s'il s'agit d'une instance **Principale** ou **Secondaire** de Policy Server.
   - La clé d'abonnement d'une instance principale de Policy Server diffère de celle des instances de Policy Server associées à TRITON - Web Security.
   - Les instances secondaires de Policy Server utilisent la même clé d'abonnement puisque une autre instance de Policy Server a déjà été associée à TRITON - Web Security.
4. S'il s'agit d'une instance **secondaire** de Policy Server, sélectionnez l'adresse IP de l'instance principale de Policy Server auprès de laquelle l'instance secondaire doit récupérer sa clé, puis cliquez sur **OK** pour revenir à la page Policy Servers (Serveurs Policy Server).

   Vous devez également cliquer sur **OK** dans la page Policy Servers (Serveurs Policy Server) 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)**.
5. S'il s'agit d'une instance **principale** de Policy Server, sélectionnez **Use the current subscription key (Utiliser la clé d'abonnement actuelle)** pour utiliser la clé d'abonnement enregistrée avec la nouvelle instance ou **Enter a subscription key (Entrer une clé d'abonnement)** pour saisir une clé d'abonnement.
   - Si vous modifiez une entrée existante, la clé et le type d'abonnement actuels s'affichent sous les boutons radio.
   - Cliquez sur **Verify Policy Server (Vérifier l'instance de Policy Server)** pour vérifier que TRITON - Web Security peut communiquer avec cette nouvelle instance de Policy Server. Si vous avez sélectionné l'option « Use the current subscription key (Utiliser la clé d'abonnement actuelle) » et que la connexion est bien établie, la clé d'abonnement s'affiche.

- Si vous n'êtes pas sûr que la nouvelle instance de Policy Server dispose d'une clé enregistrée, vous pouvez saisir la clé manuellement ou cliquer sur **Verify Policy Server (Vérifier l'instance de Policy Server)** pour voir si TRITON - Web Security détecte la clé existante pour cette instance.

6. Cliquez sur **OK** pour revenir à la page Policy Servers (Serveurs Policy Server). Vous devez de nouveau cliquer 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)**.

Fonctionnement d'un environnement à plusieurs serveurs Policy Server

Dans certains environnements distribués, comportant un grand nombre d'utilisateurs, il peut s'avérer judicieux d'installer plusieurs serveurs Policy Server. Ce choix impose toutefois de tenir compte de plusieurs éléments.

- Les informations des stratégies étant stockées dans la base de données des stratégies, leurs modifications sont automatiquement partagées par tous les serveurs Policy Server dès que vous cliquez sur **Save and Deploy (Enregistrer et déployer)**.
- La plupart des paramètres de configuration globaux (tels que les définitions des classes de risque et les options d'alerte) sont également partagés par les serveurs Policy Server.
- Les paramètres de configuration propres à un seul serveur Policy Server (tels que ses connexions à Filtering Service et à Network Agent) sont stockés localement par chaque serveur Policy Server et ne sont pas distribués.
- Pour appliquer correctement des actions de filtrage temporel (Confirmer, Temps contingenté, Accès par mot de passe ou Remplacement de compte), une ou plusieurs instances de Websense State Server sont requises. State Server autorisant le partage des informations temporelles associées à ces fonctions, les clients bénéficient exactement de l'accès Internet que vous avez défini (voir *Policy Server, Filtering Service et State Server*, page 368).

Pour passer d'une instance de Policy Server à l'autre dans TRITON - Web Security :

1. Dans la barre d'outils de Web Security, à côté de l'adresse IP de l'instance actuelle de Policy Server, cliquez sur **Switch (Changer)**.

   Si des modifications apportées à l'instance actuelle de Policy Server n'ont pas été enregistrées, un avertissement s'affiche. Pour rester connecté à l'instance actuelle de Policy Server et enregistrer vos modifications, cliquez sur **Annuler**.
2. Sélectionnez l'adresse IP ou le nom d'hôte d'un serveur Policy Server dans la liste **Connect to (Se connecter à)**.
3. Cliquez sur **OK**.

Vous êtes alors automatiquement connecté à l'instance de Policy Server sélectionnée et l'interface de TRITON - Web Security est actualisée.

Modification de l'adresse IP de Policy Server

Avant de modifier l'adresse IP de l'ordinateur Policy Server, **arrêtez tous les services Websense** s'exécutant dans cet ordinateur. Si TRITON - Web Security est également installé dans cet ordinateur, les services Websense TRITON - Web Security et Websense Web Reporting Tools sont également présents.

Après avoir modifié l'adresse IP, vous devez mettre à jour manuellement les fichiers de configuration de Websense utilisés par TRITON - Web Security, Policy Server et les autres services de Websense afin que le filtrage puisse reprendre.

Étape 1 : Mise à jour de la configuration de TRITON - Web Security

Mettez à jour TRITON - Web Security de sorte qu'il se connecte à Policy Server avec sa nouvelle adresse IP.

1. Dans l'ordinateur TRITON - Web Security, arrêtez les services **Websense Web Reporting Tools** et **Websense TRITON - Web Security** (si nécessaire).

   Si TRITON - Web Security et Policy Server sont installés dans ce même ordinateur, ces services devraient déjà être arrêtés.
2. Naviguez jusqu'au répertoire suivant :

   ```
   Websense\Web Security\tomcat\conf\Catalina\localhost\
   ```
3. Localisez le fichier **mng.xml** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
4. Ouvrez le fichier **mng.xml** dans un éditeur de texte (tel que Notepad ou vi) et remplacez chaque instance de l'ancienne adresse IP de Policy Server par la nouvelle.

   L'adresse IP de Policy Server apparaît à deux emplacements : dans la valeur **ps/default/host** et dans la valeur **psHosts**.
5. Lorsque vous avez terminé, enregistrez et fermez le fichier.

Ne redémarrez pas les services TRITON - Web Security avant d'avoir terminé les mises à jour restantes de la configuration de cette section.

Étape 2 : Mise à jour de la configuration de Policy Server

Mettez à jour le fichier de configuration de Policy Server et le fichier d'initialisation utilisé pour configurer la communication entre les composants de Websense.

1. Si vous ne l'avez pas déjà fait, arrêtez tous les services Websense dans l'ordinateur Policy Server (voir *Arrêt et démarrage des services Websense*, page 375).
2. Accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
3. Localisez le fichier **config.xml** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
4. Ouvrez le fichier **config.xml** dans un éditeur de texte et remplacez chaque instance de l'ancienne adresse IP de Policy Server par la nouvelle.
5. Lorsque vous avez terminé, enregistrez et fermez le fichier.
6. Dans le répertoire **bin**, localisez le fichier **websense.ini** et créez une copie de sauvegarde de ce fichier dans un autre répertoire.
7. Ouvrez le fichier **websense.ini** dans un éditeur de texte et remplacez chaque instance de l'ancienne adresse IP de Policy Server par la nouvelle.
8. Lorsque vous avez terminé, enregistrez et fermez le fichier.

Étape 3 : Vérification de la connexion à la base de données d'activité

Dans l'ordinateur Policy Server, utilisez l'Administrateur de la source de données ODBC de Windows pour vérifier la connexion ODBC à la base de données d'activité.

1. Sélectionnez **Démarrer** > **Paramètres** > **Panneau de configuration** > **Outils d'administration** > **Sources de données (ODBC)**.

2. Dans l'onglet **Système DSN**, sélectionnez le nom de la source de données appropriée (par défaut, **wslogdb70**), puis cliquez sur **Configurer**.
3. Vérifiez que le serveur de base de données approprié est sélectionné, puis cliquez sur **Suivant**.
4. Vérifiez les identifiants utilisés pour la connexion à la base de données, puis cliquez sur **Suivant**.
5. Acceptez les paramètres par défaut des deux écrans suivants, puis cliquez sur **Tester la source de données**.

> **Remarque**
>
> Si le test échoue, vérifiez le nom du serveur de base de données et réessayez.
>
> Si le test échoue encore alors que le nom de l'ordinateur est correct, vérifiez que le port de connexion utilisé convient et que le pare-feu autorise les communications sur le port sélectionné.

Étape 4 : Redémarrage des services Websense

1. Redémarrez l'ordinateur Policy Server. Vérifiez que tous les services Websense redémarrent normalement dans cet ordinateur.
2. Si l'instance de TRITON - Web Security utilisée pour configurer ce serveur Policy Server est installé dans un autre ordinateur, redémarrez les services **Websense Web Reporting Tools** et **Websense TRITON - Web Security** sur ce dernier.

> **Remarque**
>
> Si TRITON - Web Security est installé dans le même ordinateur que Policy Server, les administrateurs doivent utiliser la nouvelle adresse IP pour se connecter.

Fonctionnement de Filtering Service

Rubriques connexes :

- *Vérification des détails du service Filtering Service*, page 366
- *Reprise des téléchargements de la base de données principale*, page 367
- *Policy Server, Filtering Service et State Server*, page 368
- *Fonctionnement de Content Gateway*, page 372

Filtering Service est le composant de Websense qui fonctionne avec Network Agent, Content Gateway ou un produit d'intégration tiers pour filtrer l'activité Internet. Lorsqu'un utilisateur demande un site, Filtering Service reçoit sa requête, détermine la stratégie à appliquer et utilise la stratégie applicable pour déterminer comment le site est filtré.

Chaque instance de Filtering Service télécharge sa propre copie de la base de données principale Websense qu'il utilise pour déterminer comment filtrer les requêtes Internet.

Si vous utilisez plusieurs instances de Filtering Service, le composant supplémentaire Websense State Server est requis afin que les actions de filtrage temporel (Confirmer, Temps contingenté, Accès par mot de passe ou Remplacement de compte) soient correctement appliquées. State Server autorisant le partage des informations temporelles associées à ces fonctions, les clients bénéficient exactement de l'accès Internet que vous avez défini (voir *Policy Server, Filtering Service et State Server*, page 368).

Filtering Service transmet également les informations relatives à l'activité Internet à Log Server, de sorte qu'elles puissent être journalisées et utilisées dans les rapports.

Dans TRITON - Web Security, le **Résumé du Filtering Service** du tableau de bord Système répertorie l'adresse IP et l'état en cours de chaque instance de Filtering Service associée à l'instance actuelle de Policy Server. Cliquez sur l'adresse IP d'un service Filtering Service pour obtenir plus d'informations sur l'instance sélectionnée.

Vérification des détails du service Filtering Service

La page **État > Tableau de bord > Détails sur Filtering Service** permet de vérifier l'état d'une instance individuelle de Filtering Service. Cette page indique :

- L'adresse IP du service Filtering Service
- Si l'instance sélectionnée s'exécute ou non actuellement
- La version de Filtering Service

  Cette version doit correspondre à votre version de Websense, y compris aux correctifs appliqués.
- Le système d'exploitation de l'ordinateur Filtering Service
- La plate-forme Websense

  Cette information indique si Websense s'exécute en mode autonome ou est intégré à Content Gateway ou à un produit tiers.
- L'adresse IP et l'état des instances de Network Agent avec lesquels le service Filtering Service sélectionné communique
- L'adresse IP et l'état des instances de Content Gateway avec lesquelles le service Filtering Service sélectionné communique

Cliquez sur **Fermer** pour revenir au Tableau de bord Web Security.

Vérification de l'état du téléchargement de la base de données principale

Dans votre réseau, chaque instance de Filtering Service télécharge sa propre copie de la base de données principale. Lorsque vous travaillez dans TRITON - Web Security, le Résumé sur les alertes d'état de l'onglet Système de la page État > Tableau de bord présente un message d'état lorsqu'un téléchargement de la base de données principale est en cours ou si une tentative de téléchargement échoue.

Pour plus d'informations sur les téléchargements récents ou en cours de la base de données, cliquez sur **Téléchargement de la base de données** dans la barre d'outils du Tableau de bord Web Security. La page Téléchargement de la base de données comprend une entrée pour chaque instance de Filtering Service associée au serveur Policy Server actif.

Au départ, la page Téléchargement de la base de données présente un bref résumé du téléchargement, indiquant l'emplacement et la version de la base de données téléchargée et si l'opération a réussi. À partir de cette vue de résumé, vous pouvez :

- Démarrer un téléchargement de base de données pour un seul service Filtering Service (cliquez sur **Mettre à jour**)
- Démarrer des téléchargements de base de données pour toutes les instances de Filtering Service de la liste (cliquez sur **Tout mettre à jour**)
- Annuler une ou toutes les mises à jour en cours

Cliquez sur une adresse IP dans la liste située à droite pour obtenir un état plus détaillé du téléchargement de la base de données pour l'instance de Filtering Service sélectionnée.

- Si des problèmes de téléchargement sont survenus pour l'instance de Filtering Service sélectionnée, des conseils permettant de les résoudre peuvent s'afficher.
- Pour démarrer manuellement un téléchargement de base de données pour l'instance de Filtering Service sélectionnée, cliquez sur **Mettre à jour**.

Pendant le téléchargement de la base de données, l'écran d'état présente des informations détaillées sur la progression de chaque étape du téléchargement. Cliquez sur **Fermer** pour masquer les informations de progression et continuer à travailler dans TRITON - Web Security.

Reprise des téléchargements de la base de données principale

Lorsqu'un téléchargement de la base de données principale est interrompu, Websense tente automatiquement de reprendre le téléchargement. Si Filtering Service peut se reconnecter au serveur de téléchargement, le téléchargement reprend là où il s'était arrêté.

Vous pouvez redémarrer manuellement un téléchargement interrompu ou qui a échoué. Dans ce cas, le téléchargement ne reprend pas au point d'interruption mais recommence au début.

1. Dans TRITON - Web Security, sélectionnez **État > Tableau de bord**, puis cliquez sur **Téléchargement de base de données**.
2. Cliquez sur **Arrêter toutes les mises à jour** pour stopper le processus interrompu.
3. Sélectionnez une instance de Filtering Service et cliquez sur **Mettre à jour**, ou sur **Tout mettre à jour**, pour redémarrer le processus de téléchargement depuis le début.

Prise en charge de YouTube for Schools par Filtering Service

Les établissements d'enseignement qui disposent d'un déploiement logiciel de Websense Web Security ou de Web Filter peuvent utiliser un paramètre de configuration de Filtering Service pour activer YouTube for Schools. Ce service YouTube permet d'accéder à des vidéos éducatives via le réseau de l'école, y compris lorsque le reste du contenu YouTube est bloqué.

Remarque

Dans le déploiement de logiciel ou de dispositif Web Security Gateway et Gateway Anywhere, vous pouvez activer YouTube for Schools via Content Gateway au lieu d'utiliser Filtering Service.

Après vous être inscrit au programme et avoir reçu le code ou l'ID de votre compte éducatif, procédez d'abord comme suit :

- Dans TRITON - Web Security, ouvrez la page Paramètres > Général > Filtrage et vérifiez que l'option **Activer le filtrage de la recherche** située au bas de la page est bien sélectionnée.

  Vous devez activer le filtrage de recherche pour exploiter la fonctionnalité YouTube for Schools.

  Si le filtrage de la recherche n'a pas déjà été activé, cliquez sur **OK**, puis sur **Save and Deploy (Enregistrer et déployer)** pour mettre cette modification en cache et l'implémenter.
- Assurez-vous que YouTube est autorisé pour les clients auxquels un accès à YouTube for Schools sera accordé.

Lorsque cette configuration est terminée, procédez comme suit pour chaque instance de Filtering Service présente dans votre déploiement :

1. Dans l'ordinateur Filtering Service, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
2. Créez une copie de sauvegarde du fichier **eimserver.ini** dans un autre emplacement.
3. Ouvrez le fichier **eimserver.ini** original, puis ajoutez-lui les lignes suivantes :

   ```
   [SafeSearchCustomValues]
   YouTubeEDUFilter=<code_compte_éducatif>
   ```

   Remplacez <code_compte_éducatif> par le véritable code ou ID fourni par YouTube.
4. Enregistrez et fermez le fichier.
5. Redémarrez Filtering Service :
   - Sous Windows : utilisez la boîte de dialogue Services pour redémarrer **Websense Filtering Service**.
   - Sous Linux : utilisez la commande /opt/Websense/WebsenseDaemonControl pour redémarrer **Filtering Service**.

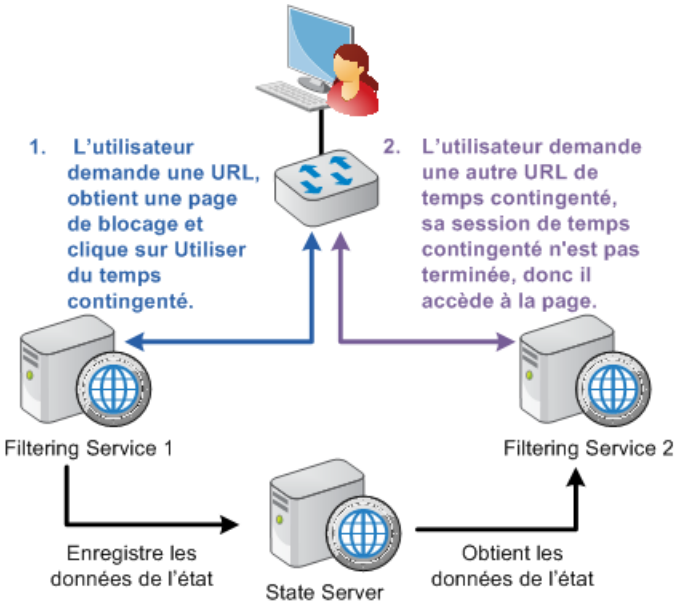
Policy Server, Filtering Service et State Server

Rubriques connexes :

- *Fonctionnement de Policy Server*, page 360
- *Fonctionnement de Filtering Service*, page 365
- *Actions de filtrage*, page 57
- *Accès par mot de passe*, page 84
- *Remplacement de compte*, page 84

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 (Temps contingenté, Confirmer) ou de remplacement (Accès par mot de passe, 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 temps contingenté, de confirmation ou de changement de session.

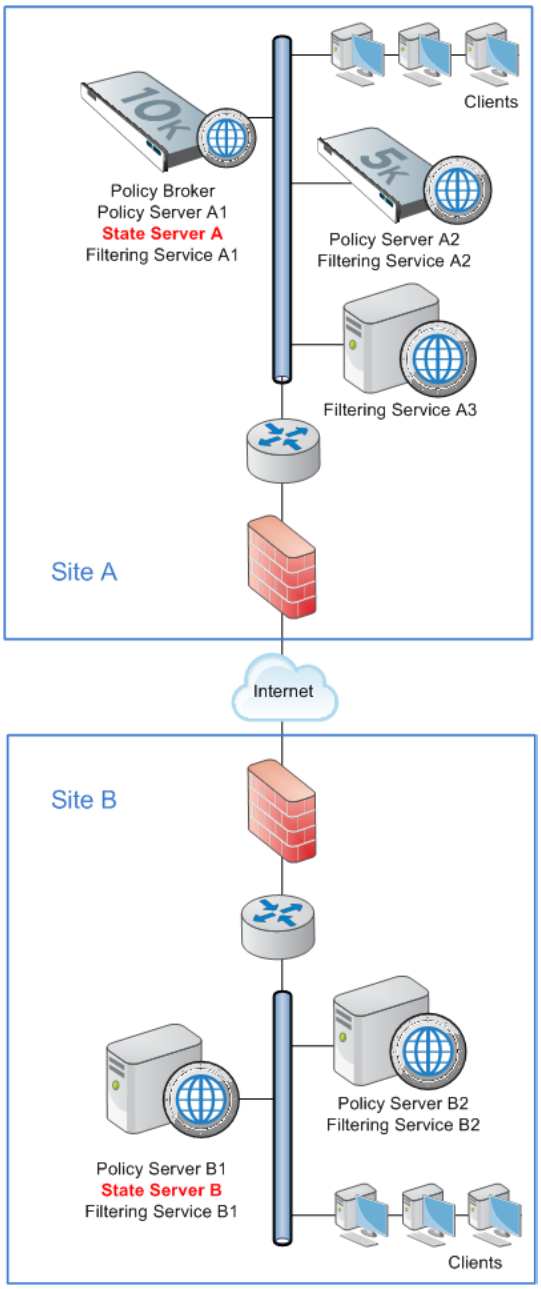


State Server est généralement installé dans un serveur Policy Server et une seule instance de State Server est requise par **déploiement logique**. Un déploiement logique est un groupe quelconque d'instances de Policy Server et de Filtering Service susceptibles de gérer les requêtes provenant du même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

Pour configurer l'instance de State Server avec laquelle communique un serveur Policy Server, utilisez la page **Paramètres > Général > Filtrage** de TRITON - Web Security (voir *Configuration des paramètres de filtrage de Websense*, page 67).

Dans une organisation géographiquement dispersée au sein de laquelle chaque emplacement dispose de ses propres instances de Policy Server et Filtering Service, déployez une unique instance de State Server (dans l'ordinateur Policy Server ou le dispositif V-Series) dans chaque emplacement. Par exemple :



Dans une organisation au sein de laquelle l'ensemble des requêtes sont filtrées par le biais d'un emplacement central, une seule instance de State Server est nécessaire.

Intégration à une solution SIEM tierce

La page **Paramètres > Général > SIEM Integration (Intégration SIEM)** vous permet de configurer Websense de sorte qu'il envoie les données des journaux de Filtering Service à une solution SIEM (Security Information and Event Management) prise en charge.

Avant d'utiliser cette page pour activer l'intégration SIEM, vérifiez qu'une instance de Websense Multiplexer a bien été installée pour chaque instance de Policy Server dans votre déploiement.

Pour chaque instance de Policy Server de votre déploiement, procédez comme suit.

1. Sélectionnez l'option **Enable SIEM integration for this Policy Server (Activer l'intégration SIEM pour ce serveur Policy Server)** pour activer la fonctionnalité d'intégration SIEM.
2. Fournissez l'**adresse IP ou le nom d'hôte** de l'ordinateur hébergeant le produit SIEM, de même que le **Port** de communication à utiliser pour envoyer les données SIEM.
3. Définissez le **Protocole de transport** (UDP ou TCP) à utiliser pour envoyer les données au produit SIEM.
4. Sélectionnez le **Format SIEM** à utiliser. Ce format détermine la syntaxe de la chaîne utilisée pour transmettre les données des journaux à l'intégration.
   - Les formats disponibles sont Arcsight CEF, Apache Common, Apache Extended, Apache Extended 2 (Splunk), Squid ou Custom (Personnalisé).
   - Si vous sélectionnez Custom (Personnalisé), un champ de texte s'affiche. Dans ce cas, saisissez ou collez la chaîne que vous souhaitez utiliser. Cliquez sur **View SIEM format strings (Afficher les chaînes de format SIEM)** pour obtenir des exemples de chaînes à utiliser comme référence ou modèle.
   - Si vous sélectionnez une option non personnalisée, un exemple de **chaîne de format** présentant les champs et les clés de valeur s'affiche.
5. 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)**.

Lorsque vous enregistrez vos modifications, Websense Multiplexer se connecte à Filtering Service et se charge de distribuer les données des journaux à Log Server et à l'intégration SIEM sélectionnée.

Notez que, bien que les mêmes données soient transmises de Filtering Service à Log Server et au produit SIEM, Log Server peut être configuré pour effectuer des tâches de traitement réductif des données (par exemple pour enregistrer les visites plutôt que les accès, ou regrouper les enregistrements des journaux). Le produit SIEM n'effectuant pas ces tâches de réduction des données, la base de données d'activité peut contenir davantage d'entrées SIEM que d'enregistrements.

Fonctionnement de Content Gateway

Rubriques connexes :
- *Fonctionnement de Filtering Service*, page 365
- *Fonctionnement de Policy Server*, page 360
- *Gestion des connexions à Content Gateway*, page 372

Content Gateway est un composant logiciel Websense propre à Linux qui fournit des services de proxy Web hautes performances aux déploiements Websense Web Security Gateway et Gateway Anywhere. Content Gateway est également utilisé en tant que proxy par les solutions Websense Data Security et Email Security Gateway.

Dans les déploiements Websense Web Security Gateway et Gateway Anywhere, Content Gateway assure les tâches suivantes :

- Analyse en temps réel du contenu et classification des sites Web afin de protéger le réseau contre tout contenu Web malveillant. Cette analyse est particulièrement précieuse pour les sites Web 2.0 qui, dynamiques et de sources multiples par nature, limitent l'efficacité de la catégorisation statique.
- Analyse avancée des fichiers permettant de détecter les fichiers infectés et malveillants et d'en bloquer le téléchargement ou le chargement
- Détection des protocoles entrants et sortants mis en tunnel sur HTTP et HTTPS et application du filtrage des protocoles

Content Gateway fonctionne avec Filtering Service pour filtrer les requêtes Internet sur la base des deux éléments suivants :

- Catégorisation statique par la base de données principale ou les définitions d'URL personnalisées
- Recatégorisation dynamique résultant de l'analyse du contenu

Lors de l'installation, Content Gateway établit une communication avec une instance de Policy Server. Cette connexion :

- Permet à Policy Server de transmettre les informations relatives à la clé d'abonnement à Content Gateway, ce qui permet de ne pas gérer les clés dans deux consoles de gestion
- Fournit à TRITON - Web Security les informations relatives aux connexions de Filtering Service à Content Gateway
- Sert à renseigner la page Paramètres > Général > Content Gateway Access (Accès à Content Gateway) dans TRITON - Web Security et rend possible le démarrage de Content Gateway Manager depuis TRITON

Gestion des connexions à Content Gateway

La page **Paramètres > Général > Content Gateway Access (Accès à Content Gateway)** permet de vérifier les informations de configuration et d'état des instances de Content Gateway associées au serveur Policy Server actuel ou de démarrer Content Gateway Manager pour une instance sélectionnée.

Lorsqu'une instance de Content Gateway est enregistrée auprès d'un serveur Policy Server, la page Content Gateway Access (Accès à Content Gateway) est actualisée automatiquement pour présenter l'adresse IP, le nom d'hôte et les informations d'état de cette instance de Content Gateway. Ces informations s'affichent dans l'un des trois tableaux :

- Si l'instance de Content Gateway fait partie d'un cluster, le tableau qui s'affiche utilise le nom du cluster comme titre. Toutes les instances de Content Gateway présentes au sein du cluster sont répertoriées. Lorsqu'il existe plusieurs clusters, plusieurs tableaux s'affichent.
- Si l'instance de Content Gateway n'est pas mise en cluster, elle s'affiche dans le tableau des instances de Content Gateway non mises en cluster.
- Si l'instance de Policy Server ne peut pas communiquer avec une instance de Content Gateway, elle s'affiche dans le tableau Not Responding (Sans réponse). Ce tableau ne s'affiche que si Policy Server ne peut pas communiquer avec une instance de Content Gateway enregistrée.

Pour démarrer Content Gateway Manager pour l'une des instances répertoriées, cliquez sur le lien correspondant dans la colonne **Adresse IP** du tableau.

Pour actualiser la description d'une instance et simplifier la gestion des connexions à Content Gateway, activez le bouton radio accolé à l'adresse IP de cette instance, puis cliquez sur **Modifier la description**.

Lorsqu'une instance de Content Gateway s'affiche dans le tableau **Not Responding (Sans réponse)** parce qu'elle a été désinstallée ou déplacée, activez le bouton radio accolé au nom de cette instance, puis cliquez sur **Supprimer**.

Après avoir modifié les descriptions de Content Gateway ou supprimé des entrées obsolètes, 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)**.

Affichage et exportation du journal d'audit

Websense fournit un suivi d'audit qui montre comment les administrateurs ont accédé à TRITON - Web Security et les modifications qu'ils ont pu apporter aux stratégies et aux paramètres. Ces informations ne sont disponibles que pour les Super administrateurs qui disposent d'autorisations sur les stratégies (voir *Autorisations du Super administrateur*, page 326).

Les administrateurs délégués exercent un contrôle important sur les activités Internet de leurs clients gérés. La surveillance de leurs modifications via le journal d'audit vous permet de vérifier que ce contrôle est exercé de façon responsable et selon les stratégies d'utilisation acceptées par l'organisation.

Utilisez la page **État > Journal d'audit** pour afficher le journal d'audit et, le cas échéant, pour exporter les parties sélectionnées dans le journal dans une feuille de calcul Excel (XLS).

Les enregistrements d'audit sont conservés pendant 60 jours. Pour les conserver plus longtemps, servez-vous de l'option d'exportation pour exporter le journal régulièrement. Le processus d'exportation ne supprime pas les enregistrements dans le journal d'audit.

Lorsque la page Journal d'audit s'affiche, les enregistrements les plus récents apparaissent. Servez-vous de la barre de défilement et des boutons de pagination situés au-dessus du journal pour consulter les enregistrements plus anciens.

Le journal présente les informations suivantes. Si un élément est tronqué, cliquez sur l'entrée partielle pour afficher son intégralité dans une fenêtre contextuelle.

Colonne	Description
Date	Date et heure de la modification, ajustées en fonction du fuseau horaire Pour assurer la cohérence des données du journal d'audit, assurez-vous que tous les ordinateurs qui exécutent les composants Websense présentent les mêmes paramètres de date et heure.
Utilisateur	Nom d'utilisateur de l'administrateur qui a effectué la modification
Serveur	Adresse IP ou nom de l'ordinateur exécutant le serveur Policy Server affecté par la modification N'apparaît que pour les modifications qui affectent Policy Server, par exemple les modifications apportées dans l'onglet Paramètres
Rôle	Rôle d'administration déléguée affecté par la modification Lorsqu'une modification affecte un client explicitement attribué en tant que client géré d'un rôle d'administration déléguée, cette modification apparaît comme affectant le rôle Super administrateur. Si la modification affecte un client membre d'une plage réseau, d'un groupe, d'un domaine ou d'une unité d'organisation attribué(e) au rôle, elle apparaît comme affectant le rôle d'administration déléguée.
Type	Élément de configuration modifié, tel qu'une stratégie, un filtre de catégories ou connexion/déconnexion
Élément	Identificateur de l'objet spécifique modifié, tel que le nom du filtre de catégories ou du rôle
Action	Type de modification apporté, par exemple ajout, suppression, modification, connexion, etc.
Précédent	Valeur d'origine, avant la modification
Actuel	Nouvelle valeur, après la modification

Tous ces éléments n'apparaissent pas pour tous les enregistrements. Par exemple, le rôle n'apparaît pas pour les enregistrements de connexion et de déconnexion.

Pour exporter les enregistrements du journal d'audit :

1. Sélectionnez une période dans la liste **Plage d'export**.

   Choisissez **60 derniers jours** pour exporter le fichier du journal d'audit complet.
2. Cliquez sur **Ok**.

   Si Microsoft Excel est installé dans l'ordinateur qui exécute TRITON - Web Security, le fichier exporté s'ouvre. Pour enregistrer ou imprimer ce fichier, utilisez les options d'Excel.

   Si Microsoft Excel n'est pas installé dans l'ordinateur qui exécute TRITON - Web Security, suivez les instructions qui s'affichent à l'écran pour localiser le logiciel ou enregistrer le fichier.

Arrêt et démarrage des services Websense

Les services Websense sont configurés pour démarrer à chaque redémarrage de l'ordinateur. Toutefois, il vous faudra dans certains cas arrêter ou démarrer un ou plusieurs composants du produit indépendamment de l'ordinateur.

> **Remarque**
> Si le service Filtering Service est en train de télécharger la base de données principale, il ne s'arrête pas avant la fin du téléchargement.

Lorsque vous arrêtez **tous les services Websense**, terminez toujours par les suivants, dans l'ordre :

1. Websense Policy Server
2. Websense Policy Broker
3. Base de données de stratégies Websense

Notez que, à moins que le problème n'affecte spécifiquement Policy Broker ou la base de données des stratégies, il est rarement nécessaire de redémarrer ces services. Dans la mesure du possible, évitez de les redémarrer.

Lorsque vous démarrez tous les services Websense, commencez systématiquement par les services de stratégie, dans le sens inverse de la fermeture (en commençant par la base de données des stratégies et en terminant par Policy Server).

Lorsque vous arrêtez les services associés à **Real-Time Monitor** :

- Arrêtez également les services TRITON - Web Security (Websense TRITON - Web Security et Websense Web Reporting Tools).
- Arrêtez les services Real-Time Monitor dans l'ordre suivant :
  1. Client Websense RTM
  2. Serveur Websense RTM
  3. Base de données Websense RTM

Démarrez les services Real-Time Monitor dans l'ordre inverse de leur fermeture (en commençant par la base de données RTM et en terminant par le client RTM).

Windows

1. Ouvrez la boîte de dialogue Services de Windows (**Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services**).
2. Cliquez du bouton droit sur le nom du service Websense, puis choisissez **Arrêter** ou **Démarrer**.

Linux

Dans les ordinateurs Linux, deux outils permettent d'arrêter et de démarrer les démons :

- Le script **WebsenseAdmin** démarre, arrête, puis redémarre **tous** les démons dans l'ordinateur.
- Le script **WebsenseDaemonControl** démarre, puis arrête des démons **individuels**.

Avertissement

N'utilisez pas la commande **kill** pour arrêter un service Websense, car cela risque de le corrompre.

Pour utiliser le script WebsenseAdmin pour démarrer ou arrêter tous les démons :

1. Accédez au répertoire **/opt/Websense**.
2. Vérifiez l'état des services Websense avec la commande suivante :

   ```
   ./WebsenseAdmin status
   ```

3. Arrêtez, démarrez ou redémarrez tous les services Websense avec les commandes :

   ```
   ./WebsenseAdmin stop
   ./WebsenseAdmin start
   ./WebsenseAdmin restart
   ```

Pour utiliser le script WebsenseDaemonControl pour démarrer ou arrêter un démon :

1. Accédez au répertoire **/opt/Websense**.
2. Entrez la commande suivante :

   ```
   ./WebsenseDaemonControl
   ```

   La liste des composants installés qui s'affiche indique si chaque processus s'exécute ou est arrêté.
3. Pour démarrer ou arrêter le processus associé, entrez la lettre associée à un composant. Pour réactualiser la liste, entrez **R**.
4. Lorsque vous avez terminé, entrez **Q** ou **X** pour fermer l'outil.

Dispositif V-Series

Dans les dispositifs Websense V-Series, utilisez Appliance Manager pour arrêter, démarrer et redémarrer les services Websense.

Pour redémarrer les services :

1. Ouvrez la page État > Général. Cette page s'affiche par défaut lorsque vous vous connectez à Appliance Manager.
2. Faites défiler l'écran jusqu'à la section Network Agent, puis cliquez sur **Restart Module (Redémarrer le module)**.
3. Après le redémarrage du module Network Agent, accédez à la section Web Security, puis cliquez sur **Restart Module (Redémarrer le module)**.

Pour arrêter les services (par exemple pour effectuer une tâche de maintenance) :

1. Naviguez jusqu'à la section Network Agent de la page État > Général, puis cliquez sur **Arrêter les services**.
2. Dans la section Websense Web Security, cliquez également sur **Arrêter les services**.
3. Lorsque vous êtes à nouveau prêt à démarrer les services :
   a. Accédez à la section Websense Web Security, puis cliquez sur **Démarrer les services**.
   b. Accédez à la section Network Agent, puis cliquez sur **Démarrer les services**.

Répertoires d'installation de Websense Web Security

Le répertoire d'installation de Websense Web Security varie selon le système d'exploitation de l'ordinateur, la version de ce système et selon si vous utilisez une nouvelle installation ou si vous avez procédé à la mise à niveau des composants existants.

Dans les ordinateurs **Windows**, les répertoires d'installation par défaut sont les suivants :

- Pour les composants installés dans des plates-formes 32 bits :
  ```
  C:\Program Files\Websense\Web Security\
  ```
- Pour les composants installés dans des plates-formes 64 bits :
  ```
  C:\Program Files (x86)\Websense\Web Security\
  ```

Dans les ordinateurs **Linux**, le répertoire d'installation par défaut est le suivant :

```
/opt/Websense/
```

Alertes

Rubriques connexes :

- *Contrôle des flux*, page 378
- *Configuration des options d'alerte générales*, page 378
- *Configuration des alertes système*, page 380
- *Configuration des alertes d'utilisation de catégories*, page 381
- *Configuration des alertes d'utilisation de protocole*, page 382

Pour simplifier le suivi et la gestion de Websense et de l'activité Internet des clients, les Super administrateurs peuvent configurer des alertes à envoyer lorsque les événements sélectionnés se produisent.

- Les **alertes Système** signalent aux administrateurs les événements de sécurité Web liés à l'état de l'abonnement et à l'activité de la base de données principale, ainsi que les événements Content Gateway, notamment la perte de contact avec un contrôleur de domaine, les problèmes d'espace des journaux, etc.

- Les **alertes d'utilisation** préviennent les administrateurs lorsque l'activité Internet des catégories ou des protocoles sélectionnés atteint les seuils configurés.

  Les alertes d'utilisation peuvent être générées pour des catégories ou des protocoles définis par Websense et personnalisés.
- Les **alertes d'activité suspecte** préviennent les administrateurs lorsque des événements du niveau de gravité sélectionné et associés à des menaces atteignent le seuil configuré.

Toutes les alertes peuvent être envoyées aux destinataires sélectionnés par courrier électronique ou SNMP.

Contrôle des flux

Rubriques connexes :

- *Alertes*, page 377
- *Configuration des options d'alerte générales*, page 378

Des contrôles intégrés aux alertes d'utilisation permettent d'éviter de générer un nombre excessif de messages d'alerte. Le paramètre **Maximum d'alertes par jour et par type d'utilisation** permet de spécifier une limite du nombre d'alertes envoyées en réponse aux requêtes des utilisateurs pour des catégories et des protocoles particuliers. Pour plus d'informations, consultez la section *Configuration des options d'alerte générales*, page 378.

Vous pouvez également définir des seuils pour chaque alerte d'utilisation de catégories et de protocoles et pour chaque alerte d'activité suspecte. Par exemple, si vous définissez un seuil de 10 pour une certaine catégorie, une alerte est générée après 10 requêtes pour cette catégorie (pour toutes les combinaisons de clients). Pour plus d'informations, consultez *Configuration des alertes d'utilisation de catégories*, page 381, et *Configuration des alertes d'utilisation de protocole*, page 382.

Supposons que le maximum d'alertes par jour soit défini sur 20 et le seuil d'alertes de catégorie sur 10. Les administrateurs ne sont alertés que les 20 premières fois où les requêtes de catégorie dépassent le seuil. Cela signifie que seules les 200 premières occurrences entraînent des messages d'alerte (seuil de 10 multiplié par la limite d'alertes de 20).

Configuration des options d'alerte générales

Rubriques connexes :

- *Alertes*, page 377
- *Configuration des alertes système*, page 380
- *Configuration des alertes d'utilisation de catégories*, page 381
- *Configuration des alertes d'utilisation de protocole*, page 382
- *Configuration des alertes d'activité suspecte*, page 384

Websense peut signaler aux administrateurs divers types d'événements système, de même que le dépassement des seuils définis pour l'utilisation d'Internet et l'activité suspecte.

La page **Paramètres > Alertes > Activer les alertes** permet de définir les paramètres de contrôle des flux et d'activer et de configurer une ou plusieurs méthodes de notification d'alerte. Après avoir activé les alertes dans cette page, servez-vous des autres pages de la section Paramètres > Alertes pour spécifier les alertes que vous souhaitez recevoir.

1. Sous Limites d'alertes par 24 heures, entrez un nombre pour définir le **Maximum d'alertes par jour et par type** à générer pour chaque utilisation de catégories, de protocoles et d'activité suspecte.

   Par exemple, vous pouvez configurer l'envoi d'une alerte d'utilisation de catégorie dès qu'une personne demande un site de la catégorie Sports à 5 reprises (seuil). Selon le nombre d'utilisateurs et leur schéma d'utilisation d'Internet, des centaines d'alertes pourraient être générées chaque jour.

   Si le maximum d'alertes par jour et par type est défini sur 10, les administrateurs sont avertis des 50 premières demandes de sites Sports effectuées au cours de la journée (5 requêtes par alerte multipliées par 10 alertes), mais pas des demandes suivantes effectuées le même jour pour cette même catégorie.
2. Cochez la case **Activer les alertes par e-mail** pour envoyer les alertes et les notifications par courrier électronique. Configurez ensuite ces paramètres de messagerie :

Adresse IPv4 ou nom du serveur SMTP	Adresse IPv4 ou nom d'hôte du serveur SMTP qui doit acheminer les alertes par e-mail
Depuis l'adresse de messagerie	Adresse e-mail à utiliser comme expéditeur des alertes
Adresse de messagerie de l'administrateur (À)	Adresse e-mail du principal destinataire des alertes
Adresses de messagerie des destinataires (Cc)	Adresses e-mail de jusqu'à 50 destinataires supplémentaires. Chaque adresse doit être placée sur une ligne distincte.

3. Cochez la case **Activer les alertes SNMP** pour envoyer des messages d'alerte via le système d'interruption SNMP de votre réseau. Fournissez ensuite les informations relatives à votre système d'interruption SNMP.

Nom de la communauté	Nom de la communauté d'interruption dans votre serveur d'interruption SNMP
Adresse IPv4 ou nom d'hôte	Adresse IPv4 ou nom d'hôte du serveur d'interruption SNMP
Port	Numéro de port utilisé par les messages SNMP. La valeur par défaut est 162.

4. Lorsque vous avez terminé, 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)**.

Configuration des alertes système

Rubriques connexes :

- *Alertes*, page 377
- *Configuration des options d'alerte générales*, page 378
- *Vérification de l'état actuel du système*, page 385

TRITON - Web Security affiche les informations détaillées de fonctionnement et d'état du système via la page **État > Alertes**, décrite à la section *Vérification de l'état actuel du système*, page 385.

Pour être sûr que les événements système importants soient signalés aux administrateurs, configurez les alertes système de Websense de sorte qu'elles soient distribuées par courrier électronique par le biais d'un système d'interruption SNMP.

Les administrateurs de Websense Web Security Gateway et Gateway Anywhere ont la possibilité d'activer les alertes système pour les événements Web Security (liés aux problèmes d'abonnement et de téléchargement des bases de données) et pour les événements Content Gateway liés à divers problèmes.

La page **Paramètres > Alertes > Système** vous permet de définir les alertes à envoyer et de sélectionner les méthodes utilisées pour envoyer chaque notification.

Pour activer une alerte, sélectionnez une ou plusieurs cases à cocher situées à droite du résumé du message pour indiquer comment avertir les administrateurs. Selon les méthodes activées dans la page Activer les alertes, les choix potentiels sont **E-mail** et **SNMP**, ou une combinaison des deux.

Pour désactiver une alerte, désactivez toutes les cases à cocher situées à droite du résumé du message.

Par défaut, toutes les alertes sont activées. Si vous avez fourni des informations SMTP pour les notifications par courrier électronique, quatre événements Web Security ne peuvent pas être désactivés :

- Le téléchargement de la base de données principale Websense a échoué.
- Le nombre d'utilisateurs en cours dépasse votre niveau d'abonnement.
- Votre abonnement arrive à expiration dans un mois.
- Votre abonnement arrive à expiration dans une semaine.

Trois autres alertes sont facultatives :

- Le nombre d'utilisateurs en cours a atteint 90 % de votre niveau d'abonnement.
- Les moteurs de recherche pris en charge par le filtrage de la recherche ont été modifiés.
- La base de données principale Websense a été mise à jour.

Dans les environnements Websense Web Security Gateway et Gateway Anywhere, vous avez la possibilité d'activer les alertes système supplémentaires suivantes :

- Un contrôleur de domaine est en panne.
- Le téléchargement de la base de données d'analyse a échoué.
- Le décryptage et l'inspection du contenu sécurisé a été désactivé.
- L'espace réservé aux journaux devient très insuffisant.
- Les informations sur votre abonnement n'ont pas pu être récupérées.

- La limite de connexions approche et des connexions vont être abandonnées.
- Des alertes non critiques ont été reçues. (Pour plus d'informations sur les conditions pouvant déclencher cette alerte, consultez la section *Alertes non critiques de Content Gateway*, page 500.)

Lorsque vous avez terminé, 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)**.

Configuration des alertes d'utilisation de catégories

Rubriques connexes :

- *Alertes*, page 377
- *Contrôle des flux*, page 378
- *Configuration des options d'alerte générales*, page 378
- *Ajout d'alertes d'utilisation de catégories*, page 382

Websense peut vous avertir lorsque l'activité Internet liée à des catégories d'URL particulières atteint un seuil défini. Vous pouvez définir des alertes pour les requêtes autorisées ou bloquées de cette catégorie.

Par exemple, vous pourriez souhaiter être prévenu(e) chaque fois que 50 requêtes ont été autorisées pour des sites de la catégorie Shopping afin de voir si vous devez placer des restrictions sur cette catégorie. Vous pourriez également souhaiter recevoir une alerte chaque fois que 100 requêtes ont été bloquées pour des sites de la catégorie Divertissement afin de savoir si les utilisateurs s'adaptent à la nouvelle stratégie d'utilisation d'Internet.

La page **Paramètres > Alertes > Utilisation de catégorie** permet d'afficher les alertes déjà définies et d'ajouter ou de supprimer des catégories d'alerte d'utilisation.

1. Consultez les listes **Alertes d'utilisation de catégorie autorisée** et **Alertes d'utilisation de catégorie bloquée** pour découvrir les catégories configurées pour des alertes, le seuil de chacune et les méthodes d'alerte sélectionnées.
2. Cliquez sur **Ajouter** sous la liste appropriée pour ouvrir la page Ajouter des alertes d'utilisation de catégorie (voir *Ajout d'alertes d'utilisation de catégories*, page 382) et configurer d'autres catégories d'URL pour les alertes.
3. Cochez la case des catégories que vous souhaitez retirer de la liste, puis cliquez sur **Supprimer** sous la liste appropriée.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Utilisation de catégorie. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout d'alertes d'utilisation de catégories

Rubriques connexes :

- *Alertes*, page 377
- *Configuration des options d'alerte générales*, page 378
- *Configuration des alertes d'utilisation de catégories*, page 381

La page **Ajouter des alertes d'utilisation de catégorie** s'affiche lorsque vous cliquez sur Ajouter dans la page Utilisation de catégorie. Cette page vous permet de sélectionner de nouvelles catégories pour des alertes d'utilisation, de définir le seuil de ces alertes et de choisir les méthodes d'alerte.

1. Cochez la case accolée à chaque catégorie à ajouter avec le même seuil et les mêmes méthodes d'alerte.

   Remarque
   Vous ne pouvez pas ajouter d'alertes d'utilisation pour les catégories exclues de la journalisation. Voir *Configuration du mode de journalisation des requêtes filtrées*, page 398.

2. Définissez le **Seuil** en sélectionnant le nombre de requêtes entraînant l'envoi d'une alerte.
3. Cochez la case de chaque méthode d'alerte désirée (**E-mail**, **SNMP**) pour ces catégories.

   Seules les méthodes d'alerte activées dans la page Alertes (voir *Configuration des options d'alerte générales*, page 378) peuvent être sélectionnées ici.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Utilisation de catégorie (voir *Configuration des alertes d'utilisation de catégories*, page 381). Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Configuration des alertes d'utilisation de protocole

Rubriques connexes :

- *Alertes*, page 377
- *Contrôle des flux*, page 378
- *Configuration des options d'alerte générales*, page 378
- *Ajout d'alertes d'utilisation de protocole*, page 383

Websense peut vous avertir lorsque l'activité Internet liée à un protocole particulier atteint un seuil défini. Vous pouvez définir des alertes pour les requêtes autorisées ou bloquées du protocole sélectionné.

Par exemple, vous pourriez souhaiter être prévenu(e) chaque fois que 50 requêtes ont été autorisées pour un protocole de messagerie instantanée spécifique afin de voir si vous devez placer des restrictions sur ce protocole. Vous pourriez également souhaiter recevoir une alerte chaque fois que 100 requêtes ont été bloquées pour un protocole de partage de fichiers (P2P) afin de savoir si les utilisateurs s'adaptent à la nouvelle stratégie d'utilisation d'Internet.

Dans l'onglet Paramètres, utilisez la page **Alertes > Utilisation de protocole** pour consulter les alertes déjà établies et ajouter ou supprimer des protocoles pour les alertes d'utilisation.

1. Consultez les listes **Alertes d'utilisation de protocole autorisée** et **Alertes d'utilisation de protocole bloquée** pour découvrir les protocoles configurés pour des alertes, le seuil de chacune et les méthodes d'alerte sélectionnées.
2. Cliquez sur **Ajouter** sous la liste appropriée pour ouvrir la page Ajouter des alertes d'utilisation de protocole (voir *Ajout d'alertes d'utilisation de protocole*, page 383) et configurer d'autres protocoles pour les alertes.
3. Cochez la case des protocoles que vous souhaitez retirer de la liste, puis cliquez sur **Supprimer** sous la liste appropriée.
4. Lorsque vous avez terminé, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Utilisation de protocole. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout d'alertes d'utilisation de protocole

Rubriques connexes :

- *Alertes*, page 377
- *Configuration des options d'alerte générales*, page 378
- *Configuration des alertes d'utilisation de protocole*, page 382

Consultez la page **Utilisation de protocole > Ajouter des alertes d'utilisation de protocole** pour sélectionner de nouveaux protocoles pour les alertes d'utilisation, définir le seuil de ces alertes et choisir les méthodes d'alerte.

1. Cochez la case accolée à chaque protocole à ajouter avec le même seuil et les mêmes méthodes d'alerte.

> **Remarque**
>
> Vous ne pouvez pas sélectionner un protocole pour les alertes si ce dernier n'est pas défini pour la journalisation dans un ou plusieurs filtres de protocoles.
>
> Les alertes de protocole ne reflètent que l'utilisation des clients gérés par un filtre de protocoles qui journalise ce protocole.

2. Définissez le **Seuil** en sélectionnant le nombre de requêtes entraînant l'envoi d'une alerte.

3. Sélectionnez la méthode d'alerte désirée (**E-mail**, **SNMP**) pour ces protocoles.

   Seules les méthodes d'alerte activées dans la page Alertes (voir *Configuration des options d'alerte générales*, page 378) peuvent être sélectionnées ici.

4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Utilisation de protocole (voir *Configuration des alertes d'utilisation de protocole*, page 382). Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Configuration des alertes d'activité suspecte

Rubriques connexes :

- *Alertes*, page 377
- *Contrôle des flux*, page 378
- *Configuration des options d'alerte générales*, page 378

Websense peut vous avertir lorsqu'une activité suspecte du niveau de gravité défini atteint le seuil spécifié. Vous pouvez définir des alertes pour les requêtes autorisées et bloquées à chaque niveau de gravité.

Content Gateway étant requis pour détecter les alertes de niveau critique et élevé, les alertes associées à ces niveaux de gravité ne peuvent pas être configurées dans les déploiements Websense Web Security et Websense Web Filter.

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)**. Des informations détaillées sur ces événements s'affichent dans le tableau de bord Threats (Menaces).

La page présente deux tableaux : **Permitted Suspicious Activity Alerts (Alertes d'activité suspecte autorisée)** et **Blocked Suspicious Activity Alerts (Alertes d'activité suspecte bloquée)**. Chaque tableau indique :

- Le niveau de **gravité** à configurer. Les quatre niveaux de gravité sont Critique, Élevée, Moyenne et Faible. Le niveau de gravité dépend de la catégorie de menace associée à l'alerte. Pour plus d'informations, consultez la section *Affectation d'un niveau de gravité à une activité suspecte*, page 39.
- Le **Seuil** d'alerte. Par défaut, le seuil des alertes de gravité critique et élevée, autorisée et bloquée, est défini sur **1**.
- Une ou plusieurs méthodes de notification. Les alertes d'activité suspecte peuvent être envoyées via **E-mail**, **SNMP** ou les deux.
- Si l'alerte est **Activée** ou non. Une coche verte indique que des alertes ont été générées pour l'activité suspecte du niveau de gravité sélectionné. Un « X » rouge indique que les alertes sont désactivées pour le niveau de gravité sélectionné.

Pour mettre à jour les paramètres des alertes d'activité suspecte :

1. Cochez la case située à gauche d'un niveau de gravité, puis cliquez sur **Activer** ou **Désactiver** pour activer ou arrêter les alertes du type sélectionné.
2. Dans le cas des alertes activées, saisissez un nombre dans le champ **Seuil** pour définir le nombre d'événements suspects entraînant la génération d'une alerte.
3. Sélectionnez chaque méthode de notification (**E-mail**, **SNMP**) à utiliser pour envoyer les alertes d'activité suspecte.

Seules les méthodes d'alerte activées dans la page Activer les alertes (voir *Configuration des options d'alerte générales*, page 378) peuvent être sélectionnées ici.

4. 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)**.

Vérification de l'état actuel du système

Utilisez la page **État > Alertes** pour obtenir des informations sur les problèmes qui affectent le bon fonctionnement de votre logiciel Websense, de l'aide sur le dépannage et consulter les détails des dernières mises à jour en temps réel de la base de données principale Websense.

La liste **Alertes actives** présente l'état des composants Websense surveillés.

- Pour plus d'informations sur les composants surveillés, cliquez sur **Sur quoi porte la surveillance ?** au-dessus de la liste des messages d'alerte.
- Pour résoudre un problème, cliquez sur le bouton **Solutions** accolé au message d'erreur ou d'avertissement.
- Pour masquer un message d'alerte, cliquez sur **Hide Persistent Alerts (Masquer les alertes permanentes)**. Si votre organisation n'utilise pas Log Server, Network Agent ou User Service, ou si vous n'envisagez pas d'activer WebCatcher, cochez la case appropriée dans la colonne **Hide Alert (Masquer l'alerte)** du tableau. Les alertes associées aux services sélectionnés ne s'affichent plus.

La liste **Mises à jour de la base de données en temps réel** vous renseigne sur les mises à jour d'urgence de la base de données principale Websense, en indiquant :

- La date et l'heure de la mise à jour
- Le type de mise à jour
- Le nouveau numéro de version de la base de données
- La raison de la mise à jour
- L'adresse IP de l'instance de Filtering Service qui a reçu la mise à jour

Ces mises à jour supplémentaires viennent compléter les mises à jour régulières et planifiées de la base de données principale et peuvent être utilisées, par exemple, pour recatégoriser un site classé temporairement dans la mauvaise catégorie. Websense vérifie la présence de mises à jour de la base de données toutes les heures.

Pour les utilisateurs de Websense Web Security, la page Alertes comprend une troisième liste : **Mises à jour de sécurité en temps réel**. Cette liste est au même format que la liste Mises à jour de la base de données en temps réel, mais indique de façon plus spécifique les mises à jour de base de données liées à la sécurité.

L'installation des mises à jour de sécurité dès leur création élimine les failles liées aux attaques de type phishing (usurpation d'identité), aux applications et au code malveillants infectant les applications ou les sites Web.

Pour plus d'informations sur les mises à jour de la sécurité en temps réel, consultez la section *Real-Time Security Updates™*, page 28.

Servez-vous du bouton **Imprimer** situé en haut de la page pour ouvrir une fenêtre secondaire présentant une version imprimable de la zone Alertes. Servez-vous des options du navigateur pour imprimer la page, qui omet toutes les options de navigation affichées dans la principale fenêtre de TRITON - Web Security.

Sauvegarde et restauration de vos données Websense

Rubriques connexes :

- *Planification des sauvegardes*, page 388
- *Exécution de sauvegardes immédiates*, page 390
- *Maintenance des fichiers de sauvegarde*, page 391
- *Restauration de vos données Websense*, page 391
- *Interruption des sauvegardes planifiées*, page 393
- *Références des commandes*, page 393

L'utilitaire de sauvegarde et de restauration de Websense simplifie la sauvegarde des données des stratégies et des paramètres Websense et permet de restaurer une configuration précédente. Les données sauvegardées par cet utilitaire sont également utilisées pour importer les informations de configuration de Websense après une mise à niveau.

Important

Assurez-vous que tous les administrateurs soient déconnectés de TRITON - Web Security avant de sauvegarder ou de restaurer votre configuration.

L'utilitaire de sauvegarde enregistre :

- 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 configuration locales, telles que les paramètres de Filtering Service et Log Server, stockées par chaque serveur Policy Server
- Les fichiers d'initialisation et de configuration des composants de Websense

Le processus de sauvegarde fonctionne de la manière suivante :

1. Vous déclenchez une sauvegarde immédiate (voir *Exécution de sauvegardes immédiates*, page 390) ou vous définissez un planning de sauvegarde (voir *Planification des sauvegardes*, page 388).
   - Vous pouvez déclencher manuellement une sauvegarde à tout moment.
   - Les fichiers de sauvegarde sont stockés dans le répertoire défini lors de l'exécution ou de la planification de la sauvegarde.
2. L'utilitaire de sauvegarde vérifie tous les composants Websense présents dans l'ordinateur, collecte les données concernées par la sauvegarde et crée un fichier d'archive. Le nom du fichier est au format suivant :

   `wsbackup_<aaaa-mm-jj_hhmmss>.tar.gz`

   Ici, <aaaa-mm-jj_hhmmss> représente la date et l'heure de la sauvegarde. L'extension **tar.gz** est un format de fichier compressé portable.

   Seul l'utilisateur racine (Linux) et les membres du groupe Administrateurs (Windows) peuvent accéder aux fichiers de sauvegarde.

Exécutez l'utilitaire de sauvegarde Websense dans chaque ordinateur comprenant des composants Websense. L'outil identifie et enregistre tous les fichiers suivants qu'il détecte dans l'ordinateur en cours :

Chemin	Nom du fichier
\Program Files *ou* **Program Files (x86)\Websense\Web Security\bin** ou **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf securewispproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf pg_hba.conf
BlockPages/*/Custom	Tous les paramètres des pages de blocage personnalisées
tomcat/conf/Catalina/Localhost	mng.xml
Windows\system32	isa_ignore.txt ignore.txt

Stockez les fichiers de sauvegarde de Websense dans un endroit sécurisé. Ces fichiers doivent faire partie des procédures de sauvegarde régulières de votre organisation.

Pour restaurer une configuration précédente :

1. Récupérez les fichiers de sauvegarde sur leur site de stockage.

2. Copiez chaque fichier de sauvegarde dans l'ordinateur Websense sur lequel il a été créé.

> **Important**
>
> N'essayez pas d'utiliser un fichier de sauvegarde créé sur une plate-forme de système d'exploitation pour restaurer la configuration d'une installation sur une autre plate-forme.
>
> Par exemple, n'essayez pas de restaurer un fichier de sauvegarde créé sous Linux dans un ordinateur Windows.

3. Exécutez l'utilitaire de sauvegarde en mode restauration.

> **Important**
>
> Servez-vous toujours de l'utilitaire de sauvegarde pour restaurer une configuration de Websense. N'utilisez pas d'autres utilitaires d'extraction pour récupérer les fichiers de l'archive.
>
> Si le fichier de sauvegarde est corrompu, vous ne pourrez pas restaurer vos paramètres.

Au cours du processus de sauvegarde, les messages d'erreur ou d'avertissement éventuels s'affichent sur l'ordinateur dans lequel la restauration est effectuée.

Planification des sauvegardes

Rubriques connexes :

- *Exécution de sauvegardes immédiates*, page 390
- *Maintenance des fichiers de sauvegarde*, page 391
- *Restauration de vos données Websense*, page 391
- *Interruption des sauvegardes planifiées*, page 393
- *Références des commandes*, page 393

Prévenez les administrateurs de Websense du planning de sauvegarde afin qu'ils puissent se déconnecter de TRITON - Web Security pendant ce processus.

Pour planifier des sauvegardes :

- Sous Windows :
  1. Ouvrez une invite de commande et localisez le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut).
  2. Entrez la commande suivante :

```
wsbackup -s -t "<m> <h> <jour_du_mois> <mois>
<jour_de_semaine>" -d <répertoire>
```

Notez que les informations de date utilisent le format **crontab** et que les guillemets et les espaces sont obligatoires.

- Sous Linux :

  1. Ouvrez une invite de commande et naviguez jusqu'au répertoire **Websense** (/opt/Websense/, par défaut).
  2. Entrez la commande suivante :

     ```
     ./WebsenseTools -b -s -t \"<m> <h> <jour_du_mois>
     <mois> <jour_de_semaine>\" -d <répertoire>
     ```

     En plus des caractères \" situés au début et à la fin de la chaîne complète de date et heure, lorsque la chaîne comprend des astérisques (*), ces derniers doivent également être entourés d'une paire \". Par exemple :

     ```
     ./WebsenseTools -b -s -t \"45 1 \"*\" \"*\" 5\"
     ```

     Ici, l'exécution de la sauvegarde est programmée à 1h45 les vendredis (quel que soit le mois ou la date).

Remplacez les variables de l'exemple par les informations suivantes :

Variable	Informations
<m>	0 à 59 Spécifie la minute exacte du démarrage de la sauvegarde
<h>	0 à 23 Spécifie l'heure du démarrage de la sauvegarde
<jour_du_mois>	1 à 31 Spécifie la date à laquelle la sauvegarde doit être effectuée. Si vous planifiez une sauvegarde pour les jours 29 à 31, l'utilitaire se sert de la procédure de substitution standard du système d'exploitation pour les mois qui ne comprennent pas cette date.
<mois>	1 à 12 Spécifie le mois au cours duquel la sauvegarde doit être effectuée
<jour_de_la_semaine>	0 à 6 Définit un jour de la semaine. 0 correspond au dimanche.

Chaque champ peut recevoir un nombre, un astérisque ou une liste de paramètres. Consultez les références du format **crontab** pour plus d'informations.

Exécution de sauvegardes immédiates

Rubriques connexes :

- *Planification des sauvegardes*, page 388
- *Maintenance des fichiers de sauvegarde*, page 391
- *Restauration de vos données Websense*, page 391
- *Interruption des sauvegardes planifiées*, page 393
- *Références des commandes*, page 393

Avant d'exécuter l'Utilitaire de sauvegarde, assurez-vous que tous les administrateurs soient déconnectés de TRITON - Web Security.

Pour déclencher une sauvegarde immédiate :

- Sous Windows :
  1. Ouvrez une invite de commande et localisez le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut).
  2. Entrez la commande suivante :

     ```
     wsbackup -b -d <répertoire>
     ```
- Sous Linux :
  1. Ouvrez une invite de commande et naviguez jusqu'au répertoire **Websense** (/opt/Websense/, par défaut).
  2. Entrez la commande suivante :

     ```
     ./WebsenseTools -b -b -d <répertoire>
     ```

Ici, <répertoire> désigne le répertoire de destination de l'archive de la sauvegarde.

Avertissement

Ne stockez pas les fichiers de sauvegarde dans le répertoire **bin** de Websense. En effet, ce répertoire est supprimé si vous désinstallez Websense.

Lorsque vous démarrez une sauvegarde immédiate, les messages d'erreur et les notifications éventuels s'affichent sur la console de l'ordinateur exécutant la sauvegarde.

Maintenance des fichiers de sauvegarde

Rubriques connexes :

- *Planification des sauvegardes*, page 388
- *Exécution de sauvegardes immédiates*, page 390
- *Restauration de vos données Websense*, page 391
- *Interruption des sauvegardes planifiées*, page 393
- *Références des commandes*, page 393

Lorsque vous effectuez une sauvegarde, un fichier de configuration (**WebsenseBackup.cfg**) est créé et stocké avec l'archive de la sauvegarde. Ce fichier de configuration spécifie :

- Le délai de conservation de l'archive dans le répertoire de sauvegarde
- La quantité maximale d'espace disque pouvant être utilisée par tous les fichiers de sauvegarde dans le répertoire

Modifiez le fichier **WebsenseBackup.cfg** dans un éditeur de texte quelconque pour changer ces paramètres :

Paramètre	Valeur
KeepDays	Nombre de jours pendant lesquels les fichiers d'archive doivent rester dans le répertoire de sauvegarde. La valeur par défaut est 365.
KeepSize	Nombre d'octets alloués aux fichiers de sauvegarde. La valeur par défaut est 10857600.

Tous les fichiers antérieurs à la valeur **KeepDays** sont retirés du répertoire de sauvegarde. Si la quantité d'espace disque allouée est dépassée, les fichiers les plus anciens sont supprimés du répertoire de sauvegarde pour faire de la place aux nouveaux.

Restauration de vos données Websense

Rubriques connexes :

- *Planification des sauvegardes*, page 388
- *Exécution de sauvegardes immédiates*, page 390
- *Maintenance des fichiers de sauvegarde*, page 391
- *Interruption des sauvegardes planifiées*, page 393
- *Références des commandes*, page 393

Lorsque vous restaurez les données de votre configuration de Websense, veillez à restaurer les données des composants présents dans l'ordinateur en cours. Assurez-vous également que tous les administrateurs soient déconnectés de TRITON - Web Security.

Si vous exécutez le processus de restauration dans l'ordinateur Policy Broker, une fois la restauration terminée, redémarrez tous les services Websense de votre déploiement. Cela inclut les services activés et désactivés dans l'ordinateur Policy Broker.

Pour démarrer le processus de restauration :

- Sous Windows :
  1. Ouvrez une invite de commande et localisez le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut).
  2. Entrez la commande suivante :

     ```
     wsbackup -r -f fichier_archive.tar.gz
     ```
- Sous Linux :
  1. Ouvrez une invite de commande et naviguez jusqu'au répertoire **Websense** (/opt/Websense/, par défaut).
  2. Entrez la commande suivante :

     ```
     ./WebsenseTools -b -r -f fichier_archive.tar.gz
     ```

> **Important**
> Le processus de restauration peut durer plusieurs minutes. Ne l'interrompez pas avant la fin.

Pendant le processus de restauration, l'utilitaire de sauvegarde arrête tous les services Websense. Si l'utilitaire ne peut pas arrêter les services, il envoie un message pour inviter l'utilisateur à les arrêter manuellement. Les services doivent être arrêtés dans l'ordre indiqué à la section *Arrêt et démarrage des services Websense*, page 375.

L'utilitaire de sauvegarde enregistre certains fichiers utilisés pour la communication avec les produits d'intégration tiers. Ces fichiers étant situés hors de la structure de répertoires de Websense, vous devez les restaurer manuellement, en copiant chacun d'eux dans le répertoire approprié.

Les fichiers qui doivent être restaurés manuellement comprennent :

Nom du fichier	Restaurer dans
isa_ignore.txt	**Windows\system32**
ignore.txt	**Windows\system32\bin**

Interruption des sauvegardes planifiées

Rubriques connexes :

- *Planification des sauvegardes*, page 388
- *Exécution de sauvegardes immédiates*, page 390
- *Maintenance des fichiers de sauvegarde*, page 391
- *Restauration de vos données Websense*, page 391
- *Références des commandes*, page 393

Pour effacer le planning de sauvegarde et arrêter les sauvegardes planifiées en cours d'exécution, ouvrez une invite de commande et accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut). Entrez la commande suivante :

```
wsbackup -u
```

Références des commandes

Rubriques connexes :

- *Planification des sauvegardes*, page 388
- *Exécution de sauvegardes immédiates*, page 390
- *Maintenance des fichiers de sauvegarde*, page 391
- *Restauration de vos données Websense*, page 391
- *Interruption des sauvegardes planifiées*, page 393

Seul l'utilisateur racine (sous Linux) ou un membre du groupe Administrateurs (sous Windows) peut exécuter l'utilitaire de sauvegarde.

Les commandes **wsbackup** et **WebsenseTools -b** acceptent les options suivantes :

- -b (ou --backup)
- -d chemin_répertoire (ou --dir chemin_répertoire)
- -f nom_complet_fichier (ou --file nom_complet_fichier)
- -h (ou --help, ou -?)
- -r (ou --restore)
- -s (ou --schedule)
- -t (ou --time)
- -u (ou --unschedule)
- -v (ou --verbose [0 - 3])

17 Administration de la génération de rapports

Rubriques connexes :

- *Configuration du mode de journalisation des requêtes filtrées*, page 398
- *Attribution de catégories aux classes de risque*, page 396
- *Configuration des préférences de génération de rapports*, page 397
- *Configuration de Log Server*, page 400
- *Paramètres d'administration de la base de données d'activité*, page 408
- *Configuration des rapports d'investigation*, page 421
- *Rapports sur activité propre*, page 425

Dans les organisations qui exploitent uniquement le compte d'administrateur par défaut (admin), tous ceux qui utilisent TRITON - Web Security ont accès à tous les outils et paramètres de génération de rapports. Dans les organisations qui exploitent l'administration déléguée, l'accès aux paramètres et aux outils de génération des rapports est contrôlé par les membres du rôle Super administrateur (voir *Modification des rôles*, page 337).

Les administrateurs qui ont accès aux paramètres de génération des rapports disposent de nombreuses options pour personnaliser les rapports au sein de leur environnement.

- La base de données principale Websense regroupe les catégories dans des **classes de risque**. Les classes de risque suggèrent des types ou des niveaux possibles de vulnérabilité représentés par les sites présents dans ces catégories. La page Paramètres > Général > Classes de risque vous permet de personnaliser les classes de risque pour votre organisation. Voir *Attribution de catégories aux classes de risque*, page 396.
- La page Paramètres > Génération de rapports > Préférences permet de configurer le serveur de messagerie utilisé pour distribuer les rapports, d'activer la fonction de génération de rapports sur l'activité propre et de configurer la durée de stockage des rapports planifiés dans l'ordinateur TRITON - Web Security. Vous pouvez également configurer Real-Time Monitor pour qu'il collecte systématiquement les données ou seulement lorsqu'il est ouvert. Voir *Configuration des préférences de génération de rapports*, page 397.

La journalisation est le processus qui consiste à stocker les informations relatives aux activités de filtrage de Websense dans une base de données d'activité afin de générer des rapports.

- La page Paramètres > Général > Journalisation permet d'activer la journalisation et de sélectionner les catégories et les informations des utilisateurs à journaliser. Pour plus d'informations, consultez la section *Configuration du mode de journalisation des requêtes filtrées*, page 398.

- La page Paramètres > Génération de rapports > Log Server permet de gérer le traitement des enregistrements de journal et les connexions à la base de données d'activité. Voir *Configuration de Log Server*, page 400.
- La page Paramètres > Génération de rapports > Base de données d'activité vous permet d'administrer cette base de données d'activité, et notamment ses options de partition, de journalisation des URL, de temps de navigation et de tendances des données. Voir *Paramètres d'administration de la base de données d'activité*, page 408.

Attribution de catégories aux classes de risque

Rubriques connexes :

- *Classes de risque*, page 54
- *Pages de blocage*, page 115
- *Exploitation des rapports pour évaluer l'efficacité du filtrage*, page 129

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

Les classes de risque sont essentiellement utilisées pour la génération de rapports. Certains graphiques du Tableau de bord Web Security surveillent l'activité Internet par classe de risque et vous permettent de générer des rapports d'investigation ou de présentation, triés par classe de risque.

La page **Paramètres > Général > Classes de risque** vous permet de vérifier ou de modifier chaque classe de risque incluse dans les catégories.

1. Sélectionnez une entrée dans la liste **Classes de risque**.
2. Examinez la liste **Catégories** pour identifier les catégories actuellement incluses dans cette classe de risque.

   Une coche indique que la catégorie est actuellement attribuée à la classe de risque sélectionnée. L'icône W bleue désigne les catégories incluses par défaut dans cette classe de risque.
3. Pour inclure ou exclure une catégorie de la classe de risque sélectionnée, cochez ou supprimez la coche de cette catégorie dans l'arborescence. Chaque catégorie peut appartenir à plusieurs Classes de risque.

   Les autres choix disponibles sont les suivants :

Option	Description
Sélectionner tout	Sélectionne toutes les catégories dans l'arborescence
Effacer tout	Désélectionne toutes les catégories dans l'arborescence
Restaurer les valeurs par défaut	Réinitialise les choix de catégories définis par Websense pour la classe de risque sélectionnée. Une icône W bleue désigne une catégorie par défaut.

4. Répétez ce processus pour chaque classe de risque.
5. Cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Configuration des préférences de génération de rapports

Rubriques connexes :

- *Rapports sur activité propre*, page 425
- *Planification des rapports de présentation*, page 143
- *Planification des rapports d'investigation*, page 172

La page **Paramètres > Génération de rapports > Préférences** vous permet de fournir les informations régissant l'envoi des rapports planifiés aux destinataires sélectionnés par courrier électronique, d'activer la fonction de génération de rapports sur l'activité propre, de définir la durée de stockage des rapports de présentation planifiés et de configurer le moment où Real-Time Monitor doit collecter les données.

1. Sous Email Reports (Envoyer les rapports par e-mail), entrez l'**adresse électronique** à afficher dans le champ « De » lorsque des rapports planifiés sont distribués par e-mail.
2. Entrez l'**Adresse IPv4 ou le nom du serveur SMTP** du serveur de messagerie à utiliser pour distribuer les rapports planifiés.
3. Cochez la case **Permettre aux utilisateurs de générer des rapports sur leur propre activité** pour autoriser les utilisateurs de votre organisation à accéder à TRITON - Web Security et à exécuter des rapports d'investigation sur leur propre activité Internet.

   Lorsque cette option est activée, l'URL utilisée pour accéder à la fonction de génération de rapports sur l'activité propre s'affiche. Voir *Rapports sur activité propre*, page 425.
4. Sous Rapports de présentation planifiés, utilisez la liste déroulante **Store reports for (Stocker les rapports pendant)** pour définir la durée de stockage des rapports dans l'ordinateur TRITON - Web Security (5 jours, par défaut).

   Notez qu'augmenter la durée de stockage des rapports a un impact sur la quantité d'espace disque requise dans l'ordinateur TRITON - Web Security. L'ordinateur TRITON - Web Security n'est pas un emplacement approprié pour le stockage à long terme des archives des rapports.
5. Servez-vous de la liste déroulante **Warn administrators... (Avertir les administrateurs)** pour définir la durée d'affichage de l'avertissement dans la page Review Reports (Examiner les rapports) avant la suppression d'un rapport de présentation planifié (3 jours, par défaut).

   L'objectif de cet avertissement est d'accorder suffisamment de temps aux administrateurs pour qu'ils puissent archiver les rapports importants dans un emplacement approprié avant leur suppression dans le serveur de gestion.
6. Sous Real-Time Monitor, activez un bouton radio pour définir le moment où Real-Time Monitor doit commencer à collecter les données des utilisateurs :

- Sélectionnez **Capture data only when Real-Time Monitor is active (Collecter les données lorsque Real-Time Monitor est actif uniquement)** (par défaut) pour améliorer les performances du système. Lorsque cette option est activée, la collecte de données commence lorsque vous démarrez Real-Time Monitor. Un bref délai (de quelques secondes) peut se produire avant que les enregistrements ne commencent à s'afficher à l'écran.
- Sélectionnez **Always capture data (Toujours collecter les données)** afin que le client Real-Time Monitor traite systématiquement les données de la base de données RTM, y compris lorsque personne ne consulte les données. Cette option peut avoir un impact notable sur les performances du système.

7. Cliquez sur **Enregistrer** pour implémenter vos modifications.

Configuration du mode de journalisation des requêtes filtrées

Rubriques connexes :

- *Présentation de la base de données d'activité*, page 406
- *Configuration de Log Server*, page 400

La page **Paramètres > Général > Journalisation** vous permet de définir les éléments suivants :

- L'adresse IP et le port utilisés par Filtering Service pour envoyer les enregistrements des journaux à Log Server
- (*Websense Web Security Gateway Anywhere*) Le port utilisé par Sync Service pour envoyer les enregistrements des journaux hybrides à Log Server
- Les informations d'identification des clients éventuellement envoyées par Filtering Service à Log Server en vue de leur utilisation dans les rapports
- Les catégories d'URL enregistrées dans le journal en vue de leur utilisation dans les rapports et les alertes d'utilisation de catégorie (voir *Configuration des alertes d'utilisation de catégories*, page 381)

Dans un environnement comprenant plusieurs serveurs Policy Server, configurez la page Journalisation séparément pour chaque instance de Policy Server. Toutes les instances de Filtering Service associées au serveur Policy Server actif envoient leurs enregistrements de journal au serveur Log Server identifié dans cette page.

Lorsque vous utilisez plusieurs serveurs Policy Server, notez que :

- Chaque serveur Policy Server peut communiquer avec une seule instance de Log Server.
- Pour que les données des rapports s'affichent correctement dans TRITON - Web Security, un serveur Log Server doit être associé à l'instance de base de Policy Server (instance de Policy Server définie lors de l'installation de TRITON - Web Security et indiquée à la page Paramètres > Général > Policy Server).

  Il s'agit généralement de l'instance de Policy Server installée avec Policy Broker (par exemple, l'instance de Policy Server installée dans le dispositif de source de stratégies complet).

- Si les champs d'adresse IP et de port de Log Server ne sont pas renseignés pour un serveur Policy Server, les instances de Filtering Service associées à ce serveur ne peuvent journaliser aucun trafic pour la génération de rapports ou d'alertes.
- Les informations relatives à la journalisation éventuelle des noms d'utilisateur et des adresses IP étant stockées centralement, ces mêmes paramètres servent à l'ensemble de votre déploiement.

  De la même façon, toutes les instances de Filtering Service et de Log Server partagent les modifications que vous apportez à la journalisation des catégories.

Si votre environnement comprend plusieurs serveurs Policy Server et Log Server, assurez-vous de vous connecter à chaque serveur Policy Server séparément et vérifiez que ce dernier communique bien avec le serveur Log Server approprié.

1. Entrez l'**Adresse IPv4 ou le nom d'hôte de Log Server**.
2. Entrez le **Port** utilisé par Filtering Service pour envoyer les enregistrements de journal à Log Server (55805, par défaut).
3. (*Websense Web Security Gateway Anywhere*) Entrez le port utilisé par Sync Service pour envoyer les enregistrements de journal du service hybride à Log Server.
4. Cliquez sur **Vérifier l'état** pour déterminer si TRITON - Web Security peut communiquer avec l'instance de Log Server via le port et l'emplacement définis.

   Un message indique si le test de la connexion a réussi. Actualisez l'adresse IP ou le nom d'hôte et le port, le cas échéant, jusqu'à ce que ce test réussisse.
5. Définissez le volume de données d'utilisateurs stockées dans les enregistrements de journal et affichées dans les rapports :
   - Pour journaliser les informations d'identification des ordinateurs qui accèdent à Internet, cochez la case **Journaliser les adresses IP**.
   - Pour journaliser les informations d'identification des utilisateurs qui accèdent à Internet, cochez la case **Journaliser le nom des utilisateurs**.

   Remarque

   Si vous ne journalisez pas les adresses IP ou les noms des utilisateurs, vos rapports ne contiennent aucune donnée relative aux utilisateurs. On parle parfois dans ce cas de **journalisation anonyme**.

   - Si vous utilisez Web Security Gateway ou Gateway Anywhere et que vous souhaitez que les tableaux du tableau de bord Threats (Menaces) présentent des informations sur le nom des périphériques sources lorsque celles-ci sont disponibles, cliquez sur **Log hostnames (Journaliser les noms d'hôte)**.

     Les informations de noms sont disponibles dans les journaux associés aux menaces uniquement. Elles ne sont pas disponibles pour l'activité Internet à laquelle aucun niveau de gravité n'est affectée.
6. Servez-vous de la liste **Journalisation de catégorie sélective** pour éventuellement définir les catégories d'URL à ne pas enregistrer. Les modifications apportées ici s'appliquent à tous les filtres de catégories de toutes les stratégies actives.

> **Remarque**
>
> Si vous désactivez la journalisation des catégories pour lesquelles des alertes d'utilisation sont configurées (voir *Configuration des alertes d'utilisation de catégories*, page 381), aucune alerte d'utilisation ne peut être envoyée.
>
> Les rapports ne peuvent pas comprendre d'informations sur les catégories non journalisées.

- Servez-vous du champ de recherche **Find category (Rechercher une catégorie)** pour accéder rapidement à une catégorie spécifique.
- Développez les catégories parentes en fonction de vos besoins pour modifier la journalisation des sous-catégories.
- Désactivez la case à cocher accolée au nom d'une catégorie pour arrêter la journalisation de cette catégorie.

  Vous devez sélectionner ou désélectionner chaque catégorie séparément. La sélection d'une catégorie parente ne sélectionne pas automatiquement ses sous-catégories. Pour simplifier vos sélections, utilisez **Sélectionner tout** et **Effacer tout**.

7. Cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Configuration de Log Server

Au cours de l'installation, vous configurez certains aspects du fonctionnement de Log Server, y compris ses interactions avec les composants de filtrage de Websense. La page **Paramètres > Génération de rapports > Log Server** vous permet d'actualiser ces paramètres ou de configurer d'autres détails du fonctionnement de Log Server.

Lorsque la mise à jour de votre configuration est terminée, cliquez sur **OK** pour mettre vos modifications en cache. Les modifications ne sont pas enregistrées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Si vous modifiez la connexion à la base de données, après l'enregistrement et le déploiement des modifications, redémarrez également le service **Websense TRITON - Web Security** au niveau du serveur de gestion afin d'actualiser la connexion à la base de données de tous les outils de génération de rapports.

Dans les environnements à plusieurs serveurs Log Server, les paramètres configurés dans cette page s'appliquent à l'instance de Log Server affectée au serveur Policy Server dont l'adresse IP ou le nom s'affiche dans la barre d'outils Web Security.

> **Remarque**
>
> La page Paramètres > Génération de rapports > Log Server remplace l'utilitaire de configuration de Log Server utilisé pour exécuter ces tâches dans les versions précédentes.

Vérification des informations de base de Log Server

Sous **Emplacement**, vérifiez l'adresse IP de Log Server. Au besoin, utilisez le champ **Port** pour mettre à jour le port par lequel Log Server communique avec Filtering Service (55805, par défaut).

Ce port doit correspondre au port de journalisation indiqué dans la page **Paramètres** > **Général** > **Journalisation**.

Configuration de la connexion à la base de données d'activité

Sous **Log Database Connection (Connexion à la base de données d'activité)**, configurez la connexion ODBC utilisée par Log Server pour se connecter à la base de données d'activité.

1. Définissez le **Nom de la source de données (DSN)** ODBC et saisissez une **Description** unique pour cette connexion à la base de données.
2. Indiquez l'**Emplacement de SQL Server** (adresse IP ou nom d'hôte, et nom de l'instance, le cas échéant) de l'installation Microsoft SQL Server hébergeant la base de données d'activité, ainsi que le **Port de connexion** utilisé pour envoyer les données à la base de données d'activité (1433, par défaut).
3. Si votre environnement utilise la mise en cluster de SQL Server, entrez l'adresse IP virtuelle du cluster.
4. Entrez le nom de la **Base de données par défaut** (wslogdb70, par défaut).
5. Activez ou non l'option **Use SSL to connect to the Log Database (Utiliser SSL pour se connecter à la base de données d'activité)**. Lorsque le cryptage SSL est activé :
   - BCP ne peut pas être utilisé pour ajouter des enregistrements dans la base de données d'activité.
   - Les connexions à la base de données d'activité sont plus lentes, ce qui affecte les performances des rapports.
   - Si vous exécutez TRITON - Web Security dans un dispositif Websense, la connexion entre la console et la base de données ne peut pas être cryptée. Cela signifie que si l'option « Forcer le cryptage du protocole » de Microsoft SQL Server est définie sur **Oui**, aucune donnée ne s'affiche dans le Tableau de bord Web Security ni dans les autres outils de génération de rapports.

Important

Lorsque les composants Microsoft SQL Server sont configurés de sorte que l'option « Faire confiance au certificat de serveur » soit définie sur **Non** (par défaut), les certificats SSL auto-signés ne sont pas acceptés pour le cryptage des connexions à la base de données.

Dans ce cas, les certificats SSL signés par une autorité de certification doivent être correctement déployés dans SQL Server, le serveur de gestion TRITON et les ordinateurs Log Server afin que vous puissiez activer l'option « Utiliser SSL » dans TRITON - Web Security.

Pour plus d'informations sur le cryptage de la base de données, reportez-vous à la documentation de SQL Server.

6. Définissez une méthode de connexion à Log Server :
   - Par défaut, l'option **Authentification SQL Server** est sélectionnée. Pour utiliser l'authentification SQL Server, fournissez le **Compte** et le **Mot de passe** SQL Server à utiliser.
   - Vous pouvez également utiliser une **Connexion sécurisée Windows (compte de connexion réseau)**. Le service Websense Log Server doit être configuré pour s'exécuter avec ce compte.
7. Cliquez sur **Tester la connexion** pour vérifier qu'il est possible de se connecter à la base de données d'activité à l'aide des identifiants fournis.

   Pour plus d'informations sur les tests effectués lorsque vous cliquez sur ce bouton, consultez la section *Test de la connexion à la base de données d'activité*, page 405.

Si vous modifiez la connexion à la base de données, après l'enregistrement et le déploiement des modifications, redémarrez également le service **Websense TRITON - Web Security** au niveau du serveur de gestion afin d'actualiser la connexion à la base de données de tous les outils de génération de rapports.

Définition du traitement des enregistrements de journal dans la base de données

Cliquez sur **Log Record Creation (Création des enregistrements dans le journal)** pour indiquer comment Log Server doit ajouter des enregistrements dans la base de données d'activité.

- **ODBC (Open Database Connectivity)** insère individuellement les enregistrements dans la base de donnée, en utilisant un pilote de base de données pour gérer les données entre Log Server et la base de données d'activité.

  Si vous sélectionnez cette option, définissez également le **Nombre maximum de connexions** pour configurer le nombre de connexions internes pouvant être établies entre Log Server et le moteur de base de données.
  - Pour Microsoft SQL Server Standard ou Enterprise, sélectionnez une valeur comprise entre 4 et 50, selon votre licence SQL Server.

    Remarque

    L'augmentation du nombre de connexions peut accroître la vitesse de traitement des enregistrements du journal, mais peut avoir un impact sur d'autres processus réseau qui utilisent le même serveur SQL Server. Dans la plupart des cas, il est préférable de définir un nombre de connexions inférieur à 20. Contactez votre administrateur de base de données pour obtenir de l'aide.
  - Pour Microsoft SQL Server Express, la valeur est définie sur **4** et n'est pas modifiable.
- **BCP (Bulk Copy Program)** (*recommandé*) insère les enregistrements dans la base de données d'activité par lots. Cette option est plus efficace que l'insertion ODBC et est activée par défaut lorsque le fichier **bcp.exe** est détecté dans l'ordinateur.

  L'option BCP n'est disponible que si vous avez installé les outils SQL Server Client (SQL Server 2005 SP4) ou les Outils de gestion - De base (SQL Server 2008) dans l'ordinateur Log Server.

  BCP ne peut pas être utilisé lorsque le cryptage SSL de SQL Server l'est également.

Si vous sélectionnez l'option BCP, définissez également les éléments suivants :

Option	Description
Emplacement du fichier BCP	Chemin d'accès au répertoire de stockage des fichiers BCP. Log Server doit pouvoir accéder à cet emplacement en lecture et en écriture. (Le dossier par défaut est C:\Program Files (x86)\Websense\Web Security\bin\Cache\BCP\.) Après avoir saisi le chemin, cliquez sur **Tester l'emplacement** pour vérifier que l'emplacement est accessible.
Taux de création du fichier	Nombre maximal de minutes consacrées par Log Server à placer les enregistrements dans un fichier de traitement par lots avant la fermeture de ce dernier et la création d'un nouveau Ce paramètre est combiné au paramètre de la taille des lots : Log Server crée un nouveau fichier de traitement par lots dès que l'une des limites est atteinte.
Taille maximale des lots	Nombre maximal d'enregistrements de journal avant la création d'un nouveau fichier de traitement par lots Ce paramètre est combiné au taux de création : Log Server crée un nouveau fichier de traitement par lots dès que l'une des limites est atteinte.

Après avoir sélectionné une méthode d'insertion des enregistrements de journal, cliquez sur **Log Cache Files (Fichiers de cache de journal)** pour indiquer où et comment les fichiers de cache de journal sont crées. Il s'agit là d'un emplacement de stockage temporaire pour les enregistrements de journal qui n'ont pas encore été traités dans la base de données d'activité ni déplacés vers des fichiers BCP.

1. Dans **Cache location (Emplacement du cache)**, indiquez l'emplacement dans lequel les fichiers de cache de journalisation de l'ordinateur Log Server doivent être stockés (C:\Program Files (x86)\Websense\Web Security\bin\Cache\, par défaut).
2. Cliquez sur **Tester l'emplacement** pour vérifier que ce chemin est accessible.
3. Dans le champ **Taux de création du fichier cache**, indiquez le nombre maximal de minutes (1, par défaut) que Log Server doit consacrer à l'envoi des informations d'accès Internet à un fichier cache du journal avant de le fermer et d'en créer un nouveau.
4. Dans le champ **Taille maximale du fichier cache**, indiquez la taille que le fichier de cache de journal doit atteindre avant que Log Server ne le ferme et en crée un nouveau.

Les paramètres de taux de création et de taille maximale du fichier fonctionnent en combinaison : Log Server crée un nouveau fichier cache de journal dès que l'une des limites est atteinte.

Ajustement des paramètres de taille de la base de données

Configurez les paramètres **Database Size Management (Gestion de la taille de la base de données)** en fonction des besoins de votre organisation. Plus le niveau de détails enregistrés est élevé, plus la base de données d'activité est volumineuse.

1. Pour réduire la taille de la base de données d'activité, cochez la case **Enable log record consolidation (Activer la consolidation des enregistrements de journal)**. Cette option combine plusieurs requêtes Internet similaires dans un même enregistrement de journal, ce qui réduit la granularité des données des rapports.

Si vous avez activé l'intégration SIEM, notez que Log Server applique la consolidation aux enregistrements de journal qu'il traite dans la base de données d'activité. Cette consolidation ne concerne pas les enregistrements transmis au produit SIEM.

Lorsque la consolidation est activée, les requêtes qui partagent tous les éléments suivants sont combinées dans un même enregistrement de journal :

- Nom du domaine (par exemple : www.websense.com)
- Catégorie
- Mot-clé
- Action (par exemple : Catégorie bloquée)
- Utilisateur/Adresse IP

L'enregistrement de journal inclut le nombre de requêtes combinées dans un enregistrement consolidé et la bande passante totale utilisée pour toutes les requêtes consolidées.

L'exécution des rapports est plus rapide lorsque la base de données d'activité est réduite. La consolidation peut cependant réduire la précision de certains rapports détaillés, du fait de la perte potentielle d'enregistrements distincts pour le même nom de domaine.

Important

Pour garantir la cohérence des rapports, créez une nouvelle partition de base de données chaque fois que vous activez ou désactivez la consolidation. De même, assurez-vous de générer des rapports à partir de partitions présentant le même paramètre de consolidation.

Avec Websense Web Security Gateway (Anywhere), lorsque la consolidation est activée, les chiffres affichés dans les rapports du filtrage Web qui incluent le trafic bloqué par l'analyse sont **inférieurs** à ceux qui s'affichent dans les rapports propres à l'analyse. Il s'agit là d'un effet secondaire du mode d'enregistrement de l'activité d'analyse.

2. Si vous activez la consolidation, définissez également l'**Intervalle de temps de la consolidation**. Cela représente la plus grande différence de temps autorisée entre les enregistrements les plus anciens et les plus récents combinés en un même enregistrement consolidé.

   Réduisez cet intervalle pour accroître la granularité de vos rapports. Augmentez cet intervalle pour optimiser la consolidation. N'oubliez pas qu'un intervalle plus important peut également accroître l'exploitation des ressources système, telles que la mémoire, le processeur et l'espace disque.

   Si vous activez la journalisation complète des URL dans la page Paramètres > Génération de rapports > Base de données d'activité, les enregistrements consolidés contiennent le chemin complet (jusqu'à 255 caractères) du premier site correspondant rencontré par Log Server.

   Supposons par exemple qu'un utilisateur ait visité les sites suivants, tous classés dans la catégorie Shopping.

   - www.domaine.com/chaussures
   - www.domaine.com/sacamains
   - www.domaine.com/bijoux

   Lorsque la journalisation complète des URL est activée, la consolidation crée une unique entrée de journal présentant 3 requêtes pour l'URL www.domain.com/chaussures.

3. Sous Accès et Visites, utilisez la case à cocher **Activer les visites** pour définir le niveau de granularité enregistré pour chaque requête Internet d'utilisateur.

   > **Remarque**
   > Il est préférable de créer une nouvelle partition de base de données avant de modifier la méthode de journalisation entre visites et accès. Pour créer une nouvelle partition de base de données, consultez la page **Paramètres > Génération de rapports > Base de données d'activité**.

   Lorsque cette option n'est **pas** activée, un enregistrement de journal distinct est créé pour chaque requête HTTP générée et présente des éléments de page différents, notamment les graphiques, les publicités, les vidéos intégrées, etc. Également appelée journalisation des accès, cette option crée une base de données d'activité beaucoup plus volumineuse et qui croît rapidement.

   Lorsque cette option est **activée**, Log Server combine les éléments individuels de la page Web (par exemple les graphiques et les publicités) dans un même enregistrement de journal comprenant les informations de bande passante de tous les éléments de la visite.

   Avec Websense Web Security Gateway (Anywhere), lorsque les visites sont activées, les chiffres affichés dans les rapports du filtrage Web qui incluent le trafic bloqué par l'analyse sont **inférieurs** à ceux qui s'affichent dans les rapports propres à l'analyse. Il s'agit là d'un effet secondaire du mode d'enregistrement de l'activité d'analyse.

Configuration de la communication avec User Service

Cliquez sur le bouton **User Service Connection (Connexion à User Service)**, puis servez-vous du champ **Intervalle de mise à jour des utilisateurs et des groupes** pour définir la fréquence de connexion de Log Server à User Service pour la récupération des informations relatives à l'affectation des noms d'utilisateur et des groupes (toutes les 12 heures, par défaut).

L'activité d'un utilisateur, dont les informations de nom d'utilisateur ou de groupe ont changé, continue à être prise en compte pour le groupe ou le nom d'utilisateur d'origine jusqu'à la prochaine mise à jour. Les organisations qui mettent fréquemment à jour leur service d'annuaire ou qui possèdent un grand nombre d'utilisateurs doivent envisager d'actualiser plus fréquemment les informations des utilisateurs/groupes.

Test de la connexion à la base de données d'activité

Les informations de connexion à la base de données utilisées par Log Server et les autres outils de génération de rapports peuvent être mises à jour à la page Paramètres > Génération de rapports > Log Server dans TRITON - Web Security.

La section Log Database Connection (Connexion à la base de données d'activité) de la page comprend un bouton **Tester la connexion**. Lorsque vous cliquez sur ce bouton, Log Server effectue les tests suivants :

1. Log Server récupère les informations mises à jour de la connexion à la base de données auprès de TRITON - Web Security.

   Si Log Server est arrêté, ou si le réseau reliant le serveur de gestion TRITON et l'ordinateur Log Server est inactif, ce test échoue. En cas d'échec de la connexion à Log Server, une erreur d'exception d'E/S s'affiche généralement.

2. Log Server utilise ODBC pour créer un nom de source de données (DSN) à utiliser lors des tests.
3. Log Server utilise le nom DSN pour établir la connexion à la base de données d'activité. Log Server vérifie ensuite que :
   - Une base de données Websense existe.
   - La version de la base de données est correcte.
4. Log Server vérifie ses autorisations sur la base de données.

   Pour plus d'informations sur les rôles et autorisations de base de données requis, consultez la section *Configuration des autorisations d'utilisateur pour Microsoft SQL Server*, page 485.
5. Log Server supprime le nom DSN qu'il a créé pour le test.
6. Log Server avertit TRITON - Web Security de la réussite de ses tests.

   En cas de notification d'échec, une erreur d'exception d'E/S s'affiche généralement.

Par ailleurs, TRITON - Web Security vérifie qu'il peut créer une connexion JDBC à la base de données. Le test TRITON - Web Security peut réussir, y compris en cas d'échec d'un test de Log Server.

Les nouvelles informations de connexion à la base de données ne sont pas utilisées tant que vous ne mettez pas vos modifications en cache avant de les enregistrer. À ce stade :

- Les nouvelles informations de connexion à la base de données sont enregistrées dans le fichier de configuration de Policy Server.
- Log Server crée un nom DSN permanent (en reproduisant le nom DSN temporaire créé lors du test de la connexion).

Redémarrez le service Websense TRITON - Web Security pour mettre à jour les outils de génération de rapports (par exemple, les rapports de présentation) et utiliser la nouvelle connexion à la base de données.

Présentation de la base de données d'activité

Rubriques connexes :

- *Tâches de la base de données*, page 407
- *Paramètres d'administration de la base de données d'activité*, page 408

La base de données d'activité (Log Database) stocke les enregistrements de l'activité Internet et les actions de filtrage Websense associées. Elle est créée pendant l'installation avec une base de données de catalogue et une partition de base de données.

La **base de données de catalogue** (wslogdb70, par défaut) fournit un unique point de connexion pour les différents composants de Websense qui doivent accéder à la base de données d'activité : tableaux de bord, Log Server, rapports de présentation et rapports d'investigation. Elle contient des informations sur la prise en charge des partitions de la base de données, y compris la liste des noms de catégorie, les définitions des classes de risque, les données de tendance, les correspondances utilisateurs/groupes, les tâches de bases de données, etc. La base de données de catalogue conserve également la liste de toutes les partitions disponibles dans la base de données.

Les **partitions de la base de données** stockent les enregistrements de journal individuels de l'activité Internet. Il existe 2 types de partitions :

- La partition de journalisation standard (wslogdb70_1, wslogdb70_2, etc.) stocke des informations sur toutes les requêtes Internet enregistrées. Les informations issues de la partition de journalisation standard servent à renseigner les rapports d'investigation et de présentation, ainsi que les graphiques des tableaux de bord.
- La partition des menaces (wslogdb70_amt_1) stocke des informations sur les requêtes auxquelles un niveau de gravité a été affecté (voir *Affectation d'un niveau de gravité à une activité suspecte*, page 39). Les informations issues de la partition des menaces servent à renseigner le tableau de bord Threats (Menaces).

De nouvelles partitions de journalisation standard sont créées en fonction de la taille ou d'un intervalle de dates. Pour plus d'informations, consultez la section *Configuration des options de partition de la base de données*, page 409.

- Lorsque les partitions sont basées sur la taille, tous les enregistrements de journal entrants sont insérés dans la partition active la plus récente répondant à la règle de taille. Lorsque la partition atteint la taille maximale désignée, une nouvelle partition est créée pour l'insertion des nouveaux enregistrements de journal.
- Lorsque les partitions sont basées sur une date, les nouvelles partitions sont créées en fonction du cycle établi. Par exemple, dans le cas d'une option de remplacement mensuelle, une nouvelle partition est créée dès que des enregistrements sont reçus pour le nouveau mois. Les enregistrements de journal entrants sont insérés dans la partition appropriée en fonction de la date.

Les partitions de journalisation standard de la base de données présentent un avantage en termes de souplesse et de performances. Par exemple, vous pouvez générer des rapports à partir d'une seule partition pour limiter l'étendue des données devant être analysées pour localiser les informations demandées.

Tâches de la base de données

Les tâches de base de données suivantes sont installées en même temps que la base de données d'activité.

Important

Si vous utilisez la version complète de Microsoft SQL Server (pas Express), le service SQL Server Agent doit s'exécuter dans l'ordinateur du moteur de base de données. Assurez-vous que ce service soit configuré pour démarrer automatiquement au redémarrage de SQL Server ou de l'ordinateur.

- La **tâche d'extraction, de transformation et de chargement (ETL, Extract, Transform and Load)** s'exécute en permanence, en recevant les données de Log Server pour ensuite les traiter et les insérer dans la partition de journalisation standard. Lorsque la conservation des données de tendance est activée, la tâche ETL est également responsable de l'insertion des données de tendance dans la base de données du catalogue.

  La tâche ETL doit s'exécuter pour traiter les enregistrements de journal dans la base de données d'activité.
- La **tâche de maintenance de la base de données** exécute des travaux de maintenance et préserve les performances optimales. Par défaut, cette tâche s'exécute la nuit.
- La **tâche de temps de navigation Internet (IBT)** analyse les données reçues et calcule le temps de navigation pour chaque client. La tâche IBT consomme beaucoup de ressources et affecte la plupart des composants de la base de données. Par défaut, cette tâche s'exécute la nuit.

- Lorsque la conservation des données de tendance est activée, la tâche **trend** utilise les données de tendance quotidiennes créées par la tâche ETL pour actualiser les enregistrements de tendance hebdomadaires, mensuels et annuels à utiliser dans les rapports de présentation.

  Même lorsque la conservation des données de tendance est désactivée, la tâche des tendances traite les données issues de la partition des menaces (AMT) afin de fournir des données de tendance au tableau de bord Threats (Menaces).

  Cette tâche s'exécute la nuit.
- La tâche **ETL AMT (Advanced Malware Threat)** reçoit, traite et insère les données dans la partition des menaces. Seuls les enregistrements de journal incluant un niveau de gravité (voir *Affectation d'un niveau de gravité à une activité suspecte*, page 39) sont enregistrés dans la partition des menaces. Les données de cette partition servent à renseigner le tableau de bord Threats (Menaces) (voir *Tableau de bord Threats (Menaces)*, page 35).

Certains aspects de ces tâches de base de données peuvent être configurés dans la page Paramètres > Génération de rapports > Base de données d'activité. Pour plus d'informations, consultez la section *Paramètres d'administration de la base de données d'activité*, page 408.

Lorsque vous configurez l'heure de début des tâches de maintenance et de temps de navigation Internet, tenez compte des ressources système et du trafic réseau. Ces tâches consomment beaucoup de ressources et peuvent ralentir les performances de la journalisation et de la génération de rapports. Lorsque la conservation des données de tendance est activée, la tâche de tendance s'exécute par défaut à 4h30. Veiller à éviter de démarrer d'autres tâches aux mêmes heures que la tâche de tendance.

Paramètres d'administration de la base de données d'activité

La page **Paramètres > Génération de rapports > Base de données d'activité** permet de gérer les éléments suivants :

- Le moment, l'emplacement et le mode de création par la base de données d'activité des nouvelles partitions de journalisation standard et des partitions à utiliser pour la génération des rapports (*Configuration des options de partition de la base de données*, page 409)
- Le moment et le mode d'exécution des tâches de maintenance (voir *Configuration des options de maintenance de la base de données d'activité*, page 412)
- L'inclusion éventuelle de l'URL complète dans les enregistrements de journal, y compris du domaine et du chemin d'accès complet à la page ou à l'élément (voir *Configuration de la journalisation des URL*, page 413)
- Le mode de calcul du temps de navigation Internet (voir *Configuration des options du temps de navigation sur Internet*, page 414)
- Le stockage éventuel et la durée de stockage des données de tendance (voir *Configuration de la conservation des données de tendance*, page 416)

Le nom de l'instance de la base de données d'activité active s'affiche en haut de la page.

Configuration des options de partition de la base de données

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 408
- *Conseils sur le dimensionnement de la base de données d'activité*, page 417
- *Configuration des options du temps de navigation sur Internet*, page 414
- *Configuration de la journalisation des URL*, page 413
- *Configuration des options de maintenance de la base de données d'activité*, page 412
- *Configuration de la conservation des données de tendance*, page 416

La section **Database Rollover Configuration (Configuration du remplacement de la base de données)** de la page Paramètres > Génération de rapports > Base de données d'activité vous permet d'indiquer l'emplacement de stockage des partitions de cette base de données et de définir leur taille. Vous pouvez également créer de nouvelles partitions manuellement au lieu d'attendre le remplacement prévu et vérifier toutes les partitions disponibles pour la génération de rapports.

Reportez-vous au graphique **Growth Rates and Sizing (Taux de croissance et taille)** situé au bas de la section Database Rollover Configuration (Configuration du remplacement de la base de données) pour examiner l'évolution de la taille moyenne quotidienne de la partition dans le temps. Ces informations peuvent se révéler utiles pour planifier une future croissance, grâce à l'identification de la fréquence de création des nouvelles partitions et la définition des options de taille et de croissance de ces partitions.

- Servez-vous de la liste déroulante située au-dessous du graphique pour configurer la **période** affichée. (La période dépend de la date de création de la partition, pas des dates couvertes par cette dernière.) Vous pouvez afficher les partitions créées au cours de la dernière semaine, du dernier mois, des 3 derniers mois, des 6 derniers mois ou afficher toutes les partitions disponibles.

  Notez que, lorsque vous sélectionnez une période plus longue, chaque partition peut s'afficher sous la forme d'un petit point dans le graphique.
- Sélectionnez ou non l'option **Show chart legend (Afficher la légende du graphique)**. Lorsqu'elle est affichée, la légende désigne les partitions (par leur nom) qui apparaissent dans le graphique.

  La légende n'est disponible que si le graphique comprend au plus 20 partitions pour la période sélectionnée.
- Pour examiner le graphique avec plus de précision, sélectionnez une section. Cliquez sur **Zoom Out (Zoom arrière)** ou sur **Reset Chart (Réinitialiser le graphique)** pour réduire le niveau de détail.

Pour obtenir de l'aide sur la taille de la base de données, consultez la section *Conseils sur le dimensionnement de la base de données d'activité*, page 417.

Pour gérer le remplacement et la croissance de la base de données :

1. À côté de **Remplacer chaque**, définissez la fréquence de création désirée des nouvelles partitions.
   - Quel que soit le moteur de base de données pris en charge, vous pouvez saisir une limite de taille pour chaque partition. Lorsque cette limite de taille est atteinte, une nouvelle partition est créée.

     La limite de taille peut être définie comme suit :
     - *SQL Server Standard ou Enterprise* : 100 à 1 000 000 Mo, par défaut 5 000
     - *Microsoft SQL Server Express* : 100 à 8 000 Mo, par défaut 5 000

- Si vous utilisez Microsoft SQL Server Standard ou Enterprise, vous pouvez également définir un intervalle temporel de remplacement de partition (toutes les 1 à 52 semaines ou tous les 1 à 12 mois).

Remarque

Si le remplacement commence au cours de l'une des périodes de pointe de la journée, le processus peut ralentir les performances.

Pour contourner ce problème, certaines organisations définissent un remplacement automatique sur une longue période ou sur une taille maximale importante, puis effectuent des remplacements manuels pour éviter que le remplacement automatique ne se produise. Pour plus d'informations sur les remplacements manuels, consultez la section *Configuration des options de maintenance de la base de données d'activité*, page 412.

N'oubliez pas que les partitions individuelles très volumineuses ne sont pas conseillées. En effet, si les données ne sont pas divisées en plusieurs partitions plus petites, les performances de la génération de rapports peuvent diminuer.

Lors de la création d'une nouvelle partition de base de données, la génération de rapports est automatiquement activée pour cette partition.

2. Sous Partition Management (Gestion des partitions), définissez les informations suivantes :
   a. Entrez le **Chemin du fichier** permettant de créer des fichiers de **Données** et de **Journal** pour les nouvelles partitions de la base de données.
   b. Sous **Taille init**, définissez la taille initiale des fichiers de **Données** et de **Journal** composant les nouvelles partitions de la base de données.
      - *SQL Server Standard ou Enterprise* : la taille initiale du fichier de données va de 100 à 500 000 Mo (par défaut, 2 000). La taille initiale du fichier du journal va de 1 à 250 000 Mo (par défaut, 100).
      - *SQL Server Express* : la taille initiale du fichier de données va de 1 à 5 000 Mo (par défaut, 100). La taille initiale du fichier du journal va de 1 à 4 000 Mo (par défaut, 100).

Remarque

Il est recommandé de calculer la taille moyenne des partitions sur une certaine période, puis de mettre à jour la taille initiale en fonction de cette valeur. Vous pouvez par exemple définir la taille initiale sur 80 % de la taille moyenne. Cette approche réduit la fréquence des agrandissements de la partition et libère des ressources pour le traitement des données au sein des partitions.

Pour effectuer ce calcul, servez-vous des informations de la liste Growth Rates and Sizing (Taux de croissance et taille) (située au-dessous de la liste des partitions disponibles).

   c. Sous **Croissance**, définissez l'incrément par lequel la taille des fichiers de **Données** et de **Journal** d'une partition doit augmenter lorsque de l'espace supplémentaire est requis.
      - *SQL Server Standard ou Enterprise* : la croissance du fichier de données va de 100 à 500 000 Mo (par défaut, 500). La croissance du fichier du journal va de 1 à 250 000 Mo (par défaut, 100).
      - *SQL Server Express* : la croissance du fichier de données va de 1 à 1 000 Mo (par défaut, 100). La croissance du fichier du journal va de 1 à 1 000 Mo (par défaut, 100).

3. Si vous voulez créer une partition lors de la prochaine exécution de la tâche ETL (voir *Tâches de la base de données*, page 407) au lieu d'attendre le prochain remplacement automatique, cliquez sur **Manually Create Partition (Créer une partition manuellement)**. Ce processus prend généralement quelques minutes.
   - Pour que la nouvelle partition utilise les modifications apportées dans la page Base de données d'activité, cliquez sur **OK**, puis sur **Save and Deploy (Enregistrer et déployer)** avant de cliquer sur **Manually Create Partition (Créer une partition manuellement)**.
   - Cliquez régulièrement sur le lien Actualiser situé sous la liste des partitions disponibles. La nouvelle partition apparaît dans la liste à la fin du processus de création.
4. Servez-vous de la liste **Partitions disponibles** pour examiner les partitions disponibles pour la génération de rapports. La liste présente les dates couvertes, de même que la taille et le nom de chaque partition.

   Cochez la case accolée au nom d'une partition, puis servez-vous des boutons situés sous la liste pour indiquer si les données de cette partition sont inclues ou exclues des rapports, ou pour supprimer cette partition.
   - Cliquez sur **Activer** pour inclure les données d'une partition sélectionnée dans les rapports. Vous devez activer au moins une partition pour la génération des rapports.
   - Cliquez sur **Désactiver** pour exclure les données d'une partition sélectionnée des rapports.

     À elles deux, les options Activer et Désactiver vous permettent de gérer le volume de données analysées lors de la génération des rapports et la vitesse de traitement de ces derniers.
   - Pour supprimer une partition devenue inutile, cliquez sur **Supprimer**. La partition sera alors supprimée lors de la prochaine exécution de la tâche nocturne de maintenance de la base de données.

     Seules les partitions activées peuvent être supprimées. Pour supprimer une partition désactivée, commencez par l'activer, puis supprimez-la.

     Avertissement

     Servez-vous de cette option avec précaution, car les partitions supprimées ne peuvent pas être récupérées.

   La suppression des partitions obsolètes minimise le nombre de partitions présentes dans la base de données d'activité, ce qui améliore les performances de cette dernière et de la génération des rapports. Servez-vous aux besoins de l'option Supprimer pour effacer des partitions individuelles. Si vous préférez supprimer les anciennes partitions en fonction d'un planning défini, consultez la section *Configuration des options de maintenance de la base de données d'activité*, page 412.
5. 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)**.

Configuration des options de maintenance de la base de données d'activité

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 408
- *Configuration des options de partition de la base de données*, page 409
- *Configuration des options du temps de navigation sur Internet*, page 414
- *Configuration de la journalisation des URL*, page 413
- *Configuration de la conservation des données de tendance*, page 416

La section **Database Maintenance (Maintenance de la base de données)** de la page Paramètres > Génération de rapports > Base de données d'activité vous permet de contrôler la période d'exécution de la tâche de maintenance, la suppression automatique éventuelle des partitions et la fréquence de cette suppression, et la fréquence d'exécution des tâches telles que la réindexation des partitions et la suppression des messages d'erreur dans les journaux.

1. Pour **Heure de début de la maintenance**, sélectionnez l'heure d'exécution de la tâche de maintenance de la base de données (par défaut 01h00).

   Le temps et les ressources système requis pour cette tâche dépendent des travaux sélectionnés dans cette section. Pour minimiser l'impact sur les autres activités et systèmes, il est préférable d'exécuter cette tâche pendant l'une des périodes de faible activité du réseau, et pas en même temps que la tâche IBT (voir *Configuration des options du temps de navigation sur Internet*, page 414).

2. Pour supprimer définitivement les partitions en fonction de leur âge, sélectionnez **Automatically delete partitions when data is older than (Supprimer automatiquement les partitions lorsque les données sont antérieures à)**, puis définissez le nombre de jours (de 1 à 1 825) devant s'écouler avant leur suppression.

Avertissement

Lorsqu'une partition a été supprimée, ses données ne peuvent pas être récupérées. Consultez la section *Configuration des options de partition de la base de données*, page 409 pour découvrir une autre manière de supprimer des partitions.

3. Cochez l'option **Activer la réindexation automatique des partitions**, puis sélectionnez le jour où cette opération doit s'effectuer automatiquement chaque semaine (le samedi, par défaut).

   Ce processus de réindexation est important pour l'intégrité de la base de données et l'optimisation de la vitesse de création des rapports.

Important

Il est préférable d'exécuter cette opération au cours d'une période de faible activité du réseau. La réindexation des partitions de la base de données consomme beaucoup de ressources et prend un certain temps. Il est donc également préférable de ne pas exécuter de rapports pendant cette opération.

4. Sélectionnez **Process failed batches during the database maintenance job (Traiter les lots en échec pendant la tâche de maintenance de la base de données)** afin que la tâche nocturne de maintenance de la base de données traite à nouveau tous les lots en échec.

   Des échecs de lot se produisent lorsque l'espace disque est insuffisant ou lorsque les autorisations de la base de données ne permettent pas d'y insérer des enregistrements de journal. En général, ces lots sont ensuite retraités et insérés avec succès dans la base de données grâce à la tâche de maintenance nocturne. Ce nouveau traitement ne peut toutefois réussir si le problème d'espace disque ou d'autorisation n'a pas été résolu.

   Si cette option n'est pas activée, les lots ayant échoué ne sont jamais retraités, mais sont éventuellement supprimés lorsque le délai (ci-dessous) est écoulé.

5. Sélectionnez **Delete failed batches after (Supprimer les lots ayant échoué après)**, définissez le nombre de jours (de 0 à 90 ; 20, par défaut) devant s'écouler avant leur suppression.

   Si cette option n'est pas activée, les lots ayant échoué sont conservés indéfiniment en vue d'un traitement ultérieur.

6. Sélectionnez **Delete the error log after (Supprimer le journal d'erreurs après)**, puis définissez le nombre de jours (0 à 90 ; 60, par défaut) devant s'écouler avant que les enregistrements des erreurs de la base de données soient supprimés de la base de données du catalogue.

   Si cette option n'est pas activée, les journaux d'erreurs sont conservés indéfiniment.

7. 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)**.

Configuration de la journalisation des URL

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 408
- *Configuration des options de partition de la base de données*, page 409
- *Configuration des options du temps de navigation sur Internet*, page 414
- *Configuration des options de maintenance de la base de données d'activité*, page 412
- *Configuration de la conservation des données de tendance*, page 416

La section **Full URL Logging (Journalisation des URL complètes)** de la page Paramètres > Génération de rapports > Base de données d'activité vous permet de définir le nombre d'enregistrements possibles pour chaque URL demandée.

Remarque

La gestion de la taille de la base de données d'activité est essentielle pour les réseaux à fort trafic. La désactivation de l'option Journalisation des URL complètes est une manière de contrôler la taille et la croissance de la base de données.

1. Sélectionnez **Enregistrer le domaine et l'URL complète de chaque site demandé** pour journaliser l'URL complète, y compris le domaine (www.domaine.com) et le chemin d'accès de la page (/produits/produitA.html).

Important

Si vous prévoyez de créer des rapports sur l'activité d'analyse, activez la journalisation des URL complètes (voir *Génération de rapports sur l'activité d'analyse*, page 196). Sinon les rapports ne pourront afficher que le domaine (www.domaine.com) du site catégorisé, même si les pages individuelles d'un site appartiennent à des catégories différentes ou contiennent des menaces différentes.

Si cette option n'est pas activée, seuls les noms de domaine sont enregistrés. Il en résulte une base de données plus petite, mais moins de détails.

Si vous activez la journalisation des URL complètes alors que la consolidation est activée, l'enregistrement consolidé contient l'URL complète du premier enregistrement du groupe consolidé. Pour plus d'informations, consultez la section *Configuration de Log Server*, page 400.

2. 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)**.

Configuration des options du temps de navigation sur Internet

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 408
- *Configuration des options de partition de la base de données*, page 409
- *Configuration de la journalisation des URL*, page 413
- *Configuration des options de maintenance de la base de données d'activité*, page 412
- *Configuration de la conservation des données de tendance*, page 416

Les rapports du Temps de navigation sur Internet (IBT) donnent un aperçu du temps passé par les utilisateurs sur Internet. Une tâche de base de données exécutée pendant la nuit calcule le temps de navigation de chaque client sur la base des nouveaux enregistrements de journal reçus au cours de la journée. Définissez les options de temps de navigation dans la section **Configuration du temps de navigation sur Internet** de la page Paramètres > Génération de rapports > Base de données d'activité.

1. Choisissez l'**Heure de début de la tâche IBT** pour la base de données IBT.

   Le temps et les ressources système requis pour cette tâche dépendent du volume de données enregistrées chaque jour. Il est préférable de ne pas exécuter cette tâche en même temps que la tâche de maintenance nocturne (voir *Configuration des options de maintenance de la base de données d'activité*, page 412) et de choisir un moment de faible activité du réseau afin de minimiser l'impact sur la génération des rapports.

   La tâche de base de données IBT peut consommer beaucoup de ressources et affecte la plupart des composants de la base de données. Si vous l'activez, définissez son heure de début de manière à ne pas interférer avec les capacités du système de la base de données à traiter les rapports planifiés et d'autres opérations importantes. De même, surveillez cette tâche afin de déterminer si un matériel plus robuste permettrait de mieux répondre à l'ensemble des besoins du traitement.

2. Pour **Average browse time per site (Temps moyen de navigation par site)**, définissez un nombre moyen de minutes de lecture du contenu d'une page Web.

   Ce nombre définit les sessions de navigation en vue des rapports sur le temps de navigation Internet. L'ouverture d'un navigateur génère du trafic HTTP. Cela représente le début d'une session de navigation. La session reste ouverte tant que du trafic HTTP est généré de façon continue au cours de l'intervalle de temps défini ici. La session de navigation est considérée comme fermée dès que ce délai s'écoule sans trafic HTTP. Une nouvelle session de navigation commence dès que du trafic HTTP est à nouveau généré.

   > **Remarque**
   >
   > Il est préférable de ne modifier le paramètre de temps moyen de navigation par site qu'aussi rarement que possible et de créer une nouvelle partition de base de données chaque fois que vous le modifiez.
   >
   > Pour ne pas obtenir d'incohérences dans les rapports, générez les rapports IBT à partir de partitions utilisant la même valeur de temps moyen de navigation par site.

   N'oubliez pas que certains sites Web utilisent l'actualisation automatique pour fréquemment mettre leur contenu à jour. Un site d'actualités qui rajoute régulièrement les dernières infos à l'affichage en est un exemple. Cette actualisation génère du nouveau trafic HTTP. De ce fait, lorsque ce type de site reste ouvert, de nouveaux enregistrements de journal sont générés à chaque actualisation du site. Le trafic HTTP ne s'interrompt pas suffisamment longtemps pour que la session de navigation se ferme.

3. Définissez une valeur **Browse time for last site read (Temps de navigation pour la lecture du dernier site)** pour connaître le temps passé à lire le dernier site avant la fin d'une session de navigation.

   Lorsque le délai d'inactivité du trafic HTTP est supérieur au seuil du temps moyen de navigation « par site », la session est interrompue et la valeur du temps de navigation de « lecture du dernier site » est ajoutée au temps de session.

4. Pour activer les rapports détaillés incluant le temps de navigation liés aux rapports d'investigation, cochez la case **Calculer le temps de navigation détaillé pour les rapports d'investigation détaillés**.

   > **Important**
   >
   > L'activation des calculs détaillés du temps de navigation augmente la taille de la Base de données d'activité et peut également affecter ses performances. Lorsque vous utilisez cette option, surveillez attentivement la croissance de la base de données d'activité et les performances globales de la génération des rapports.

   Lorsque le temps de navigation détaillé est désactivé, la tâche IBT poursuit les calculs servant à inclure le temps de navigation dans les rapports récapitulatifs.

5. 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)**.

Configuration de la conservation des données de tendance

Rubriques connexes :

- *Paramètres d'administration de la base de données d'activité*, page 408
- *Configuration des options de partition de la base de données*, page 409
- *Configuration de la journalisation des URL*, page 413
- *Configuration des options de maintenance de la base de données d'activité*, page 412
- *Configuration des options du temps de navigation sur Internet*, page 414

La base de données d'activité peut éventuellement stocker les données des tendances de l'activité Internet pour les exploiter dans les rapports de présentation. Lorsque les rapports des tendances sont activés, la tâche de base de données ETL (voir *Tâches de la base de données*, page 407) ajoute les données de tendances quotidiennes dans la base de données du catalogue et la tâche de tendance s'exécute chaque nuit pour stocker les informations hebdomadaires, mensuelles et annuelles sur les tendances.

La section **Trend Data Retention (Conservation des données de tendances)** de la page Paramètres > Génération de rapports > Base de données d'activité vous permet de définir la durée de conservation des données de tendance dans la base de données d'activité.

1. Cochez la case **Store trend data (Stocker les données de tendance)** pour demander à la tâche ETL de stocker les données des tendances et pour activer la tâche de tendances nocturne.

   Les données de tendance ne sont calculées que pour les données collectées lorsque cette option est activée.

   Les données stockées dans la base de données avant l'activation de la conservation des données de tendance et les données collectées après la désactivation de cette option ne peuvent pas être incluses dans les rapports de tendances.

   Lorsque cette option est désactivée, la tâche de base de données des tendances s'exécute uniquement pour traiter les données liées aux menaces dans la partition AMT.
2. Définissez la durée de conservation des données de tendances hebdomadaires, mensuelles et annuelles. Notez que le fait d'augmenter la durée de stockage des données de tendances accroît la taille de la base de données d'activité (voir *Conseils sur le dimensionnement de la base de données d'activité*, page 417).

   Remarque

   Les données de tendances étant stockées dans la base de données du catalogue et non dans la base de données des partitions, leurs périodes de stockage ne dépendent pas de la durée de conservation des partitions.

   Les périodes de stockage par défaut des données de tendances sont les suivantes :

	SQL Server	SQL Server Express
Daily (Quotidien)	90 jours	60 jours
Weekly (Hebdomadaire)	26 semaines	13 semaines
Monthly (Mensuel)	18 mois	6 mois
Yearly (Annuel)	5 ans	3 ans

La tâche de tendance nocturne purge les données antérieures à la période de conservation définie.

3. 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)**.

Conseils sur le dimensionnement de la base de données d'activité

Rubriques connexes :

- *Configuration des options de partition de la base de données*, page 409
- *Configuration du mode de journalisation des requêtes filtrées*, page 398
- *Configuration de la journalisation des URL*, page 413

Il est difficile de prévoir avec précision la taille de la base de données d'activité, car elle dépend d'un certain nombre de facteurs, notamment du nombre d'utilisateurs filtrés et de demandes moyennes par seconde. Par ailleurs, la taille varie également selon si la base de données d'activité est configurée ou non pour :

- Enregistrer les accès ou les visites associés à chaque requête Web (voir *Configuration de Log Server*, page 400)

  Enregistrer les accès garantit un haut niveau de détail, mais enregistrer les visites peut réduire la taille de la base de données de 40 % environ.

- Consolider les enregistrements de journal (voir *Configuration de Log Server*, page 400)

  Par défaut, toutes les requêtes sont enregistrées en tant que visites ou accès distincts. Lorsque vous activez la consolidation, les requêtes similaires (accès, par le même utilisateur, aux sites du même domaine, et auxquels la même action de filtrage s'applique) effectuées au cours d'une période définie sont journalisées sous forme d'enregistrement de journal unique. Ce fonctionnement permet de réduire la taille de la base de données d'activité de 60 % environ.

- Stocker l'URL complète de chaque requête journalisée (voir *Configuration de la journalisation des URL*, page 413)

  L'enregistrement des URL complètes permet d'obtenir des informations précises sur les sites visités par un utilisateur, mais fait plus que doubler la taille de la base de données d'activité.

- Enregistrer lesrequêtes de toutes les catégories (voir *Configuration du mode de journalisation des requêtes filtrées*, page 398)

  Par défaut, les demandes de sites sont enregistrées pour toutes les catégories. Pour réduire la taille de la base de données d'activité, vous pouvez ne pas enregistrer les sites appartenant à des catégories qui, par exemple, ne présentent pas de risque de sécurité ou de responsabilité légale pour votre organisation.

  L'impact de cette modification dépend du nombre de catégories non enregistrées et de la fréquence à laquelle les utilisateurs demandent des sites appartenant à ces catégories.

- Effectuer des calculs de temps de navigation détaillés (voir *Configuration des options du temps de navigation sur Internet*, page 414)

  Pour créer des rapports d'investigation détaillés incluant le temps de navigation, la tâche IBT doit calculer en détail ce temps de navigation. Stocker les données de temps de navigation détaillés augmente toutefois la taille de la base de données et peut également affecter ses performances.

- Stocker les données de tendances (voir *Configuration de la conservation des données de tendance*, page 416)

  Stocker les données de tendances permet de générer des rapports sur les tendances de l'activité Internet des utilisateurs tout au long d'une journée, d'une semaine ou d'une période plus longue mais, en parallèle, accroît la taille de la base de données d'activité. Plus la période de stockage des données est longue, plus la taille de la base de données est affectée.

Pour surveiller la taille moyenne quotidienne de vos partitions de journalisation standard actives et inactives, servez-vous du graphique **Growth Rates and Sizing (Taux de croissance et taille)** de la page Paramètres > Génération de rapports > Base de données d'activité. Ces informations vous aideront à identifier les tendances du volume de trafic dans le temps et vous permettront de mieux prévoir la croissance future.

À mesure que vous collectez des informations sur la taille moyenne, ajustez vos paramètres de remplacement **Taille initiale** et **Croissance** (via la section Partition Management (Gestion des partitions) de la page Paramètres > Génération de rapports > Base de données d'activité).

La meilleure pratique consiste à définir la valeur Taille initiale sur 80 % environ de la **taille moyenne des partitions** au cours de la période de remplacement (semaine, mois, etc.). Cette approche vise à :

- Réduire la fréquence de croissance de la partition
- Libérer des ressources pour le traitement des données au sein des partitions
- Éviter toute affectation d'espace disque inutile lors de la création de la partition

  Les parties inutilisées de l'espace initialement attribué à une partition ne peuvent pas être récupérées tant que la partition n'a pas été supprimée.

Configuration des rapports du tableau de bord

La page **Paramètres > Génération de rapports > Tableau de bord** vous permet de configurer la période maximale d'affichage des éléments dans les tableaux de bord Threats (Menaces), Risques, Usage et Système.

Si vous utilisez Websense Web Security Gateway ou Gateway Anywhere, choisissez éventuellement aussi de créer un référentiel d'analyse pour stocker les données sur les fichiers liés à l'activité malveillante détectée au sein de votre réseau.

Configuration de la période maximale des graphiques du tableau de bord

Par défaut, les graphiques, compteurs et tableaux de tous les onglets de la page État > Tableau de bord présentent au maximum **30 jours** de données. Cette limite a été établie afin de réduire le temps nécessaire pour charger le Tableau de bord, optimiser les performances globales de TRITON - Web Security et réduire la charge de travail de la base de données d'activité.

Si vous utilisez les versions Standard et Enterprise de Microsoft SQL Server, vous pouvez configurer les graphiques des tableaux de bord sur une période plus longue. Étendre la période maximale peut toutefois affecter fortement les performances de TRITON - Web Security et de la base de données d'activité.

- Pour modifier la période maximale disponible dans les graphiques des tableaux de bord Risques, Usage et Système, sous General Dashboard Data (Données générales des tableaux de bord), sélectionnez une valeur dans la liste déroulante **Show a maximum of (Afficher un maximum de)**.
  - Étendre la période n'affecte pas la taille de la base de données d'activité, mais accroît le temps nécessaire pour l'interroger, récupérer les informations et actualiser les graphiques des tableaux de bord.
  - Si vous utilisez Microsoft SQL Server Express, la période maximale est de 30 jours et n'est pas modifiable.
- Pour modifier la période maximale disponible dans le tableau de bord Threats (Menaces) et la page Event Details (Détails de l'événement), sous Threats Data (Données sur les menaces), sélectionnez une valeur dans la liste déroulante **Keep Threats data for (Conserver les données du tableau de bord Menaces pendant)**.
  - Les données détaillées du tableau de bord Threats (Menaces) n'étant pas stockées dans la même partition que les données de journalisation standard, étendre la période augmente également la taille de la base de données d'activité.
  - Lorsque le stockage des données d'analyse associées aux menaces est activé (voir ci-dessous), le référentiel d'analyse tente de stocker les données pour la période sélectionnée ici. Toutefois, lorsque la taille maximale du référentiel est atteinte, les anciens enregistrements sont automatiquement supprimés pour faire de la place pour les nouveaux enregistrements.
  - Si vous utilisez Microsoft SQL Server Express, la période maximale est de 30 jours et n'est pas modifiable.

Notez que les données ne sont pas toujours disponibles pour toute la période sélectionnée. Si votre solution Websense Web Security n'a été installée que 7 jours auparavant, par exemple, les rapports générés sur 30 jours présentent uniquement les données des 7 jours pendant lequel le filtrage a été effectué.

Exemple de données du tableau de bord Threats (Menaces)

Pour obtenir quelques exemples des types de données pouvant s'afficher dans le tableau de bord Threats (Menaces) sans générer de trafic réseau potentiellement dangereux, vous pouvez importer des échantillons de données.

Ces échantillons étant chargés dans la base de données d'activité, puis combinés aux véritables données générées au sein de votre réseau, il est préférable de ne les charger que dans un environnement de test ou d'évaluation.

Pour désigner clairement ces échantillons de données, le nom intermédiaire **Démo** (par exemple, Sam Démo Smith et Lisa Démo Brady) est attribué à chacun des utilisateurs de la base de données des échantillons. Par ailleurs, l'horodatage de l'activité des utilisateurs est antérieur à la création de la partition de la base de données d'activité contenant les données.

Pour charger ces échantillon dans la base de données, cliquez sur **Sample Data (Échantillon de données)**, puis cliquez sur **Import Sample Data (Importer les échantillons de données)**. Lorsque vous cliquez sur **OK**, puis sur **Save and Deploy (Enregistrer et déployer)**, les données sont chargées dans la base de données d'activité. Quelques secondes plus tard, le tableau de bord Threats (Menaces) est actualisé et présente les nouvelles données.

Configuration du stockage des données d'analyse

Dans les déploiements Websense Web Security Gateway et Gateway Anywhere, les données d'analyse liées aux menaces peuvent inclure :

- Des informations sur la source (adresse IP, nom du périphérique et utilisateur) qui tente d'envoyer des données
- Des informations sur la cible (adresse IP, URL et emplacement géographique) à laquelle les données sont envoyées
- Les informations d'en-tête associées à la tentative d'envoi des données
- Une copie des véritables données envoyées (par exemple, sous forme de fichier texte, de feuille de calcul, de fichier ZIP)

Si vous activez le stockage des données d'analyse, définissez également l'emplacement de stockage du **référentiel d'analyse** (base de données spécialisée), la taille maximale que cette base de données peut atteindre et la durée de stockage de ces données.

1. Sous Incident Data for Forensic Investigation (Données des incidents pour analyse), cochez la case **Store forensic data about Threats incidents for further investigation (Stocker les données d'analyse liées aux incidents associés aux menaces pour analyse ultérieure)** pour créer le référentiel d'analyse.

   Si votre déploiement comprend une solution Websense Data Security, ce nouveau référentiel d'analyse est similaire à celui de Data Security. Plus petit, le référentiel Web Security stocke uniquement des informations sur les incidents affichés dans le tableau de bord Threats (Menaces).
2. Choisissez ensuite de stocker des détails d'analyse pour les **Requêtes bloquées uniquement** ou pour **Toutes les requêtes** (bloquées et autorisées).
3. Définissez le **Chemin d'accès** de l'emplacement de stockage du référentiel d'analyse.
   - Ce répertoire doit déjà exister.
   - Le chemin d'accès peut être local (dans le serveur de gestion TRITON) ou distant.
   - Assurez-vous que l'emplacement sélectionné pour ce référentiel dispose de suffisamment d'espace libre pour pouvoir atteindre la taille maximale définie (ci-dessous).
4. Fournissez les identifiants de connexion d'un compte disposant d'autorisations en lecture, écriture et suppression sur le répertoire du référentiel d'analyse.
   - Sélectionnez **Use Local System account (Utiliser le compte Système local)** lorsque aucune autorisation spéciale ni accès au réseau n'est nécessaire pour accéder à ce répertoire.
   - Sélectionnez **Utiliser ce compte** pour utiliser un compte de domaine, puis saisissez le **Nom d'utilisateur**, le **Mot de passe** et le **Domaine** de ce compte.

   Cliquez sur **Tester la connexion** pour vérifier que le comte sélectionné peut accéder au référentiel d'analyse.
5. Pour définir la taille maximale que le référentiel d'analyse peut atteindre, saisissez la **Taille maximale** en Go (par défaut, 20) du référentiel d'analyse.
   - Si vous utilisez SQL Server Express, cette valeur n'est pas modifiable.
   - Lorsque la taille maximale est atteinte **ou** lorsque les enregistrements atteignent la limite d'âge définie pour les données du tableau de bord Threats (Menaces), les enregistrements sont automatiquement purgés du référentiel.
6. 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)**.

Configuration des rapports d'investigation

Rubriques connexes :

- *Connexion à la base de données et paramètres par défaut des rapports*, page 421
- *Options d'affichage et de sortie*, page 423

Les rapports d'investigation vous permettent de rechercher des informations sur l'utilisation Internet dans votre organisation de façon interactive. Voir *Rapports d'investigation*, page 152.

Le lien Options de la page principale des rapports d'investigation permet de choisir quelle base de données d'activité est utilisée pour la génération des rapports. Il permet également de modifier l'affichage par défaut des rapports détaillés. Voir *Connexion à la base de données et paramètres par défaut des rapports*, page 421.

Le fichier **wse.ini** permet de configurer certains paramètres par défaut liés à l'affichage des rapports récapitulatifs et des rapports multi-niveaux. Il permet également de mieux contrôler la taille par défaut des pages utilisées lors de la publication d'un rapport au format PDF. Voir *Options d'affichage et de sortie*, page 423.

Connexion à la base de données et paramètres par défaut des rapports

Rubriques connexes :

- *Configuration des rapports d'investigation*, page 421
- *Options d'affichage et de sortie*, page 423
- *Rapports récapitulatifs*, page 154
- *Rapports récapitulatifs multi-niveaux*, page 158

Utilisez la page **Rapports d'investigation > Options** pour vous connecter à la base de données d'activité désirée et contrôler les paramètres par défaut de l'affichage détaillé des rapports d'investigation.

Les modifications apportées dans cette page affectent vos rapports. Les autres administrateurs, de même que les utilisateurs enregistrés pour la journalisation de leur activité propre, peuvent modifier ces valeurs pour leurs propres activités de génération de rapports.

1. Choisissez la base de données d'activité à utiliser pour les rapports d'investigation.
   - Cochez la case **Afficher la base de données de catalogue** pour vous connecter à la base de données d'activité au sein de laquelle Log Server effectue la journalisation. Passez à l'étape 2.
   - Pour accéder à une autre base de données d'activité, désactivez l'option **Afficher la base de données de catalogue**, puis saisissez les informations suivantes :

Champ	Description
Serveur	Entrez le nom ou l'adresse IP de l'ordinateur dans lequel la base de données d'activité est stockée. Si votre environnement utilise la mise en cluster de SQL Server, entrez l'adresse IP virtuelle du cluster.

Champ	Description
Base de données	Entrez le nom de la base de données d'activité.
ID utilisateur	Entrez l'ID utilisateur d'un compte autorisé à accéder à la base de données. Ne renseignez pas ce champ si Log Server a été configuré pour utiliser une connexion sécurisée pour accéder à la base de données d'activité.
Mot de passe	Entrez le mot de passe du compte spécifié. Dans le cas d'une connexion approuvée, ne renseignez pas ce champ.

2. Sélectionnez les paramètres par défaut suivants pour les rapports détaillés.

Champ	Description
Sélectionnez la plage de dates par défaut des rapports d'investigation.	Choisissez la plage de dates pour l'affichage initial des rapports récapitulatifs.
Sélectionnez le format de rapport détaillé par défaut.	Choisissez **Sélection intelligente de colonnes** pour afficher les rapports détaillés avec ses colonnes par défaut définies pour les informations rapportées. Choisissez **Sélection personnalisée de colonnes** pour définir avec précision les colonnes de l'affichage initial dans tous les rapports détaillés. Servez-vous de la liste Colonnes disponibles pour effectuer vos sélections. Les utilisateurs pourront modifier les colonnes affichées après avoir généré le rapport.
Type de rapport	Indiquez si les rapports détaillés doivent initialement présenter : • **Détail** : chaque enregistrement s'affiche sur une ligne distincte ; l'heure peut être affichée. • **Résumé** : regroupe en une seule entrée tous les enregistrements qui partagent un élément commun. L'élément spécifique varie en fonction des informations utilisées dans le rapport. En général, la colonne située immédiatement à droite avant la mesure présente l'élément résumé. L'heure ne peut pas être affichée.
Colonnes disponibles / Rapport en cours	Sélectionnez un nom de colonne dans la liste Colonnes disponibles et cliquez sur la flèche appropriée pour le déplacer vers la liste Rapport en cours. La liste Rapport en cours peut contenir jusqu'à 7 colonnes. Une fois que la liste Rapport en cours contient toutes les colonnes des rapports détaillés initiaux, définissez l'ordre des colonnes. Sélectionnez une entrée dans la liste et utilisez les boutons vers le haut et vers le bas pour modifier sa position.

3. Cliquez sur **Enregistrer les options** pour enregistrer immédiatement toutes les modifications.

Options d'affichage et de sortie

Rubriques connexes :

- *Configuration des rapports d'investigation*, page 421
- *Connexion à la base de données et paramètres par défaut des rapports*, page 421
- *Sortie dans un fichier*, page 176

Vous pouvez ajuster la manière dont certains choix et résultats de rapports apparaissent dans les rapports d'investigation récapitulatifs et multi-niveaux. Vous pouvez également spécifier la taille par défaut des pages lorsque les rapports sont publiés au format PDF.

Ces options de configuration des rapports d'investigation sont définies dans le fichier **wse.ini** (situé par défaut dans le répertoire C:\Program Files *ou* Program Files (x86)\Websense\Web Security\webroot\Explorer\).

Le tableau suivant présente la liste des paramètres qui affectent l'affichage et la sortie des rapports d'investigation, ce qu'ils contrôlent et leur valeur par défaut. (Ne modifiez AUCUN autre paramètre du fichier wse.ini.)

Paramètre	Description
maxUsersMenu	La base de données doit comprendre moins d'utilisateurs que cette valeur (par défaut, 5 000) pour afficher Utilisateur en tant que choix de rapport dans la liste Utilisation d'Internet par.
maxGroupsMenu	La base de données doit comprendre moins de groupes que cette valeur (par défaut, 3 000) pour afficher Groupe en tant que choix de rapport dans la liste Utilisation d'Internet par. **Remarque :** pour que Groupe apparaisse dans la liste Utilisation d'Internet par, plusieurs groupes doivent exister. De même, pour que Domaine apparaisse dans la liste Utilisation d'Internet par, plusieurs domaines doivent exister. Il n'existe pas de valeur maximale pour les domaines.
maxUsersDrilldown	Ce paramètre fonctionne avec le paramètre warnTooManyHits pour contrôler les moments où l'option Utilisateur doit s'afficher en rouge. L'affichage en rouge indique que le choix de l'option Utilisateur entraîne la production d'un rapport très volumineux dont l'exécution peut être longue. Si le nombre d'utilisateurs est supérieur à cette valeur (par défaut, 5 000), et le nombre d'accès supérieur à la valeur warnTooManyHits, l'option Utilisateur s'affiche en rouge dans les différentes listes déroulantes et de valeurs. Si le nombre d'utilisateurs est supérieur à cette valeur mais que le nombre d'accès est inférieur à la valeur warnTooManyHits, l'option Utilisateur s'affiche dans sa couleur habituelle, le rapport produit étant de taille plus raisonnable.
maxGroupsDrilldown	L'option Groupe s'affiche en rouge pendant l'exploration verticale si le nombre de groupes est supérieur à ce nombre dans le rapport proposé (par défaut, 2 000). L'affichage en rouge indique que le choix de l'option Groupe entraîne la production d'un rapport très volumineux dont l'exécution peut être longue.

Paramètre	Description
warnTooManyHits	Ce paramètre fonctionne avec le paramètre maxUsersDrilldown pour contrôler le moment où l'option Utilisateur doit s'afficher en rouge. Si le nombre d'utilisateurs est supérieur à la valeur maxUsersDrilldown, mais que le nombre d'accès est inférieur à cette valeur (par défaut, 10 000), l'option Utilisateur ne s'affiche *pas* en rouge. Si le nombre d'utilisateurs est supérieur à la valeur maxUsersDrilldown et que le nombre d'accès est supérieur à cette valeur, l'option Utilisateur s'affiche en rouge. L'affichage en rouge indique que le choix de l'option Utilisateur entraîne la production d'un rapport très volumineux dont l'exécution peut être longue.
hitsPerPage	Ce paramètre détermine le nombre maximal d'éléments (par défaut, 100) affichés par page. (Ce paramètre n'affecte pas les rapports imprimés.)
maxOutputBufferSize	Ce paramètre correspond à la quantité maximale de données (en octets) pouvant être affichée sur la page principale des rapports d'investigation. Si les données demandées dépassent cette limite (par défaut 4 000 000, ou 4 millions d'octets), un message apparaît en rouge à la fin du rapport pour indiquer que certains résultats ne sont pas affichés. Si cela pose un problème, des valeurs supérieures permettent d'afficher une plus grande quantité de données dans un rapport. Toutefois, si des erreurs de mémoire surviennent, pensez à réduire cette valeur.
sendMulti	Cette option est désactivée (0) par défaut. Définissez-la sur 1 (activée) pour diviser les très grands rapports détaillés planifiés en plusieurs fichiers de 10 000 lignes chacun. Les fichiers représentant un même rapport sont compressés et envoyés aux destinataires par courrier électronique. Les fichiers du rapport peuvent ensuite être extraits avec des utilitaires de compression courants.
maxSlices	Ce paramètre correspond au nombre maximal de secteurs distincts (par défaut, 6) d'un graphique en secteurs, y compris le secteur Autre, qui combine toutes les valeurs non représentées dans les secteurs individuels.
timelineCompressionThreshold	Cette option est utilisée uniquement pour l'Activité utilisateur par jour ou par mois, lorsque l'option 'Regrouper les accès similaires/Afficher tous les accès' est disponible. Le rapport réduit tous les accès de la même catégorie survenant au cours du nombre de secondes définies ici (par défaut, 10).
PageSize	Pour simplifier la diffusion ou l'impression, les rapports d'investigation peuvent être publiés au format PDF (Portable Document Format). La taille des pages (par défaut, Lettre) peut être : • A4 (21,59 x 27,49 cm) • Lettre (21,59 x 27,94 cm)

Rapports sur activité propre

Rubriques connexes :

- *Configuration des préférences de génération de rapports*, page 397
- *Rapports sur activité propre*, page 177
- *Rapports d'investigation*, page 152

Vous pouvez activer cette fonction pour permettre aux utilisateurs d'afficher des rapports d'investigation sur leur propre activité Internet. Cela leur permet de voir quels types d'informations sont collectés à leur propos, afin de respecter la législation en vigueur dans la plupart des pays. De plus, l'affichage de leur propre activité peut encourager certains utilisateurs à modifier leurs habitudes de navigation afin de respecter la politique Internet de leur organisation.

Pour activer la fonction de rapport sur activité propre :

1. Ouvrez la page **Paramètres** > **Général** > **Services d'annuaire** et configurez le service d'annuaire utilisé pour authentifier les utilisateurs qui accèdent à TRITON - Web Security avec leurs identifiants réseau. Il est possible que cette opération ait déjà été effectuée précédemment pour activer le filtrage par noms d'utilisateur et de groupe. Voir *Services d'annuaire*, page 75.
2. Ouvrez la page **Paramètres** > **Génération de rapports** > **Préférences** et cochez la case **Permettre aux utilisateurs de générer des rapports sur leur propre activité**. Voir *Configuration des préférences de génération de rapports*, page 397.

Après avoir activé cette option, assurez-vous de fournir aux utilisateurs les informations dont ils ont besoin pour exécuter ces rapports :

- L'URL permettant d'accéder à l'interface de rapport sur activité propre :

  ```
  https://<adresse_IP>:9443/mng/login/pages/
  selfReportingLogin.jsf
  ```

  Remplacez <adresse_IP> par l'adresse IP de l'ordinateur TRITON - Web Security.

  Rappelez aux utilisateurs qu'ils peuvent enregistrer cette URL sous forme de favori ou de signet en vue d'une utilisation future.

  Les administrateurs et les utilisateurs peuvent également accéder à la page de connexion des rapports sur activité propre en ouvrant la page de connexion de TRITON - Web Security et en cliquant sur le lien Rapports sur activité propre.

- Le nom d'utilisateur et le mot de passe à utiliser pour la connexion

  Les utilisateurs du rapport sur activité propre doivent saisir leur nom d'utilisateur et leur mot de passe réseau lors de leur connexion.

18 Configuration du réseau

Rubriques connexes :

- *Configuration de Network Agent*, page 428
- *Vérification de la configuration de Network Agent*, page 435

Lorsque vous exécutez Websense Web Security ou Websense Web Filter en mode autonome (sans intégration à un proxy ou un pare-feu), Websense Network Agent permet d'effectuer les opérations suivantes :

- Filtrage du contenu Internet
- Gestion des protocoles réseau et des applications Internet
- Gestion de la bande passante
- Journalisation du volume d'octets transféré

Dans un déploiement intégré de Websense, un produit tiers (passerelle, pare-feu ou cache) peut gérer l'acheminement des requêtes des utilisateurs vers Websense pour le filtrage et le renvoi des pages de blocage vers les clients. Dans cet environnement, Network Agent peut tout de même être utilisé pour filtrer les requêtes non HTTP, fournir plus de détails sur la journalisation ou les deux.

En outre, Websense Web Security Gateway peut détecter les protocoles avec mise en tunnel sur HTTP (voir *Détection des protocoles mis en tunnel*, page 186) et fournir certaines capacités de gestion de la bande passante (voir *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270), indépendamment de Network Agent.

Network Agent surveille en permanence l'utilisation globale du réseau, y compris les octets transférés via le réseau. L'agent envoie des résumés d'utilisation à Websense à intervalles prédéfinis. Chaque résumé comprend l'heure de début et de fin, le total d'octets transférés et les octets utilisés par protocole.

Par défaut, Network Agent fournit également des données sur l'utilisation de la bande passante à Policy Server et les données sur la journalisation du filtrage à Filtering Service.

Network Agent est généralement configuré de manière à voir tout le trafic de votre réseau. Il distingue :

- Les requêtes envoyées par des ordinateurs internes à des ordinateurs internes (accès à un serveur intranet, par exemple)
- Les requêtes envoyées par des ordinateurs internes à des ordinateurs externes tels que des serveurs Web (requêtes Internet d'utilisateur, par exemple)

Ces dernières constituent le principal problème dans la surveillance de l'utilisation Internet par les employés.

Configuration de Network Agent

Rubriques connexes :

- *Configuration des paramètres globaux*, page 428
- *Configuration des paramètres locaux*, page 430
- *Configuration des paramètres des cartes réseau*, page 431
- *Ajout ou modification des adresses IP*, page 434

Après l'installation de Network Agent, utilisez TRITON - Web Security afin de configurer son comportement pour la surveillance de votre réseau. Les paramètres de Network Agent sont répartis dans deux sections principales :

- Les **Paramètres globaux** affectent toutes les instances de Network Agent. Utilisez-les pour :
  - Identifier les ordinateurs de votre réseau
  - Dresser la liste des ordinateurs de votre réseau dont Network Agent doit surveiller les requêtes **entrantes** (par exemple les serveurs Web internes)
  - Définir le calcul de la bande passante et le comportement de la journalisation des protocoles
- Les **Paramètres locaux** ne s'appliquent qu'à l'instance de Network Agent sélectionnée. Utilisez-les pour :
  - Identifier l'instance de Filtering Service associée à chaque Network Agent
  - Noter les proxy et les caches utilisés par les ordinateurs surveillés par cette instance de Network Agent
  - Configurer l'utilisation de chaque carte réseau de l'ordinateur Network Agent (pour surveiller les requêtes, envoyer les pages de blocage, ou les deux)

    Les paramètres des cartes réseau déterminent également quel segment du réseau est surveillé par chaque instance de Network Agent.

Configuration des paramètres globaux

Rubriques connexes :

- *Configuration des paramètres locaux*, page 430
- *Configuration des paramètres des cartes réseau*, page 431
- *Ajout ou modification des adresses IP*, page 434

La page **Paramètres > Network Agent > Global** permet de définir le comportement de base pour la surveillance et la journalisation de toutes les instances de Network Agent.

La liste **Describe Your Network (Décrire votre réseau)** identifie les adresses IP qui composent votre réseau au format IPv4 ou IPv6. Par défaut, Network Agent ne surveille pas le trafic (communications réseau internes) circulant entre ces adresses IP.

Network Agent n'utilise pas cette liste pour désigner les adresses IP à surveiller pour les requêtes Internet. Ce comportement est configuré séparément pour chaque carte réseau de Network Agent (voir *Configuration des paramètres des cartes réseau*, page 431). Cette liste sert uniquement à exclure le trafic interne (connexions LAN et intranet) de la surveillance.

Un jeu d'entrées initial est fourni par défaut. Vous pouvez ajouter d'autres entrées, ou modifier ou supprimer des entrées existantes.

La liste **Trafic interne à surveiller** comprend toutes les adresses IPv4 ou IPv6 internes (comprises dans la liste Décrire votre réseau) dont Network Agent **doit** surveiller le trafic. Elle peut par exemple inclure des serveurs Web internes pour vous aider à effectuer le suivi des connexions internes.

Toutes les requêtes envoyées depuis le réseau vers les ordinateurs internes spécifiés sont surveillées. Par défaut, cette liste est vide.

- Cliquez sur **Ajouter** pour ajouter une adresse IP ou une plage d'adresses IP dans la liste appropriée. Les deux formats IPv4 et IPv6 sont pris en charge. Pour plus d'informations, consultez la section *Ajout ou modification des adresses IP*, page 434.
- Pour modifier une plage ou une adresse IP de la liste, cliquez sur son entrée. Pour plus d'informations, consultez la section *Ajout ou modification des adresses IP*, page 434.
- Pour retirer une entrée de la liste, cochez la case accolée à la plage ou à l'adresse IP, puis cliquez sur **Supprimer**.

Les options **Paramètres supplémentaires** vous permettent de déterminer la fréquence à laquelle Network Agent calcule l'utilisation de la bande passante, et si le trafic des protocoles est journalisé et à quelle fréquence.

Champ	Procédure
Intervalle de calcul de la bande passante	Entrez un nombre compris entre 1 et 300 pour spécifier la fréquence, en secondes, à laquelle Network Agent doit calculer l'utilisation de la bande passante. Une entrée de 300, par exemple, indique à Network Agent de calculer la bande passante toutes les 5 minutes. La valeur par défaut est 10 secondes.
Journaliser régulièrement le trafic de protocoles	Cochez cette option pour activer le champ Intervalle de journalisation.
Intervalle de journalisation	Entrez un nombre compris entre 1 et 300 pour spécifier la fréquence, en minutes, à laquelle Network Agent doit journaliser les protocoles. Une entrée de 60, par exemple, indique à Network Agent d'écrire dans le fichier journal toutes les heures. La valeur par défaut est 1 minute.

Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Configuration des paramètres locaux

Rubriques connexes :

- *Configuration des paramètres globaux*, page 428
- *Configuration des paramètres des cartes réseau*, page 431

La page **Paramètres > Network Agent > Paramètres locaux** permet de configurer le comportement du filtrage, les informations du proxy et les autres paramètres de l'instance de Network Agent sélectionnée.

- Pour accéder à la page Paramètres locaux d'une instance de Network Agent, ouvrez Paramètres > Network Agent et placez votre souris sur l'option **Global**. Une liste d'adresses IP s'affiche. Sélectionnez celle de l'instance à configurer.
- L'adresse IP de l'instance de Network Agent sélectionnée apparaît dans la barre de titre du panneau de contenu.

Servez-vous des paramètres **Définition de Filtering Service** pour spécifier quel service Filtering Service est associé à l'instance de Network Agent sélectionnée, et précisez comment répondre aux requêtes Internet lorsque Filtering Service n'est pas disponible.

Champ	Procédure
Adresse IP de Filtering Service	Sélectionnez l'instance de Filtering Service associée à cette instance de Network Agent.
Si Filtering Service n'est pas disponible	Sélectionnez **Autoriser** pour autoriser toutes les requêtes ou sélectionnez **Bloquer** pour bloquer toutes les requêtes jusqu'à ce que Filtering Service soit de nouveau disponible. La valeur par défaut est Autoriser.

Pour s'assurer que les requêtes des utilisateurs soient correctement surveillées, filtrées et journalisées, servez-vous de la liste **Proxy et caches** pour spécifier l'adresse IP du serveur proxy ou cache qui communique avec Network Agent.

- Cliquez sur **Ajouter** pour ajouter une adresse ou une plage d'adresses IPv4 ou IPv6 dans la liste (voir *Ajout ou modification des adresses IP*, page 434).
- Pour modifier une plage ou une adresse IP de la liste, cliquez sur son entrée.
- Pour retirer une entrée de la liste, cochez la case accolée à la plage ou à l'adresse IP, puis cliquez sur **Supprimer**.

Utilisez la liste **Cartes réseau** pour configurer des cartes réseau individuelles. Cliquez sur une carte réseau dans la colonne **Nom**, puis passez à la section *Configuration des paramètres des cartes réseau*, page 431, pour d'autres instructions.

Les options **Paramètres avancés de Network Agent** sont utilisées dans les cas suivants :

- Des requêtes HTTP circulent dans votre réseau via un port non standard.

  Par défaut, les **Ports utilisés pour le trafic HTTP** sont **8080, 80** (lorsque Websense est intégré à un pare-feu, un proxy ou un cache) ou **Tous** (dans un déploiement autonome).

- Vous souhaitez que Network Agent ignore le trafic qui circule sur certains ports.

  Cochez la case **Configure this Network Agent instance to ignore traffic on the following ports (Configurer cette instance de Network Agent pour ignorer le trafic sur les ports suivants)**, puis entrez un ou plusieurs ports.

  Si vous avez déployé Websense Content Gateway, cette option peut permettre d'éviter la journalisation en double du trafic HTTPS.

- Le Support technique de Websense vous demande de modifier des options de débogage à des fins de dépannage.

  Les options Paramètres de débogage ne doivent pas être modifiées sans l'intervention de notre Support technique.

Champ	Description
Mode	• Aucun (par défaut) • Général • Erreur • Détails • Bande passante
Sortie	• Fichier (par défaut) • Fenêtre
Port	55870 (par défaut)

Lorsque vos modifications sont terminées, cliquez sur **OK** pour les mettre en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Configuration des paramètres des cartes réseau

Rubriques connexes :

- *Configuration de Network Agent*, page 428
- *Configuration des paramètres de surveillance d'une carte réseau*, page 433
- *Ajout ou modification des adresses IP*, page 434

La page **Network Agent > Paramètres locaux > Configuration des cartes réseau** permet de spécifier comment Network Agent se sert de chaque carte réseau disponible pour surveiller et gérer l'utilisation du réseau.

La section **Informations sur la carte réseau** présente le contexte des modifications apportées, en indiquant l'**Adresse IP** de la carte réseau, une brève **Description** et son **Nom**. Ces informations vous permettent de vérifier que vous configurez bien la carte réseau appropriée.

Surveillance

Dans une configuration à plusieurs cartes réseau, vous pouvez définir l'une d'elles pour la surveillance du trafic et une autre pour l'envoi des pages de blocage. Une carte réseau au moins doit être utilisée pour la surveillance du trafic, mais plusieurs peuvent l'être.

Servez-vous de la section **Surveillance** pour indiquer à Network Agent s'il doit ou non **Utiliser cette carte réseau pour surveiller le trafic**.

- Si cette carte réseau n'est pas utilisée pour la surveillance, désactivez sa case à cocher et passez à la section suivante.
- Si la carte réseau est utilisée pour la surveillance, cochez sa case, puis cliquez sur **Configurer**. La page Configuration du comportement de la surveillance apparaît. Pour obtenir des instructions, consultez la section *Configuration des paramètres de surveillance d'une carte réseau*, page 433.

Autres options des cartes réseau

Outre la configuration des options de surveillance, vous pouvez également déterminer d'autres comportements pour vos cartes réseau :

1. Sous Blocage, assurez-vous que la carte réseau appropriée apparaît bien dans le champ **Carte réseau de blocage**. Si vous configurez plusieurs cartes réseau, les paramètres de chacune d'elles doivent correspondre à ceux de ce champ. En d'autres termes, une seule carte réseau est utilisée pour le blocage.
2. Si vous exécutez Websense en mode **Autonome**, l'option **Filtrer et journaliser les demandes HTTP** est activée et ne peut pas être modifiée.
3. Si vous avez intégré Websense à une application ou un périphérique tiers, utilisez les options **Intégrations** pour préciser comment cette instance de Network Agent doit filtrer et journaliser les requêtes HTTP. Les options qui ne s'appliquent pas à votre environnement sont désactivées.
   - Sélectionnez **Journaliser les demandes HTTP** pour améliorer la précision des rapports Websense.
   - Sélectionnez **Filtrer toutes les demandes non envoyées sur les ports HTTP** pour utiliser Network Agent pour filtrer uniquement les requêtes HTTP qui ne passent pas par le produit d'intégration.
4. Sous Gestion des protocoles, indiquez si Network Agent doit utiliser cette carte réseau pour filtrer les protocoles non HTTP :
   - Activez l'option **Filtrer les demandes de protocole non HTTP** pour activer la fonction de gestion des protocoles. Cela permet à Websense de filtrer les applications Internet et les méthodes de transfert de données, telles que celles utilisées pour la messagerie instantanée, la diffusion multimédia en streaming, le partage de fichiers, la messagerie Internet, etc. Pour plus d'informations, consultez *Filtrage des catégories et des protocoles*, page 50, et *Fonctionnement des protocoles*, page 264.

- Activez l'option **Mesurer l'utilisation de bande passante par protocole** pour activer la fonction Bandwidth Optimizer. Network Agent utilise cette carte réseau pour surveiller l'utilisation de la bande passante de votre réseau par chaque protocole ou application. Pour plus d'informations, consultez la section *Exploitation de Bandwidth Optimizer pour gérer la bande passante*, page 270.

Configuration des paramètres de surveillance d'une carte réseau

La page **Paramètres locaux > Configuration de carte réseau > Liste de surveillance** permet de spécifier quelles adresses IP sont surveillées par Network Agent via la carte réseau sélectionnée.

1. Sous Liste de surveillance, spécifiez les requêtes surveillées par Network Agent :
   - **Toutes** : Network Agent surveille les requêtes de toutes les adresses IP qu'il voit utiliser la carte réseau sélectionnée. En général, cela comprend tous les ordinateurs situés sur le même segment de réseau que la carte réseau ou l'ordinateur Network Agent en cours.
   - **Aucune** : Network Agent ne surveille aucune requête.
   - **Spécifique** : Network Agent surveille uniquement les segments réseau inclus dans la Liste de surveillance.
2. Si vous sélectionnez Spécifique, cliquez sur **Ajouter**, puis désignez les adresses IP que Network Agent doit surveiller (au format IPv4 ou IPv6). Pour plus d'informations, consultez la section *Ajout ou modification des adresses IP*, page 434.

   Remarque

   Vous ne pouvez pas entrer de plages d'adresses IP qui se chevauchent. Si les plages se chevauchent, les mesures de la bande passante du réseau risquent d'être imprécises et le filtrage basé sur la bande passante peut ne pas s'appliquer correctement.

   Pour retirer une adresse IP ou une plage réseau, cochez l'élément approprié dans la liste, puis cliquez sur **Supprimer**.
3. Sous Exceptions de liste de surveillance, identifiez tous les ordinateurs internes que Network Agent doit exclure de la surveillance.

   Par exemple, Network Agent peut ignorer les requêtes provenant du serveur CPM. De cette façon, ce dernier ne viendra pas encombrer le journal Websense ni les résultats du moniteur d'état.

   a. Pour identifier un ordinateur, cliquez sur **Ajouter**, puis entrez son adresse IP au format IPv4 ou IPv6.

   b. Répétez ce processus pour identifier d'autres ordinateurs.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Configuration de carte réseau. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Ajout ou modification des adresses IP

Rubriques connexes :

- *Configuration des paramètres globaux*, page 428
- *Configuration des paramètres locaux*, page 430
- *Configuration des paramètres des cartes réseau*, page 431

Utilisez la page **Ajouter des adresses IP** ou **Modifier des adresses IP** pour apporter des modifications dans les listes suivantes de Network Agent : Définition du réseau interne, Trafic interne à surveiller, Proxy et caches, Liste de surveillance ou Exceptions de liste de surveillance.

- Les adresses et les plages IPv4 et IPv6 sont prises en charge.
- Lorsque vous ajoutez ou modifiez une plage d'adresses IP, assurez-vous qu'elle n'empiète pas sur une entrée existante (adresse IP unique ou plage d'adresses) dans la liste.
- Lorsque vous ajoutez ou modifiez une seule adresse IP, assurez-vous qu'elle ne fasse pas partie d'une plage apparaissant déjà dans la liste.

Pour ajouter une nouvelle adresse IP ou plage d'adresses IP :

1. Sélectionnez le bouton radio **Adresse IP** ou **Plage d'adresses IP**.
2. Entrez une plage ou une adresse IP valide.
3. Cliquez sur **OK** pour revenir à la page précédente des paramètres de Network Agent. La nouvelle plage ou adresse IP s'affiche dans le tableau approprié.

   Pour revenir à la page précédente sans mettre vos modifications en cache, cliquez sur **Annuler**.
4. Au besoin, répétez ce processus pour chaque adresse IP supplémentaire.

Lorsque vous modifiez une plage ou une adresse IP existante, la page Modifier des adresses IP affiche l'élément sélectionné avec le bouton radio approprié déjà activé. Effectuez les modifications nécessaires, puis cliquez sur **OK** pour revenir à la page précédente.

Lorsque vos modifications sont terminées, cliquez sur **OK** dans la page des paramètres de Network Agent. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Vérification de la configuration de Network Agent

Après avoir configuré Network Agent dans TRITON - Web Security, vous pouvez utiliser tout analyseur de paquets tiers pour vérifier que les ordinateurs de votre réseau sont bien visibles par le logiciel Websense.

Assurez-vous que la carte réseau que vous avez configurée en tant que carte réseau de surveillance de Network Agent puisse voir le trafic provenant des adresses IP de tous les segments du réseau que l'instance de Network Agent doit surveiller. (Cette configuration s'effectue à la page Paramètres locaux > Configuration de carte réseau > Liste de surveillance. Voir *Configuration des paramètres de surveillance d'une carte réseau*, page 433.)

Si des paquets provenant de certaines adresses IP ne sont pas visibles par la carte réseau de surveillance :

- Vérifiez la configuration du réseau et les exigences de placement des cartes réseau (consultez le Centre Installation et déploiement ou le Guide de démarrage rapide de Network Agent).
- Vérifiez que vous avez correctement configuré la carte réseau de surveillance (voir *Configuration des paramètres des cartes réseau*, page 431).

19 Dépannage

Servez-vous de cette section pour trouver des solutions aux problèmes courants avant de contacter le support technique.

Le site Web du support technique de Websense propose une vaste Base de données de connaissances et des forums de clients, disponibles à l'adresse support.websense.com. Lancez des recherches par mot-clé ou phrase, ou parcourez le contenu par produit et version.

Les instructions relatives au dépannage sont regroupées dans les sections suivantes :

- *Problèmes d'installation et d'abonnement*
- *Problèmes de la base de données principale*, page 439
- *Problèmes de filtrage*, page 445
- *Problèmes liés à Network Agent*, page 450
- *Problèmes de configuration et d'identification des utilisateurs*, page 453
- *Problèmes de messages de blocage*, page 463
- *Problèmes liés aux journaux, aux messages d'état et aux alertes*, page 465
- *Problèmes liés à Policy Server et à la base de données des stratégies*, page 469
- *Problèmes d'administration déléguée*, page 471
- *Problème de Log Server et de la base de données d'activité*, page 472
- *Problèmes des rapports d'investigation et de présentation*, page 487
- *Autres problèmes de génération de rapports*, page 494
- *Problèmes d'interopérabilité*, page 499
- *Conseils et outils de dépannage*, page 515

Problèmes d'installation et d'abonnement

- *Il existe un problème d'abonnement.*, page 438
- *Impossible de vérifier la clé d'abonnement*, page 438
- *Après la mise à niveau, absence de certains utilisateurs dans TRITON - Web Security*, page 439

Il existe un problème d'abonnement.

Une clé d'abonnement valide est nécessaire pour télécharger la Base de données principale Websense et effectuer un filtrage de l'activité Internet. Lorsque votre abonnement arrive à expiration ou n'est pas valide, et lorsque la base de données principale n'a pas été téléchargée depuis plus de deux semaines, le résumé sur les alertes d'état présente un avertissement dans l'onglet Système de la page État > Tableau de bord.

- Vérifiez que vous avez saisi votre clé d'abonnement exactement telle que vous l'avez reçue. La clé d'abonnement respecte la casse.
- Vérifiez que votre abonnement n'est pas arrivé à expiration. Voir *Clé d'abonnement*, page 441.
- Vérifiez que la base de données principale a bien été téléchargée avec succès au cours des deux dernières semaines. Vous pouvez vérifier l'état du téléchargement dans TRITON - Web Security : cliquez sur **Téléchargement de la base de données** dans la page État > Tableau de bord.

  Pour résoudre les problèmes de téléchargement de cette base de données, consultez la section *Échec du téléchargement de la base de données principale*, page 440.

Si vous avez saisi la clé correctement mais que l'erreur d'état persiste, ou si votre abonnement est arrivé à expiration, contactez Websense, Inc. ou votre revendeur agréé.

Lorsque votre abonnement expire, les paramètres de TRITON - Web Security déterminent si tous les utilisateurs obtiennent un accès Internet non filtré ou si toutes les requêtes Internet sont bloquées. Pour plus d'informations, consultez la section *Votre abonnement*, page 24.

Impossible de vérifier la clé d'abonnement

Lorsque vous saisissez votre clé d'abonnement, Filtering Service tente de se connecter au serveur de téléchargement de la base de données Websense afin de la vérifier et de télécharger la base de données principale.

Lorsque Filtering Service ne parvient pas à se connecter au serveur de téléchargement de la base de données, des erreurs d'abonnement et de téléchargement de base de données s'affichent dans TRITON - Web Security.

- Si le serveur de téléchargement de base de données est en panne, le problème doit se résoudre rapidement de lui-même.
- Si Filtering Service ne parvient pas à se connecter au serveur de téléchargement, consultez les sections *Accès Internet*, page 441, et *Vérification des paramètres du pare-feu ou du serveur proxy*, page 442, afin de vérifier que Filtering Service et votre environnement réseau sont correctement configurés et autorisent la connexion.

Après la mise à niveau, absence de certains utilisateurs dans TRITON - Web Security

Si vous avez défini votre service d'annuaire sur Active Directory après avoir mis Websense à niveau, il est possible que des noms d'utilisateur ne s'affichent pas dans TRITON - Web Security. Cela se produit lorsque les noms d'utilisateur comprennent des caractères n'appartenant pas au jeu de caractères UTF-8.

Pour prendre en charge LDAP 3.0, le programme d'installation de Websense remplace le jeu de caractères MBCS par le jeu UTF-8 pendant la mise à niveau. Par conséquent, les noms d'utilisateur qui comprennent des caractères non UTF-8 ne sont pas reconnus correctement.

Pour résoudre ce problème, définissez manuellement le jeu de caractères sur MBCS :

1. Sélectionnez **Paramètres** > **Général** > **Services d'annuaire**.
2. Assurez-vous que **Active Directory (en mode natif)** soit sélectionné sous Annuaires, en haut de la page.
3. Cliquez sur **Paramètres avancés de l'annuaire**.
4. Sous Jeu de caractères, cliquez sur **MBCS**. Il vous faudra peut-être faire défiler les éléments pour voir cette option.
5. Cliquez sur **OK** pour mettre la modification en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Problèmes de la base de données principale

- *Utilisation de la base de données pour le filtrage initial*, page 439
- *Base de données principale âgée de plus d'une semaine*, page 440
- *Échec du téléchargement de la base de données principale*, page 440
- *Échec du téléchargement de la base de données principale à l'heure définie*, page 445
- *Contact du support technique pour les problèmes de téléchargement de la base de données*, page 445

Utilisation de la base de données pour le filtrage initial

La base de données principale Websense héberge les définitions de catégories et de protocoles qui constituent la base du filtrage du contenu Internet.

Une version partielle de la base de données principale est installée en même temps que Websense dans chaque ordinateur Filtering Service. Cette base de données partielle est utilisée pour activer la fonction de filtrage de base dès que vous entrez votre clé d'abonnement.

Vous devez télécharger la base de données dans son intégralité pour qu'un filtrage complet soit effectué. Pour plus d'informations, consultez la section *Base de données principale Websense*, page 27.

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

Base de données principale âgée de plus d'une semaine

La Base de données principale de Websense héberge les définitions des catégories et des protocoles qui constituent la base du filtrage du contenu Internet. Websense télécharge les modifications apportées à la base de données principale en fonction du planning défini dans TRITON - Web Security. Par défaut, le téléchargement est programmé pour s'exécuter une fois par jour.

Pour déclencher manuellement le téléchargement de la base de données :

1. Ouvrez la page **État > Tableau de bord**, puis cliquez sur **Téléchargement de la base de données**.
2. Cliquez sur **Mettre à jour** à côté de l'instance de Filtering Service appropriée pour démarrer le téléchargement de la base de données, ou cliquez sur **Tout mettre à jour** pour démarrer le téléchargement dans tous les ordinateurs Filtering Service.

   Remarque

   Après le téléchargement des mises à jour de la base de données principale, l'utilisation du processeur peut être de 90 % ou plus pendant quelques minutes pendant le chargement de la base de données dans la mémoire locale. Il est généralement préférable de programmer les téléchargements en dehors des heures de pointe.

3. Pour continuer à travailler pendant le téléchargement de la base de données, cliquez sur **Fermer**.

   Cliquez sur le bouton **Téléchargement de la base de données** à tout moment pour afficher l'état du téléchargement.

Si une nouvelle version de la base de données principale ajoute ou supprime des catégories ou des protocoles, les administrateurs qui exécutent des tâches de gestion de stratégies liées aux catégories ou aux protocoles (par exemple qui modifient un jeu de catégories) au moment du téléchargement peuvent recevoir des erreurs. Bien que de telles mises à jour soient assez rares, il est préférable d'éviter, dans la mesure du possible, de modifier des éléments liés aux catégories, aux protocoles et aux filtres pendant la mise à jour d'une base de données.

Échec du téléchargement de la base de données principale

Si vous n'arrivez pas à télécharger la base de données principale Websense :

- Vérifiez que vous avez correctement saisi votre clé d'abonnement dans TRITON - Web Security et que cette clé n'est pas arrivée à expiration (*Clé d'abonnement*, page 441).
- Vérifiez que l'ordinateur Filtering Service peut accéder à Internet (voir *Accès Internet*, page 441).
- Vérifiez les paramètres du pare-feu ou du serveur proxy pour vous assurer que Filtering Service peut se connecter au serveur de téléchargement de Websense (voir *Vérification des paramètres du pare-feu ou du serveur proxy*, page 442).

- Vérifiez que l'ordinateur de téléchargement dispose de suffisamment d'espace disque (voir *Espace disque insuffisant dans l'ordinateur Filtering Service*, page 443) et de mémoire (voir *Mémoire insuffisante dans l'ordinateur Filtering Service*, page 444).
- Recherchez la présence dans le réseau d'une application ou d'un dispositif, par exemple un logiciel antivirus, susceptible d'empêcher la connexion du téléchargement (voir *Applications restrictives*, page 444).

Clé d'abonnement

Pour vérifier que la clé d'abonnement a été saisie correctement et n'est pas arrivée à expiration :

1. Sélectionnez **Paramètres > Général > Compte**.
2. Comparez la clé que Websense, Inc. ou votre revendeur vous a envoyée avec celle qui apparaît dans le champ **Clé d'abonnement**. La clé doit reproduire la même combinaison de majuscules/minuscules que votre document.
3. Vérifiez la date accolée à **Date d'expiration de la clé**. Si cette date est dépassée, contactez votre revendeur ou Websense, Inc., afin de renouveler votre abonnement.
4. Si vous avez modifié la clé dans la boîte de dialogue Paramètres, cliquez sur **OK** pour activer la clé et le téléchargement de la base de données.

Pour démarrer manuellement un téléchargement de la base de données, ou pour vérifier l'état du dernier téléchargement, cliquez sur **Téléchargement de la base de données** dans la barre d'outils située en haut de la page État > Tableau de bord.

Accès Internet

Pour télécharger la base de données principale, l'ordinateur Filtering Service envoie une commande **HTTP post** aux serveurs de téléchargement aux URL suivantes :

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com

Pour vérifier que Filtering Service peut accéder à Internet pour communiquer avec le serveur de téléchargement :

1. Ouvrez un navigateur dans l'ordinateur exécutant Filtering Service.
2. Entrez l'URL suivante :

   http://download.websense.com/

   Si l'ordinateur peut ouvrir une connexion HTTP auprès de ce site, une page de redirection s'affiche et le navigateur affiche la page d'accueil de Websense.

   Si ce n'est pas le cas, assurez-vous que l'ordinateur :

   - Peut communiquer sur le port 80, ou sur le port désigné dans votre réseau pour le trafic HTTP
   - Est configuré de manière à effectuer correctement les recherches DNS
   - Est configuré pour utiliser les serveurs proxy éventuellement nécessaires (voir *Vérification des paramètres du pare-feu ou du serveur proxy*, page 442)

Assurez-vous également que certaines règles de votre passerelle ne bloquent pas le trafic HTTP provenant de l'ordinateur Filtering Service.

3. Pour vérifier que l'ordinateur peut communiquer avec le site de téléchargement, utilisez l'une des méthodes suivantes :
   - À l'invite de commande, entrez la commande suivante :
     ```
     ping download.websense.com
     ```
     Vérifiez que le ping obtient bien une réponse du serveur de téléchargement.
   - Utilisez Telnet pour vous connecter à **download.websense.com 80**. Si vous voyez un curseur et aucun message d'erreur, vous pouvez vous connecter au serveur de téléchargement.

Vérification des paramètres du pare-feu ou du serveur proxy

Si la base de données principale est téléchargée via un pare-feu ou un serveur proxy exigeant une authentification, assurez-vous qu'un navigateur de l'ordinateur Filtering Service puisse charger correctement les pages Web. Si les pages s'ouvrent normalement mais que la base de données principale n'est pas téléchargée, vérifiez les paramètres du serveur proxy dans le navigateur Web.

Microsoft Internet Explorer :

1. Sélectionnez **Outils** > **Options Internet**, puis l'onglet **Connexions**.
2. Cliquez sur **Paramètres réseau** et prenez note des paramètres indiqués sous **Serveur proxy**.

Mozilla Firefox :

1. Sélectionnez **Outils** > **Options** >, puis l'onglet **Avancé**.
2. Dans l'onglet **Réseau** (généralement sélectionné par défaut), cliquez sur **Paramètres**.

   La boîte de dialogue Paramètres de connexion indique si le navigateur est configuré pour se connecter à un serveur proxy. Notez les paramètres du proxy.

Ensuite, assurez-vous que Websense soit configuré pour utiliser le même serveur proxy pour effectuer le téléchargement.

1. Sélectionnez **Paramètres** > **Général** > **Téléchargement de base de données**.
2. Vérifiez que l'option **Utiliser un serveur proxy ou un pare-feu** est activée et que le serveur et le port appropriés apparaissent.
3. Vérifiez l'exactitude de tous les paramètres d'**Authentification**. Vérifier le nom d'utilisateur et le mot de passe, en respectant l'orthographe et la casse.

   Si Websense doit fournir des informations d'authentification, le pare-feu ou le serveur proxy doit être configuré pour accepter l'authentification de base ou en texte clair. Des informations sur l'activation de l'authentification de base sont disponibles sur le site support.websense.com.

Si un pare-feu limite l'accès à Internet au moment où Websense Express télécharge habituellement la base de données, ou limite la taille d'un fichier pouvant être transféré via HTTP, Websense ne peut pas télécharger la base de données. Pour déterminer si le pare-feu est la cause du problème de téléchargement, voyez si l'une de ses règles est susceptible de bloquer le téléchargement, puis modifiez au besoin les heures de téléchargement dans TRITON - Web Security (voir *Configuration des téléchargements de la base de données*, page 28).

Espace disque insuffisant dans l'ordinateur Filtering Service

Filtering Service doit disposer de suffisamment d'espace disque pour télécharger la base de données principale compressée dans le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut). De même, l'espace disque disponible doit lui permettre de décompresser et de charger la base de données. En règle générale, Websense, Inc. recommande un espace disque disponible d'au moins 4 Go dans le lecteur de téléchargement.

Un avertissement signale que l'espace disque disponible sur l'ordinateur Filtering Service est inférieur à 4 Go.

Sous les systèmes Windows, utilisez l'Explorateur de Windows pour vérifier l'espace disque disponible :

1. Ouvrez **Poste de travail** dans l'Explorateur Windows (pas dans Internet Explorer).
2. Sélectionnez le lecteur sur lequel Websense est installé. Par défaut, Websense est situé sur le lecteur C.
3. Cliquez du bouton droit sur le lecteur et sélectionnez **Propriétés**.
4. Dans l'onglet Général, vérifiez que l'espace disque disponible est supérieur ou égal à 4 Go. Si l'espace disponible sur le lecteur est insuffisant, supprimez les fichiers inutiles pour libérer l'espace requis.

Dans les systèmes Linux, utilisez la commande **df** pour vérifier la quantité d'espace disponible dans le système de fichiers sur lequel Websense est installé :

1. Ouvrez une session sur le terminal.
2. À l'invite, entrez :

   ```
   df -h /opt
   ```

   Websense est généralement installé dans le répertoire /opt/Websense/bin/. S'il est installé en un autre emplacement, utilisez ce chemin.
3. Assurez-vous que l'espace disque disponible soit supérieur ou égal à 4 Go. Si l'espace disponible sur le lecteur est insuffisant, supprimez les fichiers inutiles pour libérer l'espace requis.

Si, après avoir corrigé les problèmes d'espace disque, vous ne pouvez toujours pas télécharger la base de données principale :

1. Arrêtez tous les services Websense dans l'ordinateur Filtering Service (voir *Arrêt et démarrage des services Websense*, page 375).
2. Supprimez les fichiers **Websense.xfr** et **Websense** (sans extension) dans le répertoire **bin** de Websense.
3. Redémarrez les services Websense.
4. Démarrez manuellement le téléchargement de la base de données (ouvrez la page **État > Tableau de bord** de TRITON - Web Security, puis cliquez sur **Téléchargement de base de données**).

Mémoire insuffisante dans l'ordinateur Filtering Service

La mémoire nécessaire pour exécuter Websense, télécharger la base de données principale et mettre à jour cette dernière dépend de la taille de votre réseau.

- Dans le cas d'un petit réseau, 2 Go de mémoire sont conseillés (Windows et Linux).
- Vous trouverez des recommandations système complètes dans le Centre Installation et déploiement.

Lorsque la mémoire disponible dans l'ordinateur Filtering Service descend au-dessous de 512 Mo, le système génère un message d'alerte de fonctionnement. Ce calcul ne tient pas compte de l'espace lié à la mémoire tampon et au cache.

Si l'ordinateur répond aux exigences indiquées dans le Centre Installation et déploiement et si Filtering Service peut télécharger la base de données principale, il est peu probable que la condition de mémoire faible pose des problèmes.

Si Filtering Service ne peut pas charger la base de données principale, vous devrez toutefois libérer de la mémoire sur l'ordinateur ou ajouter de la mémoire RAM.

Pour vérifier la mémoire disponible dans un système Windows :

1. Ouvrez le Gestionnaire des tâches.
2. Sélectionnez l'onglet **Performances**.
3. Vérifiez la **Mémoire physique** totale disponible.

Vous pouvez également utiliser l'Analyseur de performances de Windows (Démarrer > Outils d'administration > Performances) pour collecter ces informations.

Pour vérifier la mémoire disponible dans un système Linux :

1. Ouvrez une session sur le terminal.
2. À l'invite, entrez :

   ```
   top
   ```

3. Calculez la mémoire totale disponible en ajoutant **Mem: av** et **Swap: av**.

Pour résoudre les problèmes de mémoire insuffisante, vous pouvez ajouter de la mémoire RAM à l'ordinateur ou migrer les applications qui sollicitent fortement la mémoire dans un autre ordinateur.

Applications restrictives

Certaines applications restrictives, telles que les logiciels antivirus, les applications de limite de taille ou les systèmes de détection des intrusions, peuvent interférer avec les téléchargements de la base de données. Dans la mesure du possible, configurez Websense pour qu'il passe directement à la dernière passerelle de sorte qu'il n'ait pas besoin de se connecter à ces applications ou dispositifs. Vous pouvez également :

1. Désactivez les restrictions liées à l'ordinateur Filtering Service et à l'emplacement de téléchargement de la base de données principale.

   Pour obtenir des instructions sur la modification de la configuration du périphérique ou du dispositif, consultez sa documentation.
2. Tentez de télécharger la Base de données principale.

Si cette modification n'a aucun effet, reconfigurez l'application ou le dispositif pour y inclure l'ordinateur exécutant Filtering Service.

Échec du téléchargement de la base de données principale à l'heure définie

Il est possible que l'heure et la date du système ne soient pas définis correctement dans l'ordinateur Filtering Service. Websense utilise l'horloge du système pour déterminer l'heure du téléchargement de la base de données principale.

Si le téléchargement ne s'effectue pas du tout, consultez *Échec du téléchargement de la base de données principale*, page 440.

Contact du support technique pour les problèmes de téléchargement de la base de données

Si les problèmes de téléchargement de la base de données principale persistent à la fin de la procédure de dépannage de cette section d'aide, envoyez les informations suivantes au support technique de Websense :

1. Le message d'erreur exact qui s'affiche dans la boîte de dialogue Téléchargement de la base de données
2. Les adresses IP externes des ordinateurs qui tentent de télécharger la base de données
3. Votre clé d'abonnement Websense
4. La date et l'heure de la dernière tentative
5. Le nombre d'octets transférés, le cas échéant
6. Ouvrez une fenêtre d'invite de commande et exécutez la commande **nslookup** sur **download.websense.com**. Si la connexion au serveur de téléchargement est établie, communiquez les adresses IP renvoyées au service technique.
7. Ouvrez une fenêtre d'invite de commande et exécutez la commande **tracert** sur **download.websense.com**. Si la connexion au serveur de téléchargement est établie, envoyez le suivi du routage au Support technique.
8. Un suivi de paquets ou une capture de paquets exécuté(e) sur le serveur de téléchargement Websense pendant une tentative de téléchargement
9. Un suivi de paquets ou une capture de paquets exécuté(e) sur la passerelle réseau pendant la même tentative de téléchargement
10. Les fichiers suivants du répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) : **websense.ini**, **eimserver.ini** et **config.xml**.

Pour obtenir les coordonnées du support technique, consultez le portail support.websense.com/.

Problèmes de filtrage

- *Dysfonctionnement de Filtering Service*, page 446
- *User Service non disponible*, page 446
- *Classement incorrect des sites dans la catégorie Technologies de l'information*, page 448
- *Mots-clés non bloqués*, page 448
- *Problème de filtrage des URL de filtre d'accès limité ou personnalisé*, page 449

- *Requêtes FTP non bloquées comme prévu*, page 449
- *Non application des stratégies de groupe ou d'utilisateur*, page 449
- *Utilisateurs distants non filtrés par la stratégie appropriée*, page 449

Dysfonctionnement de Filtering Service

Lorsque Filtering Service ne fonctionne pas, les requêtes Internet ne peuvent être ni filtrées ni journalisées.

Filtering Service peut s'arrêter dans les cas suivants :

- L'ordinateur Filtering Service ne dispose pas de suffisamment d'espace disque (voir *Espace disque insuffisant dans l'ordinateur Filtering Service*, page 443).
- Un téléchargement de la base de données principale a échoué du fait d'un manque d'espace disque (voir *Échec du téléchargement de la base de données principale*, page 440).
- Le fichier **websense.ini** est manquant ou corrompu.
- Vous avez arrêté le service (par exemple après la création de pages de blocage personnalisées) et vous ne l'avez pas redémarré.

Filtering Service peut également sembler arrêté si vous avez redémarré plusieurs services Websense sans le faire dans l'ordre approprié. Lorsque vous redémarrez plusieurs services, n'oubliez pas de démarrer la base de données de stratégies, Policy Broker et Policy Server avant les autres services Websense.

Pour résoudre ces problèmes :

- Vérifiez que l'ordinateur Filtering Service dispose d'au moins 3 Go d'espace disque disponible. Vous pouvez éventuellement supprimer des fichiers inutiles ou ajouter des capacités supplémentaires.
- Naviguez jusqu'au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut), et vérifiez que vous pouvez ouvrir le fichier **websense.ini** dans un éditeur de texte. Si ce fichier est corrompu, remplacez-le par un fichier de sauvegarde.
- Regardez dans l'Observateur d'événements de Windows ou dans le fichier **websense.log** si des messages d'erreur sont liés au service Filtering Service (voir *Conseils et outils de dépannage*, page 515).
- Déconnectez-vous de TRITON - Web Security, redémarrez Policy Server, puis redémarrez Filtering Service (voir *Arrêt et démarrage des services Websense*, page 375).

  Attendez une minute avant de vous reconnecter à TRITON - Web Security.

User Service non disponible

Lorsque User Service ne fonctionne pas, ou lorsque Policy Server ne peut pas communiquer avec ce service, Websense ne peut pas appliquer correctement les stratégies de filtrage basées sur les utilisateurs.

User Service peut sembler arrêté si vous avez redémarré Policy Server après avoir redémarré d'autres services Websense. Pour résoudre ce problème :

1. Redémarrez le service Websense Policy Server (voir *Arrêt et démarrage des services Websense*, page 375).
2. Démarrez ou redémarrez Websense User Service.
3. Fermez TRITON - Web Security.

   Attendez une minute avant de vous reconnecter à TRITON - Web Security.

Si le problème n'est pas résolu à la fin de la procédure précédente :

- Regardez dans l'Observateur d'événements de Windows ou dans le fichier **websense.log** si des messages d'erreur sont liés au service User Service (voir *Conseils et outils de dépannage*, page 515).
- Naviguez jusqu'au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut), et vérifiez que vous pouvez ouvrir le fichier **websense.ini** dans un éditeur de texte. Si ce fichier est corrompu, remplacez-le par un fichier de sauvegarde.

Utilisation intensive du processeur dans l'ordinateur Filtering Service

Lorsque le processeur de l'ordinateur Filtering Service est surchargé (du fait du volume de traitement effectué par Filtering Service ou des demandes des autres logiciels en exécution dans l'ordinateur Filtering Service), la navigation des utilisateurs peut ralentir puisque le traitement des requêtes de sites prend davantage de temps.

Pendant les périodes de pic d'utilisation du processeur (supérieure à 95 %), il est possible que Filtering Service ne puisse pas traiter les requêtes du tout, ce qui altère le filtrage.

Pour corriger ce problème, commencez par utiliser le Gestionnaire des taches (Windows) ou la commande **top** (Linux) pour identifier les processus qui sollicitent intensivement le processeur.

- Certaines applications peuvent-elles être exécutées à partir d'un autre ordinateur ?
- Pouvez-vous installer Filtering Service dans un ordinateur dédié ?

Si Filtering Service consomme beaucoup de temps de traitement :

- Évaluez le volume de trafic que doit traiter Filtering Service. Les recherches DNS pouvant requérir un temps de traitement assez important, vous pouvez envisager d'installer une instance de Filtering Service supplémentaire pour équilibrer la charge.
- Évaluez votre utilisation des mots-clés et des expressions régulières. Utilisez-vous un grand nombre d'expressions régulières ou de mots-clés, ou encore des expressions régulières très complexes ?

  Réduire le nombre de mots-clés et d'expressions régulières, ou supprimer ou simplifier les expressions régulières complexes, peut améliorer les performances de Filtering Service.

Classement incorrect des sites dans la catégorie Technologies de l'information

Les versions 4.0 et ultérieures d'Internet Explorer acceptent les recherches saisies dans la barre d'adresse. Lorsque cette option est activée, si l'utilisateur entre uniquement un nom de domaine dans la barre d'adresse (**websense** au lieu de **http://www.websense.com**, par exemple), Internet Explorer considère l'entrée comme une requête de recherche et non comme une requête de site. Il affiche le site le plus ressemblant recherché par l'utilisateur, et la liste des sites les plus proches.

Par conséquent, Websense autorise, bloque ou limite la requête en fonction de l'état de la catégorie Technologies de l'information/Moteurs de recherche et portails de la stratégie active, pas en fonction de la catégorie du site demandé. Pour que Websense filtre en fonction de la catégorie du site demandé, désactivez les recherches à partir de la barre d'adresse :

1. Sélectionnez **Outils > Options Internet**.
2. Ouvrez l'onglet **Avancé**.
3. Dans le champ Rechercher à partir de la barre d'adresse, sélectionnez :
   - Internet Explorer 5, 6 et 7 : **Ne pas effectuer de recherche à partir de la barre d'adresse**
   - Internet Explorer 8 : **Ne pas envoyer d'adresses inconnues à votre moteur de recherche automatique**
4. Cliquez sur **OK**.

Mots-clés non bloqués

Les causes potentielles de ce problème sont les suivantes : l'option **Désactiver le blocage par mot-clé** est activée, ou le site dont l'URL contient le mot-clé utilise une commande **post** pour envoyer des données à votre serveur Web.

Pour vérifier que le blocage par mot-clé est activé :

1. Sélectionnez **Paramètres > Général > Filtrage**.
2. Sous Filtrage général, vérifiez la liste **Options de recherche de mots-clés**. Si **Désactiver le blocage par mot-clé** apparaît, sélectionnez une autre option dans la liste. Pour plus d'informations sur les options disponibles, consultez *Configuration des paramètres de filtrage de Websense*, page 67.
3. Cliquez sur **OK** pour mettre la modification en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Si un site utilise une commande **post** pour envoyer des données à votre serveur Web, Websense ne reconnaît pas les paramètres de filtrage par mot-clé pour cette URL. À moins que votre produit d'intégration ne reconnaisse les données envoyées via la commande post, les utilisateurs peuvent toujours accéder aux URL contenant des mots-clés bloqués.

Pour voir si une URL utilise une commande post, affichez la source de l'URL depuis votre navigateur. Si le code source contient la chaîne « <method=post> », la commande post est utilisée pour charger l'URL.

Problème de filtrage des URL de filtre d'accès limité ou personnalisé

Si l'URL HTTPS d'un filtre d'accès limité ou d'une liste d'URL personnalisées (recatégorisées ou non filtrées) n'est pas filtrée comme prévu, il se peut qu'un produit d'intégration convertisse l'URL en un format non reconnu par Filtering Service.

Les produits d'intégration non proxy convertissent les URL du format domaine au format IP. Par exemple, l'URL **https://<domaine.com>** est lue en tant que **https://<adresse_IP>:443**. Lorsque cela se produit, Filtering Service ne peut pas associer l'URL envoyée par le produit d'intégration à l'URL personnalisée ou au filtre d'accès limité, et ne filtre donc pas le site de façon appropriée.

Pour contourner ce problème, ajoutez à la fois les adresses IP et les URL des sites que vous souhaitez filtrer à l'aide d'URL personnalisées ou de filtres d'accès limité.

Requêtes FTP non bloquées comme prévu

Dans le cas d'une intégration aux pare-feu Check Point®, Websense requiert l'activation de **l'affichage des dossiers** dans le navigateur du client pour reconnaître et filtrer les requêtes FTP.

Lorsque l'affichage des dossiers n'est pas activé, les requêtes FTP envoyées au proxy FireWall-1 sont envoyées à Websense avec un préfixe « http:// ». Websense filtre donc ces requêtes en tant que requêtes HTTP et non FTP.

Non application des stratégies de groupe ou d'utilisateur

Un certain nombre de facteurs peuvent être à l'origine du non filtrage de la stratégie d'utilisateurs et de groupes que vous avez définie. Pour plus d'informations, consultez les rubriques suivantes et la Base de connaissances.

- *User Service non disponible*, page 446
- *Utilisateurs distants non filtrés par la stratégie appropriée*, page 449
- *Connectivité et configuration du service d'annuaire*, page 458
- *Configuration du service d'annuaire dans TRITON - Web Security*, page 458
- *Identification des utilisateurs et Windows Server 2008*, page 459
- *User Service sous Linux*, page 461
- *Filtrage incorrect des utilisateurs distants*, page 462

Utilisateurs distants non filtrés par la stratégie appropriée

Lorsqu'un utilisateur distant se connecte au réseau à l'aide d'identifiants du domaine mis en cache (informations de connexion réseau), Websense applique la stratégie attribuée à cet utilisateur, ou au groupe ou au domaine de l'utilisateur, le cas échéant. Si aucune stratégie n'est attribuée à l'utilisateur, au groupe ou au domaine, ou si l'utilisateur se connecte à l'ordinateur avec un compte d'utilisateur local, Websense applique la stratégie Par défaut.

Il peut cependant arriver qu'un utilisateur ne soit pas filtré par une stratégie d'utilisateur ou de groupe, ni par la stratégie Par défaut. Cela se produit lorsque l'utilisateur se connecte à l'ordinateur distant avec un compte d'utilisateur local et que

la dernière partie de l'adresse MAC (Media Access Control) de l'ordinateur distant chevauche une adresse IP réseau à laquelle une stratégie a été attribuée. Dans ce cas, la stratégie attribuée à cette adresse IP particulière est appliquée à l'utilisateur distant.

Problèmes liés à Network Agent

- *Network Agent non installé*, page 450
- *Non exécution de Network Agent*, page 450
- *Network Agent ne surveille aucune carte réseau*, page 451
- *Network Agent ne peut pas communiquer avec Filtering Service*, page 451

Network Agent non installé

Network Agent doit être installé pour que le filtrage par protocoles puisse s'effectuer. Avec certaines intégrations, Network Agent permet également une journalisation plus précise.

Si vous utilisez un produit d'intégration et que vous n'avez pas besoin de la journalisation ni du filtrage par protocoles de Network Agent, vous pouvez masquer le message d'état « Aucun agent Network Agent n'est installé ». Pour obtenir des instructions, consultez la section *Vérification de l'état actuel du système*, page 385.

Dans le cas d'une installation autonome, Network Agent doit être installé pour surveiller et filtrer le trafic réseau. Pour obtenir des instructions sur l'installation, consultez le Centre Installation et déploiement, puis la section *Configuration de Network Agent*, page 428.

Non exécution de Network Agent

Network Agent doit être installé pour que le filtrage par protocoles puisse s'effectuer. Avec certaines intégrations, Network Agent permet également une journalisation plus précise.

Dans le cas d'une installation autonome, Network Agent doit s'exécuter pour surveiller et filtrer le trafic réseau.

Pour résoudre ce problème :

1. Ouvrez la boîte de dialogue Services de Windows (voir *Boîte de dialogue Services de Windows*, page 515) pour voir si le service **Websense Network Agent** a démarré.
2. Redémarrez les services **Websense Policy Broker** et **Websense Policy Server** (voir *Arrêt et démarrage des services Websense*, page 375).
3. Démarrez ou redémarrez le service **Websense Network Agent**.
4. Fermez TRITON - Web Security.
5. Attendez une minute avant de vous reconnecter à TRITON - Web Security.

Si le problème n'est toujours pas résolu :

- Regardez dans l'**Observateur d'événements de Windows** si des messages d'erreur sont liés au service Network Agent (voir *Observateur d'événements de Windows*, page 516).
- Regardez dans le fichier **Websense.log** si des messages d'erreur sont liés au service Network Agent (voir *Fichier journal Websense*, page 516).

Network Agent ne surveille aucune carte réseau

Pour surveiller le trafic réseau, Network Agent doit être associé à une carte réseau au moins.

Si vous ajoutez ou retirez des cartes réseau de l'ordinateur Network Agent, vous devez actualiser votre configuration de Network Agent.

1. Dans TRITON - Web Security, sélectionnez **Paramètres**.
2. Dans le panneau de navigation gauche, sous Network Agent, sélectionnez l'adresse IP de l'ordinateur Network Agent.
3. Assurez-vous que toutes les cartes réseau de l'ordinateur sélectionné apparaissent dans la liste.
4. Assurez-vous qu'une carte réseau au moins soit configurée pour surveiller le trafic réseau.

Pour plus d'informations, consultez la section *Configuration de Network Agent*, page 428.

Network Agent ne peut pas communiquer avec Filtering Service

Network Agent doit pouvoir communiquer avec Filtering Service pour imposer vos stratégies d'utilisation d'Internet.

- Avez-vous modifié l'adresse IP de l'ordinateur Filtering Service ou réinstallé Filtering Service ?

  Dans l'affirmative, consultez la section *Mise à jour des informations d'ID unique ou de l'adresse IP de Filtering Service*, page 451.
- L'ordinateur Network Agent contient-il plus de 2 cartes réseau ?

  Dans l'affirmative, consultez la section *Configuration du réseau*, page 427, pour vérifier vos paramètres Websense.
- Avez-vous reconfiguré le commutateur connecté à l'ordinateur Network Agent ?

  Dans l'affirmative, reportez-vous au Centre Installation et déploiement pour vérifier votre configuration matérielle, et à la section *Configuration de Network Agent*, page 428, pour vérifier vos paramètres Websense.

Si aucune de ces solutions ne convient, consultez la section *Configuration des paramètres locaux*, page 430, pour plus d'informations sur l'association entre Network Agent et Filtering Service.

Mise à jour des informations d'ID unique ou de l'adresse IP de Filtering Service

Lorsque Filtering Service a été désinstallé puis réinstallé, Network Agent n'actualise pas automatiquement l'identificateur interne (UID) de Filtering Service. TRITON - Web Security tente alors d'interroger Filtering Service avec l'ancien ID unique, qui n'existe plus.

De même, lorsque vous modifiez l'adresse IP de l'ordinateur Filtering Service, cette modification n'est pas automatiquement enregistrée.

Pour rétablir la connexion à Filtering Service :

1. Ouvrez TRITON - Web Security.

   Un message d'état indique qu'une instance de Network Agent ne peut pas se connecter à Filtering Service.
2. Cliquez sur **Paramètres** en haut du panneau de navigation situé à gauche.
3. Dans le panneau de navigation gauche, sous Network Agent, sélectionnez l'adresse IP de l'ordinateur Network Agent.
4. En haut de la page, sous Définition de Filtering Service, développez la liste **Adresse IP du serveur**, puis sélectionnez l'adresse IP de l'ordinateur Filtering Service.
5. Cliquez sur **OK** en bas de la page pour mettre la mise à jour en cache. Les modifications ne sont pas implémentées tant que vous ne cliquez pas sur **Save and Deploy (Enregistrer et déployer)**.

Mémoire insuffisante dans l'ordinateur Network Agent

Network Agent alloue la mémoire de fonctionnement dont il a besoin au démarrage. Lorsque la mémoire est fortement limitée dans l'ordinateur Network Agent, l'agent :

- Ne peut pas démarrer, ou
- Ne peut pas surveiller le trafic

Dans les deux cas, le filtrage et la journalisation dépendant des informations de Network Agent ne peuvent pas s'effectuer. En conséquence, les utilisateurs peuvent parfois accéder à des sites ou des applications habituellement bloqué(e)s.

Pour évaluer l'utilisation de la mémoire dans l'ordinateur Network Agent, utilisez le Gestionnaire des taches (sous Windows) ou la commande**top** (sous Linux). Pour résoudre ce problème, vous pouvez :

- Augmenter la quantité de mémoire RAM de l'ordinateur
- Déplacer les applications ou les composants qui sollicitent fortement la mémoire vers un autre ordinateur
- Simplifier votre configuration de Network Agent de manière à réduire la quantité de mémoire nécessaire

Utilisation intensive du processeur dans l'ordinateur Network Agent

Lorsque le processeur de l'ordinateur Network Agent est surchargé de demandes issues des autres logiciels en exécution dans cet ordinateur, l'agent est incapable de détecter et de journaliser le trafic. Dans un environnement autonome, cela peut impliquer que toutes les requêtes de sites Web et d'applications Internet effectuées par les utilisateurs sont autorisées, y compris celles qui sont habituellement bloquées.

Pour corriger ce problème, commencez par utiliser le Gestionnaire des taches (Windows) ou la commande **top** (Linux) pour identifier les processus qui sollicitent intensivement le processeur.

- Certaines applications peuvent-elles être exécutées à partir d'un autre ordinateur ?
- Pouvez-vous installer Network Agent dans un ordinateur dédié ?

Problèmes de configuration et d'identification des utilisateurs

- *Non application des stratégies basées sur les utilisateurs et les groupes*, page 453
- *Défaut de communication de Filtering Service avec un agent d'identification transparente*, page 454
- *Autorisations insuffisantes de DC Agent*, page 455
- *Défaut d'accès de DC Agent au fichier requis*, page 456
- *Impossible d'ajouter des utilisateurs et des groupes dans TRITON - Web Security*, page 457
- *User Service sous Linux*, page 461

Non application des stratégies basées sur les utilisateurs et les groupes

Si Websense utilise des stratégies d'ordinateur ou de réseau, ou la stratégie **Par défaut**, pour filtrer les requêtes Internet alors même que des stratégies d'utilisateur ou de groupe ont été attribuées, ou lorsqu'une stratégie d'utilisateur ou de groupe inappropriée est appliquée, procédez comme suit pour cerner le problème :

- Si vous utilisez des groupes imbriqués dans Windows Active Directory, les stratégies attribuées à un groupe parent s'appliquent aux utilisateurs appartenant à un sous-groupe, et non directement au groupe parent. Pour plus d'informations sur la hiérarchie des utilisateurs et des groupes, consultez la documentation de votre service d'annuaire.
- Le cache de User Service peut être obsolète. User Service met en cache les correspondances nom d'utilisateur/adresse IP pendant 3 heures. Pour effacer et recréer le cache, accédez à la section User Service Cache (Cache de User Service) dans la page Paramètres > Général > Services d'annuaire de TRITON - Web Security, puis cliquez sur **Effacer le cache**.
- User Service a pu être installé à l'aide du compte Invité, ce qui correspond pour le contrôleur de domaine à un utilisateur anonyme. Si le contrôleur de domaine a été configuré pour ne pas donner la liste des utilisateurs et des groupes à un utilisateur anonyme, User Service n'est pas autorisé à télécharger cette liste. Voir *Modification des autorisations de DC Agent, Logon Agent et User Service*, page 460.
- Si l'utilisateur qui n'est pas filtré correctement travaille sur un ordinateur fonctionnant sous Windows XP SP2, le problème peut provenir du Pare-feu de connexion Internet (ICF) de Windows, inclus et activé par défaut sous Windows XP SP2. Pour plus d'informations sur le pare-feu Windows ICF, consultez l'Article #320855 de la Base de connaissances de Microsoft.

  Pour que DC Agent ou Logon Agent obtienne les informations de connexion des utilisateurs d'un ordinateur fonctionnant sous Windows XP SP2 :

1. Dans l'ordinateur Client, sélectionnez **Démarrer** > **Paramètres** > **Panneau de configuration** > **Centre de sécurité** > **Pare-feu Windows**.
2. Ouvrez l'onglet **Exceptions**.
3. Activez l'option **Partage de fichiers et d'imprimantes**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue Pare-feu de connexion Internet (ICF), puis fermez toutes les autres fenêtres ouvertes.

Si aucune des étapes précédentes ne résout ce problème, consultez les rubriques suivantes ou recherchez des informations supplémentaires sur notre portail support.websense.com.

- *Connectivité et configuration du service d'annuaire*, page 458
- *Configuration du service d'annuaire dans TRITON - Web Security*, page 458
- *Identification des utilisateurs et Windows Server 2008*, page 459

Défaut de communication de Filtering Service avec un agent d'identification transparente

Si vous utilisez DC Agent, Logon Agent, eDirectory Agent ou RADIUS Agent pour identifier les utilisateurs en transparence, Filtering Service doit pouvoir communiquer avec l'agent pour appliquer correctement les stratégies basées sur les utilisateurs. Lorsque cette communication ne pas être établie, l'utilisateur peut être filtré par une stratégie basée sur l'adresse IP ou par la stratégie Par défaut.

Pour résoudre ce problème :

1. Vérifiez que le service ou le démon de l'agent s'exécute.
   - **Sous Windows** : utilisez la boîte de dialogue Services de Windows pour vérifier que Websense DC Agent, Websense Logon Agent, Websense eDirectory Agent ou Websense RADIUS Agent s'exécute.
   - **Sous Linux** : accédez au répertoire **/opt/Websense/** et servez-vous de la commande suivante pour vérifier que Logon Agent, eDirectory Agent ou RADIUS Agent s'exécute :

     ```
     ./WebsenseAdmin -status
     ```
2. Vous pouvez envoyer une commande **ping** à l'ordinateur de l'agent d'identification transparente à partir de l'ordinateur Filtering Service. Pour vérifier que le système DNS est correctement configuré, essayez l'adresse IP et le nom d'hôte de l'ordinateur de l'agent d'identification transparente. Par exemple :

   ```
   ping 10.55.127.22
   ping transid-host
   ```
3. Le port de communication reliant l'ordinateur de l'agent d'identification transparente et l'ordinateur Filtering Service doit être ouvert. Les ports par défaut sont les suivants :
   - DC Agent : 30600
   - Logon Agent : 30602
   - eDirectory Agent : 30700
   - RADIUS Agent : 30800

4. L'adresse IP ou le nom d'hôte, et le port corrects de l'agent sont indiqués à la page **Paramètres > Général > Identification des utilisateurs** dans TRITON - Web Security.

Si le service semble s'exécuter normalement et qu'il ne semble pas y avoir de problèmes de communication réseau entre l'ordinateur Filtering Service et l'ordinateur de l'agent :

- Servez-vous de la boîte de dialogue Services de Windows ou de la commande / opt/Websense/WebsenseDaemonControl pour redémarrer l'agent.
- Servez-vous de l'Observateur d'événements de Windows (voir *Observateur d'événements de Windows*, page 516) ou du fichier **websense.log** (voir *Fichier journal Websense*, page 516) de l'ordinateur de l'agent pour voir si des messages d'erreur relatifs à l'agent d'identification transparente sont présents.

Autorisations insuffisantes de DC Agent

DC Agent a pu être installé sous forme de service à l'aide du compte Invité, ce qui correspond pour le contrôleur de domaine à un utilisateur anonyme.

Pour effectuer la détection de domaines (dont DC Agent a besoin pour créer et gérer le fichier dc_config.txt) ou pour interroger les ordinateurs, le service Websense DC Agent doit disposer d'autorisations d'**administrateur de domaine**. Dans certains environnements (en général, les très grands réseaux d'entreprise), DC Agent doit disposer des autorisations d'**administrateur d'entreprise**.

Si vous avez désactivé la détection de domaines et l'interrogation des stations de travail et que vous vous contentez d'interroger les contrôleurs de domaine tout en gérant le fichier dc_config.txt manuellement, DC Agent peut s'exécuter comme n'importe quel utilisateur réseau disposant d'accès en lecture sur le contrôleur de domaine.

Pour accorder des privilèges d'administrateur de domaine à DC Agent :

1. Dans l'ordinateur DC Agent, créez un compte d'utilisateur et donnez-lui un nom descriptif, tel que **WsUserID**. Ce compte vise uniquement à fournir un contexte de sécurité à DC Agent lorsqu'il demande des informations au service d'annuaire.
   - Attribuez des privilèges d'**administrateur de domaine** au nouveau compte pour tous les domaines.
   - Affectez le même mot de passe à ce compte dans tous les domaines.
   - Définissez ce mot de passe pour qu'il n'expire jamais.

   Notez ce nom d'utilisateur et son mot de passe.
2. Ouvrez la boîte de dialogue **Services** de Windows (Démarrer > Outils d'administration > Services).
3. Faites défiler l'écran jusqu'au service **Websense DC Agent**, cliquez du bouton droit sur son nom, puis sélectionnez Arrêter.
4. Cliquez de nouveau sur le nom de ce service avec le bouton droit, sélectionnez **Propriétés**, puis ouvrez l'onglet **Connexion**.
5. Sélectionnez **Ce compte** et saisissez le nom du compte et le mot de passe que vous avez créé pour DC Agent. Certains domaines exigent que le nom du compte soit saisi au format domaine\nom d'utilisateur.
6. Cliquez sur **OK** pour revenir à la boîte de dialogue Services.

7. Cliquez de nouveau du bouton droit sur le nom du service, puis choisissez **Démarrer**.
8. Fermez la boîte de dialogue Services.

Il vous faudra peut-être également attribuer les mêmes privilèges d'administration à User Service qu'à DC Agent.

Défaut d'accès de DC Agent au fichier requis

DC Agent fonctionne en identifiant les contrôleurs de domaine du réseau, puis en les interrogeant pour satisfaire les sessions de connexion des utilisateurs. Par défaut, l'agent vérifie automatiquement les contrôleurs de domaine existants et détecte les nouveaux domaines ou contrôleurs de domaine ajoutés dans le réseau. Il stocke alors ces informations dans un fichier intitulé **dc_config.txt**, situé dans le répertoire **bin** de Websense dans l'ordinateur DC Agent.

Une alerte signalant que DC Agent ne peut pas accéder à ce fichier peut s'afficher lorsque :

- DC Agent ne peut pas ouvrir le fichier avec des autorisations en lecture ou en écriture.
  - Assurez-vous que le compte de domaine utilisé pour exécuter DC Agent dispose d'autorisations en lecture et en écriture sur ce fichier et son répertoire.
  - Si le fichier est présent et n'est pas protégé contre l'écriture, assurez-vous de pouvoir l'ouvrir manuellement et qu'il n'est pas corrompu.
- DC Agent ne peut pas créer le fichier, car il ne trouve pas les informations sur les contrôleurs de domaine.
  - Si User Service est installé dans un ordinateur Linux, vérifiez que vous avez effectué la procédure de configuration WINS requise. Pour obtenir des instructions complètes, consultez la section *User Service sous Linux*, page 461.
  - Si User Service est installé dans un ordinateur Windows Server 2008, vérifiez que le service s'exécute avec des identifiants d'**administrateur de domaine**. Voir *Modification des autorisations de DC Agent, Logon Agent et User Service*, page 460.
  - Vérifiez que NetBIOS pour TCP/IP est activé et que les ports NetBIOS (137, 138, 139 et 445), reliant l'ordinateur DC Agent et le contrôleur de domaine, sont ouverts.

    Si User Service s'exécute sous Windows, vérifiez que les ports NetBIOS reliant l'ordinateur User Service et le contrôleur de domaine sont également ouverts.
  - Vérifiez que le service Explorateur d'ordinateur s'exécute dans tous les ordinateurs Windows 2008 Server qui hébergent DC Agent, User Service ou Active Directory. Voir *Activation du service Explorateur d'ordinateur*, page 459.
- DC Agent ne trouve pas d'entrées valide dans le fichier.
  - Vérifiez qu'une entrée de contrôleur de domaine au moins est activée dans le fichier. Si toutes les entrées sont désactivées, DC Agent a en fait reçu l'ordre de cesser de fonctionner.

- Vérifiez que le format de toutes les entrées du fichier est valide. Par exemple :

```
[WEST_DOMAIN]
dcWEST1=on
dcWEST2=on
[EAST_DOMAIN]
dcEAST1=on
dcEAST2=off
```

Page des domaines et des contrôleurs de DC Agent vide

Par défaut, DC Agent effectue automatiquement une **détection de domaines** afin d'identifier les contrôleurs de domaine du réseau. Les informations relatives aux domaines et aux contrôleurs sont stockées dans un fichier nommé **dc_config.txt**. Les informations issues du fichier dc_config.txt sont récupérées et affichées dans la page Paramètres > Identification des utilisateurs > DC Agent Domains and Controllers (Domaines et contrôleurs de DC Agent) dans TRITON - Web Security.

Cette page peut afficher un texte d'erreur uniquement dans les cas suivants :

- DC Agent a été installé récemment et la détection de domaines est encore en cours.
- Un administrateur a modifié le fichier **dc_config.txt** pour désactiver l'interrogation de tous les contrôleurs de domaine du réseau.
- Un élément empêche DC Agent d'effectuer la détection de domaines.

Assurez-vous que :

- La détection de domaines de DC Agent est activée dans la page **Paramètres > Identification des utilisateurs > DC Agent** de chaque instance de DC Agent installée dans votre réseau.
- DC Agent a eu suffisamment de temps pour terminer sa détection de domaines.
- Aucune alerte de DC Agent ne s'affiche dans la page État > Alertes.

Si une alerte de DC Agent s'affiche, consultez les sections *Autorisations insuffisantes de DC Agent*, page 455, et *Défaut d'accès de DC Agent au fichier requis*, page 456. Les instructions de ces articles permettent de vérifier que DC Agent dispose des autorisations requises et peut accéder au réseau pour effectuer la détection des domaines et créer le fichier dc_config.txt.

Impossible d'ajouter des utilisateurs et des groupes dans TRITON - Web Security

Divers problèmes peuvent vous empêcher d'afficher la liste des utilisateurs et des groupes lorsque vous tentez d'ajouter des clients dans TRITON - Web Security. Pour plus d'informations, consultez les rubriques suivantes et la Base de connaissances.

- *Connectivité et configuration du service d'annuaire*, page 458
- *Configuration du service d'annuaire dans TRITON - Web Security*, page 458
- *Identification des utilisateurs et Windows Server 2008*, page 459

Connectivité et configuration du service d'annuaire

Vérifiez que l'ordinateur Websense User Service et votre serveur d'annuaire s'exécutent et peuvent communiquer via le réseau. Les ports utilisés par défaut pour la communication avec le service d'annuaire sont les suivants :

139	Communication NetBIOS : Active Directory
389	Communication LDAP : Active Directory, Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
636	Port SSL : Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
3268	Active Directory
3269	Port SSL : Active Directory

Par ailleurs, tenez compte des éléments suivants :

- Si vous utilisez Windows Active Directory en mode **mixte** et que User Service s'exécute dans un ordinateur Windows Server 2008, le compte utilisé pour exécuter User Service doit disposer de privilèges d'administrateur sur l'annuaire. Cet élément est également requis pour d'autres versions de Windows Server.

  Pour vérifier ou modifier le compte User Service, consultez la section *Modification des autorisations de DC Agent, Logon Agent et User Service*, page 460.
- Si vous exécutez Active Directory en mode **natif**, définissez User Service de sorte qu'il s'exécute en tant que compte Système local. Aucun compte ne doit être affecté au véritable service.

  User Service se connecte à l'annuaire avec le nom d'utilisateur et le mot de passe d'administrateur configurés dans la page Paramètres > Général > Services d'annuaire > Ajouter un serveur de catalogue global de TRITON - Web Security.
- Si vous exécutez User Service dans un ordinateur Linux qui communique avec un service d'annuaire de type Windows, consultez la section *User Service sous Linux*, page 461, pour obtenir d'autres instructions.
- Vérifiez qu'un pare-feu ne bloque pas la communication établie entre TRITON - Web Security et User Service sur le port 55815. Au besoin, ouvrez le port bloqué.

Configuration du service d'annuaire dans TRITON - Web Security

Si vous rencontrez des problèmes lorsque vous ajoutez des utilisateurs et des groupes dans TRITON - Web Security, assurez-vous d'avoir fourni des informations de configuration complètes et précises sur votre service d'annuaire.

1. Sélectionnez Paramètres > Général > Services d'annuaire.
2. Sélectionnez le service d'annuaire utilisé par votre organisation.
3. Vérifiez sa configuration. Pour plus d'informations, consultez la section *Services d'annuaire*, page 75, et ses sous-rubriques.

Si Websense User Service est installé dans un ordinateur Linux et est configuré pour communiquer avec Active Directory, consultez la section *User Service sous Linux*, page 461, pour plus d'informations sur la configuration requise.

Identification des utilisateurs et Windows Server 2008

L'ajout d'utilisateurs et de groupes dans TRITON - Web Security pose parfois des problèmes si vous avez installé un ou plusieurs des composants Windows Server 2008 suivants :

- Websense User Service
- Windows Active Directory

Si votre réseau utilise Active Directory en mode mixte, le service Explorateur d'ordinateur de Windows doit s'exécuter sur l'ordinateur dans lequel User Service est installé, ainsi que sur l'ordinateur qui exécute Active Directory 2008. Par défaut, ce service est activé dans les versions précédentes de Windows. Il est toutefois désactivé par défaut sous Windows Server 2008.

Par ailleurs, lorsque User Service est installé sous Windows Server 2008 et que vous utilisez Active Directory en mode mixte, vous devez configurer User Service avec des droits de domaine pour qu'il puisse accéder aux informations d'Active Directory.

Si vous exécutez User Service sous Linux et que vous utilisez Active Directory 2008, une configuration supplémentaire est requise. Voir *User Service sous Linux*, page 461.

Pour activer le service Explorateur d'ordinateur dans l'ordinateur approprié, consultez la section *Activation du service Explorateur d'ordinateur*, page 459.

Pour configurer User Service pour qu'il puisse accéder aux informations de l'annuaire, consultez la section *Modification des autorisations de DC Agent, Logon Agent et User Service*, page 460.

Activation du service Explorateur d'ordinateur

La configuration de Websense permet d'activer le service Explorateur d'ordinateur lors de l'installation des composants suivants sous Windows Server 2008.

- Websense User Service
- Websense DC Agent
- Websense Logon Agent

Si vous avez choisi de ne pas le démarrer ou si le programme d'installation a rencontré un problème, vous devez activer ce service manuellement.

Exécutez la procédure suivante dans chaque ordinateur exécutant un composant affecté :

1. Vérifiez que le Partage de fichier réseau est bien activé dans Windows.
   a. Sélectionnez **Démarrer** > **Réseau**, puis cliquez sur **Centre Réseau et partage**.
   b. Cliquez sur **Paramètres de partage avancés** et activez l'option **Partage de fichiers et d'imprimantes**.

2. Sélectionnez **Panneau de configuration** > **Outils d'administration** > **Services**.
3. Double-cliquez sur **Explorateur d'ordinateur** pour ouvrir la boîte de dialogue Propriétés.
4. Définissez le type de démarrage sur **Manuel**.
5. Cliquez sur **Démarrer**.
6. Remplacez le type de démarrage par **Automatique**. Vous serez ainsi certain que le service démarrera automatiquement chaque fois que l'ordinateur redémarre.
7. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue Services.
8. Reprenez cette procédure dans chaque ordinateur exécutant Windows Server 2008 et un composant affecté.

Modification des autorisations de DC Agent, Logon Agent et User Service

DC Agent, Logon Agent et User Service ont parfois besoin de s'exécuter en tant que compte autorisé à accéder au service d'annuaire.

1. Dans l'ordinateur qui exécute le contrôleur de domaine, créez un compte d'utilisateur, par exemple **Websense**. Vous pouvez utiliser un compte existant, mais un compte Websense est préférable car il vous permet de définir le mot de passe pour qu'il n'expire pas. Aucun privilège spécial n'est nécessaire.

   Définissez le mot de passe pour qu'il n'expire jamais. Ce compte fournit uniquement un contexte de sécurité pour l'accès aux objets de l'annuaire.

   Notez le nom d'utilisateur et le mot de passe définis pour ce compte, car ils seront nécessaires aux étapes 6 et 7.
2. Dans l'ordinateur qui exécute un composant affecté, sélectionnez **Démarrer** > **Programmes** > **Outils d'administration** > **Services**.
3. Sélectionnez l'entrée du service Websense appropriée (répertoriée ci-dessous), puis cliquez sur **Arrêter**.
   - Websense DC Agent
   - Websense Logon Agent
   - Websense User Service
4. Double-cliquez sur l'entrée du service Websense.
5. Dans l'onglet **Connexion**, sélectionnez l'option **Ce compte**.
6. Entrez le nom d'utilisateur du compte Websense créé à l'étape 1. Par exemple : **NomDomaine\websense**.
7. Entrez et confirmez le mot de passe Windows de ce compte.
8. Cliquez sur **OK** pour refermer la boîte de dialogue.
9. Sélectionnez l'entrée du service Websense dans la boîte de dialogue Services, puis cliquez sur **Démarrer**.
10. Reprenez cette même procédure pour chaque instance de Websense DC Agent, Logon Agent et User Service présente dans votre réseau.

User Service sous Linux

Si vous envisagez d'appliquer des stratégies de filtrage aux utilisateurs individuels et aux groupes de votre réseau, une procédure de configuration spéciale est requise pour s'assurer que Websense peut correctement identifier les utilisateurs dans les réseaux qui exécutent Websense User Service sur un serveur Linux et l'un des éléments suivants :

- Utilisation d'Active Directory en mode mixte
- Utilisation envisagée de Websense Logon Agent pour l'identification transparente des utilisateurs via Active Directory en mode natif
- Utilisation de DC Agent pour l'identification transparente des utilisateurs

Dans ces environnements, Websense doit être configuré pour communiquer avec un serveur WINS (Windows Internet Name Server) pour convertir les noms de domaine en adresses IP de contrôleur de domaine. La procédure exacte dépend de votre environnement.

Si votre réseau utilise Windows Active Directory en mode mixte :

1. Dans TRITON - Web Security, ouvrez la page **Paramètres > Général > Services d'annuaire**.
2. Sélectionnez **Windows Active Directory (Mode mixte)**. Il s'agit là de l'option par défaut.
3. Entrez le nom et le mot de passe de l'utilisateur administrateur.
4. Saisissez le nom du **Domaine**.

   Si votre organisation utilise plusieurs domaines, saisissez le nom d'un domaine approuvé par tous les domaines qui authentifient vos utilisateurs.
5. Entrez l'adresse IP d'un serveur WINS (Windows Internet Name Server) capable de convertir le nom de domaine saisi ci-dessus en adresse IP de contrôleur de domaine.
6. 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)**.

Si votre réseau utilise Active Directory (Mode natif) et que vous devez configurer les paramètres WINS :

1. Ouvrez la page **Paramètres > Général > Services d'annuaire**.
2. Fournissez des identifiants d'administrateur et identifiez le serveur WINS (Windows Internet Name Server), comme suit.
   a. Sélectionnez **Windows Active Directory (Mode mixte)** (option par défaut).
   b. Entrez le nom et le mot de passe de l'utilisateur administrateur.
   c. Saisissez le nom du **Domaine**.

      Si votre organisation utilise plusieurs domaines, saisissez le nom d'un domaine approuvé par tous les domaines qui authentifient vos utilisateurs.

d. Entrez l'adresse IP d'un serveur WINS (Windows Internet Name Server) capable de convertir le nom de domaine saisi ci-dessus en adresse IP de contrôleur de domaine.

e. Cliquez sur **OK** pour mettre vos modifications en cache.

f. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter ces modifications.

3. Dans la page Services d'annuaire, sélectionnez **Active Directory (Mode natif)**.
4. Configurez les serveurs de catalogue global et les autres paramètres de votre service d'annuaire. Pour obtenir de l'aide, consultez la section *Windows Active Directory (en mode natif)*, page 76.
5. 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)**.

Utilisateurs distants non invités à s'authentifier manuellement

Si vous avez configuré les utilisateurs distants de sorte qu'ils s'authentifient manuellement lorsqu'ils accèdent à Internet, il peut arriver que certains d'entre eux ne soient pas invités à s'authentifier. Cela se produit lorsque des adresses IP du réseau ont été configurées pour ignorer l'authentification manuelle.

Lorsqu'un utilisateur distant accède au réseau, Websense lit la dernière partie de l'adresse MAC (Media Access Control) de son ordinateur. Si celle-ci correspond à une adresse IP du réseau configurée pour ignorer l'authentification manuelle, l'utilisateur distant n'est pas invité à s'authentifier manuellement lorsqu'il accède à Internet.

La solution consiste à reconfigurer l'adresse IP réseau pour qu'elle utilise l'authentification manuelle. Une autre solution consiste à désactiver l'authentification manuelle pour l'utilisateur distant concerné.

Filtrage incorrect des utilisateurs distants

Lorsque certains utilisateurs distants ne sont pas filtrés, ou ne sont pas filtrés par les stratégies qui leur sont attribuées, recherchez dans les journaux de RADIUS Agent le message **Error receiving from server: 10060** (sous Windows) ou **Error receiving from server: 0** (sous Linux).

Cela se produit généralement lorsque le serveur RADIUS ne reconnaît pas RADIUS Agent comme un client (source des requêtes RADIUS). Vérifiez que votre serveur RADIUS est correctement configuré (reportez-vous au document technique Using RADIUS Agent for Transparent User Identification (Utilisation de RADIUS Agent pour l'identification transparente des utilisateurs)).

Si vous avez installé un logiciel de filtrage à distance (voir *Filtrage des utilisateurs hors site*, page 237), les utilisateurs hors site ne peuvent pas être filtrés si le client Remote Filtering ne peut pas communiquer avec le serveur Remote Filtering via le réseau.

Pour obtenir des instructions sur la configuration du logiciel de filtrage à distance, reportez-vous au document technique Remote Filtering Software (Logiciel de filtrage à distance).

Problèmes de messages de blocage

- *Aucune page de blocage affichée pour un type de fichier bloqué*, page 463
- *Erreur du navigateur à la place de la page de blocage*, page 463
- *Affichage d'une page blanche à la place de la page de blocage*, page 464
- *Défaut d'affichage des messages de blocage de protocoles*, page 464
- *Affichage d'un message de blocage de protocole à la place de la page de blocage*, page 465

Aucune page de blocage affichée pour un type de fichier bloqué

Lorsque le blocage de types de fichiers est utilisé, le message de blocage n'est pas toujours visible pour l'utilisateur. Par exemple, lorsqu'un fichier téléchargeable fait partie d'une trame interne (iframe) dans un site autorisé, le message de blocage envoyé à cette trame n'est pas visible car la taille de la trame est égale à zéro.

Le problème provient uniquement de l'affichage. L'utilisateur ne peut pas accéder au fichier bloqué ni le télécharger.

Erreur du navigateur à la place de la page de blocage

Si les utilisateurs reçoivent un message d'erreur à la place d'une page de blocage, les deux causes les plus probables sont les suivantes :

- Le navigateur de l'utilisateur est configuré pour utiliser un proxy externe. La plupart des navigateurs permettent d'utiliser un proxy externe. Assurez-vous que le navigateur n'est pas configuré avec cette option.
- Il existe un problème d'identification ou de communication avec l'ordinateur Filtering Service.

Si les paramètres du navigateur de l'utilisateur sont corrects, vérifiez que l'adresse IP de l'ordinateur Filtering Service est correctement répertoriée dans le fichier **eimserver.ini**.

1. Arrêtez **Websense Filtering Service** (voir *Arrêt et démarrage des services Websense*, page 375).
2. Accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).
3. Ouvrez le fichier **eimserver.ini** dans un éditeur de texte.
4. Sous **[WebsenseServer]**, insérez une ligne vide, puis entrez :

   ```
   BlockMsgServerName = <Adresse IP de Filtering Service>
   ```

   Par exemple, si l'adresse IP de Filtering Service est 10.201.72.15, entrez :

   ```
   BlockMsgServerName = 10.201.72.15
   ```
5. Enregistrez et fermez le fichier.
6. Redémarrez Filtering Service.

Si l'ordinateur Filtering Service a plusieurs cartes réseau et que la page de blocage ne s'affiche toujours pas correctement après la modification du fichier **eimserver.ini**, tentez d'utiliser les adresses IP des autres cartes réseau pour le paramètre **BlockMsgServerName**.

Si la page de blocage ne s'affiche toujours pas, assurez-vous que les utilisateurs puissent accéder en lecture aux fichiers des répertoires de pages de blocage dans Websense :

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

Si ce problème de page de blocage persiste, recherchez d'autres conseils de dépannage sur notre portail support.websense.com.

Affichage d'une page blanche à la place de la page de blocage

Lorsque des publicités sont bloquées, ou lorsqu'un navigateur ne reconnaît pas correctement le codage associé à une page de blocage, l'utilisateur peut recevoir une page blanche à la place de la page de blocage. Les causes potentielles de ce problème sont les suivantes :

- Lorsque la catégorie Publicités est bloquée, Websense confond parfois les requêtes de fichier graphique avec les requêtes de publicité, et affiche alors une image vierge à la place du message de blocage (méthode habituelle de blocage des publicités). Si l'URL demandée se termine par .gif ou toute autre extension similaire, l'utilisateur doit la saisir une nouvelle fois en ignorant la partie *.gif. Voir *Blocage des publicités graphiques*, page 117.
- Certains navigateurs plus anciens peuvent ne pas reconnaître le codage des pages de blocage. Pour que les caractères soient correctement reconnus, configurez votre navigateur pour qu'il affiche le jeu de caractères approprié (UTF-8 pour le français, l'allemand, l'italien, l'espagnol, le Brésilien, le portugais, le chinois simplifié, le chinois traditionnel ou le coréen ; et Shift_JIS pour le japonais). Consultez la documentation de votre navigateur pour obtenir des instructions, ou mettez-le à niveau avec une version plus récente.

Défaut d'affichage des messages de blocage de protocoles

Les messages de blocage de protocoles peuvent ne pas apparaître, ou apparaître après un certain délai, pour les raisons suivantes :

- Pour que les messages de blocage de protocoles s'affichent correctement, User Service doit être installé dans un ordinateur Windows. Pour plus d'informations, consultez le Centre Installation et déploiement.
- Les messages de blocage de protocoles peuvent ne pas atteindre les ordinateurs clients si Network Agent est installé dans un ordinateur équipé de plusieurs cartes réseau et que l'une d'elles ne surveille pas le même segment réseau que Filtering Service. Vérifiez que l'ordinateur Filtering Service dispose d'un accès aux ordinateurs clients par les protocoles NetBIOS et SMB (Server Message Block), et que le port 15871 n'est pas bloqué.

- Un message de blocage de protocole peut être légèrement retardé ou apparaître sur un ordinateur interne d'où proviennent les données de protocole demandées (et non sur l'ordinateur client), lorsque Network Agent est configuré pour surveiller les requêtes **envoyées** aux ordinateurs internes.
- Si le client filtré ou l'ordinateur de filtrage Websense exécute Windows 200x, le service Windows **Messenger** doit s'exécuter pour que le message de blocage de protocole s'affiche. Dans la boîte de dialogue Services de Windows de l'ordinateur client ou du serveur, vérifiez que le service Messenger s'exécute (voir *Boîte de dialogue Services de Windows*, page 515). Même si le message de blocage ne s'affiche pas, les demandes de protocole restent bloquées.

Affichage d'un message de blocage de protocole à la place de la page de blocage

Si votre produit d'intégration n'envoie pas d'informations HTTPS à Websense, ou si Websense s'exécute en mode autonome, Network Agent peut confondre une requête de site HTTPS bloquée par les paramètres des catégories avec une requête de protocole. Par conséquent, un message de blocage de protocole apparaît. La requête HTTPS est également journalisée en tant que requête de protocole.

Problèmes liés aux journaux, aux messages d'état et aux alertes

- *Où puis-je trouver les messages d'erreur liés aux composants de Websense ?*, page 466
- *Alertes d'état de Websense*, page 466
- *Génération de deux enregistrements de journal pour une seule requête*, page 468
- *Usage Monitor indisponible*, page 469
- *Non exécution d'Usage Monitor*, page 469

Où puis-je trouver les messages d'erreur liés aux composants de Websense ?

Lorsque des erreurs ou des avertissements sont liés aux principaux composants de Websense, des messages d'alerte s'affichent dans la page **État > Alertes** de TRITON - Web Security. De plus, par défaut, de brefs messages d'alerte s'affichent dans la liste **Résumé sur les alertes d'état** en haut de l'onglet Système de la page **État > Tableau de bord** (voir *Alertes d'état de Websense*, page 466).

- Cliquez sur le résumé d'une alerte dans le tableau de bord pour afficher ses informations détaillées dans la page État > Alertes.
- Cliquez sur **Solutions** à côté d'un message de la page État > Alertes pour obtenir de l'aide au dépannage.

Les erreurs, les avertissements et les messages provenant des composants de Websense, ainsi que les messages d'état du téléchargement de la base de données, sont stockés dans le fichier **websense.log** du répertoire **bin** de Websense (voir *Fichier journal Websense*, page 516).

Dans le cas de composants Websense installés dans des ordinateurs Windows, vous pouvez également consulter l'Observateur d'événements de Windows. Voir *Observateur d'événements de Windows*, page 516.

Alertes d'état de Websense

Par défaut, l'onglet Système du Tableau de bord Web Security présente un **Résumé sur les alertes d'état** qui répertorie les problèmes éventuellement rencontrés par composant surveillé par votre logiciel Websense. Cela comprend :

- La base de données du filtrage initial est utilisée.
- La base de données principale est téléchargée pour la première fois.
- La base de données principale date de plus d'une semaine.
- WebCatcher n'est pas disponible.
- Log Server n'est pas en cours d'exécution.
- Le planificateur des rapports de présentation n'est pas connecté à la base de données d'activité.
- La tâche ETL de la base de données d'activité n'a pas pu être effectuée depuis 4 heures.
- Log Server n'est pas en cours d'exécution.
- Espace disque faible dans l'ordinateur Log Server
- Une mise à jour de la base de données principale est en cours.
- Le téléchargement de la base de données principale a échoué.
- Espace disque faible dans l'ordinateur TRITON - Web Security
- La base de données d'activité n'est pas disponible.
- Une ou plusieurs taches de rapport de présentation ont échoué.
- Aucun Log Server n'est configuré pour un serveur Policy Server.
- La base de données d'activité n'est pas disponible.
- Le répertoire du cache de Log Server contient plus de 100 fichiers en cache.

- Log Server n’a pas reçu les données de Filtering Service depuis plus d’une heure.
- Aucune carte réseau de surveillance n’est configurée pour un agent Network Agent.
- Mémoire faible dans l’ordinateur Network Agent
- Filtering Service n’est pas actif.
- Espace disque faible dans l’ordinateur Filtering Service
- Utilisation intensive du processeur dans l’ordinateur Filtering Service
- DC Agent ne dispose pas des autorisations suffisantes.
- Filtering Service ne peut pas communiquer avec Logon Agent.
- Filtering Service ne peut pas communiquer avec eDirectory Agent.
- Usage Monitor ne s’exécute pas.
- L’emplacement du référentiel d’analyse n’est pas accessible.
- Un problème de configuration interfère avec la collecte des données d’analyse des menaces.
- Aucun Filtering Service n’est configuré pour un agent Network Agent.
- Utilisation intensive du processeur dans l’ordinateur Network Agent
- Aucun Network Agent n’est configuré pour un serveur Policy Server.
- Network Agent n’est pas en cours d’exécution.
- Mémoire faible dans l’ordinateur Filtering Service
- Une instance de DC Agent ne parvient pas à accéder à un fichier requis.
- Filtering Service ne peut pas communiquer avec DC Agent.
- Filtering Service ne peut pas communiquer avec RADIUS Agent.
- Usage Monitor n’est pas disponible.
- Le référentiel d’analyse a atteint 90 % de sa taille maximale.
- La suppression de certains enregistrements du référentiel d’analyse est programmée d’ici une semaine.

Si vous êtes abonné à Websense Web Security Gateway ou Gateway Anywhere, Websense surveille Content Gateway pour envoyer des alertes sur les conditions suivantes :

- Content Gateway ne s’exécute pas.
- Content Gateway n’est pas disponible.

Si vous êtes abonné à Websense Web Security Gateway Anywhere, ou si votre abonnement comprend à la fois des composants de sécurité du Web et des données, Websense surveille l’interopérabilité des composants pour envoyer des alertes sur les conditions suivantes :

- Une instance de Sync Service ne s’exécute pas.
- Aucune instance de Sync Service n’est associée à une instance de Policy Server.
- Les composants sur site ne parviennent pas à se connecter au service hybride.
- Des informations requises pour activer le filtrage hybride sont absentes.
- Une instance de Directory Agent ne s’exécute pas.
- Aucune instance de Directory Agent n’est associée à une instance de Policy Server.

- L'espace disque est faible dans la partition qui héberge Sync Service.
- 24 heures se sont écoulées depuis que Sync Service a téléchargé les fichiers journaux du service hybride.
- Le service hybride a envoyé des alertes.
- 24 heures se sont écoulées depuis que Sync Service a envoyé des fichiers journaux à Log Server.

L'icône accolée au message d'alerte définit l'impact potentiel de la condition associée.

Le message est informatif et ne reflète pas le problème de votre installation (par exemple, WebCatcher n'est pas activé ou Filtering Service télécharge une mise à jour de la base de données principale).

La condition d'alerte peut éventuellement se transformer en problème, mais ne gênera pas tout de suite le filtrage ni la génération des rapports (par exemple, la base de données principale a plus d'une semaine ou la clé d'abonnement est sur le point d'expirer).

Un composant Websense ne fonctionne pas (n'a pas été configuré ou ne s'exécute pas), ce qui peut gêner le filtrage ou la génération des rapports, ou votre abonnement est arrivé à expiration.

Cliquez sur un message d'alerte dans le résumé sur les alertes d'état pour ouvrir la page État > Alertes et obtenir d'avantage d'informations sur les conditions d'alerte actuelles. Cliquez sur **En savoir plus** (pour les alertes informatives) ou sur **Solutions** (pour les erreurs et les avertissements) pour obtenir davantage de détails et des conseils de dépannage.

Lorsqu'une Alerte d'état indique que le service hybride a envoyé des messages, consultez le tableau Hybrid Filtering Alerts (Alertes du filtrage hybride) pour obtenir davantage de détails.

Dans certains cas, si vous recevez des messages d'erreur ou d'état relatifs à un composant que vous n'utilisez pas ou que vous avez désactivé, vous pouvez choisir de masquer les messages d'alerte. Pour plus d'informations, consultez la section *Vérification de l'état actuel du système*, page 385.

Génération de deux enregistrements de journal pour une seule requête

Lorsque le Planificateur de paquets QoS de Windows est installé dans le même ordinateur que Network Agent, deux requêtes sont journalisées pour chaque requête HTTP ou de protocole provenant de l'ordinateur Network Agent. (Cette duplication ne se produit pas avec les requêtes provenant des ordinateurs clients de votre réseau.)

Pour résoudre ce problème, désactivez le Planificateur de paquets QoS de Windows dans l'ordinateur Network Agent.

Ce problème ne se produit pas si vous utilisez Network Agent pour toutes les journalisations. Pour plus d'informations, consultez la section *Configuration des paramètres des cartes réseau*, page 431.

Usage Monitor indisponible

Pour activer les alertes d'utilisation decatégories et de protocoles et Real-Time Monitor, vous devez avoir installé le composant Websense Usage Monitor. En général, une seule instance d'Usage Monitor est installée pour chaque serveur Policy Server de votre réseau. Usage Monitor peut être installé dans l'ordinateur Policy Server.

Lorsque vous installez le composant Usage Monitor, assurez-vous qu'il peut communiquer avec :

- Policy Server sur les ports 55806 et 40000
- Policy Broker sur le port 55880
- Filtering Service et Real-Time Monitor sur le port 55809

Usage Monitor doit également pouvoir recevoir des informations de Policy Server et Filtering Service sur son port d'écoute : 55813.

Non exécution d'Usage Monitor

Lorsque Websense Usage Monitor est arrêté :

- Les informations d'accès aux catégories et aux protocoles ne peuvent pas être collectées en vue de la génération d'alertes.
- Les alertes d'utilisation de catégories et de protocoles ne peuvent pas être générées.
- Real-Time Monitor ne reçoit pas les données de l'activité Internet.

Pour démarrer Usage Monitor :

- Sous Windows : ouvrez la boîte de dialogue Services de Windows, parcourez l'écran jusqu'à Websense Usage Monitor, cliquez du bouton droit sur ce service, puis sélectionnez **Démarrer**.
- Sous Linux : servez-vous de la commande **/opt/Websense/WebsenseDaemonControl**.

Si Usage Monitor ne démarre pas, consultez l'Observateur d'événements de Windows ou le fichier **websense.log** pour obtenir des informations sur l'erreur du service.

Problèmes liés à Policy Server et à la base de données des stratégies

- *Oubli du mot de passe*, page 470
- *Non démarrage du service Websense Policy Database*, page 470
- *Arrêt inopiné de Policy Server*, page 471

Oubli du mot de passe

Si vous êtes Super administrateur ou administrateur délégué et que vous utilisez un compte local pour vous connecter à TRITON Unified Security Center, tout administrateur de sécurité globale peut réinitialiser le mot de passe. Les Super administrateurs globaux peuvent gérer les comptes et les mots de passe via la page Paramètres > Administrateurs dans TRITON.

Lorsque aucun Super administrateur global n'est disponible, les administrateurs qui utilisent des comptes locaux peuvent demander un nouveau mot de passe via le lien **Mot de passe oublié** de la page de connexion de TRITON.

- Un mot de passe temporaire est alors envoyé à l'adresse électronique associée à votre compte d'administrateur.
- Ce mot de passe temporaire est valide pendant 30 minutes seulement. Si vous laissez s'écouler plus de 30 minutes avant de tenter de vous connecter avec ce mot de passe temporaire, vous devrez redemander un nouveau mot de passe.
- Dès que vous vous connectez à l'aide du mot de passe temporaire, vous êtes invité à saisir un nouveau mot de passe.

Non démarrage du service Websense Policy Database

Le service Websense Policy Database s'exécute en tant que compte spécial : **WebsenseDBUser**. Si ce compte rencontre des problèmes de connexion, la base de données des stratégies ne peut pas démarrer.

Pour résoudre ce problème, modifiez le mot de passe du compte WebsenseDBUser.

1. Ouvrez une session dans l'ordinateur Policy Database avec des droits d'administrateur local.
2. Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Gestion de l'ordinateur**.
3. Dans le panneau de navigation, sous Outils système, développez **Utilisateurs et groupes locaux**, puis sélectionnez **Utilisateurs**. Les informations de l'utilisateur apparaissent dans le panneau de contenu.
4. Cliquez du bouton droit sur **WebsenseDBUser** et sélectionnez **Définir le mot de passe**.
5. Entrez et confirmez le nouveau mot de passe de ce compte d'utilisateur, puis cliquez sur **OK**.
6. Fermez la boîte de dialogue Gestion de l'ordinateur.
7. Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Services**.
8. Cliquez du bouton droit sur **Websense Policy Database** et choisissez **Propriétés**.
9. Dans l'onglet Connexion de la boîte de dialogue Propriétés, entrez les nouvelles informations du mot de passe WebsenseDBUser, puis cliquez sur **OK**.
10. Cliquez de nouveau du bouton droit sur Websense Policy Database et sélectionnez **Démarrer**.

    Lorsque le service a démarré, fermez la boîte de dialogue Services.

Arrêt inopiné de Policy Server

Lorsque le disque dur de l'ordinateur Policy Server n'a plus d'espace disque, le service ou le démon Websense Policy Server s'arrête. Même si le manque d'espace disque résulte d'une condition temporaire (par exemple, une autre application crée de volumineux fichiers temporaires, puis les supprime), Policy Server ne redémarre pas automatiquement.

- Si Filtering Service ou Network Agent est installé dans l'ordinateur Policy Server, un message d'alerte d'état de TRITON - Web Security affichera un avertissement pour indiquer que l'espace disque commence à manquer.
- Lorsque Policy Server s'arrête, un message d'alerte d'état s'affiche dans TRITON - Web Security.

Redémarrez manuellement Policy Server pour corriger ce problème immédiatement. Identifiez ensuite l'application qui consomme la totalité de l'espace disponible dans cet ordinateur. Vous pourrez alors déterminer si la meilleure solution consiste à déplacer cette application vers un autre ordinateur ou à ajouter de l'espace disque dans l'ordinateur Policy Server.

Problèmes d'administration déléguée

- *Les clients gérés ne peuvent pas être supprimés de leur rôle.*, page 471
- *Erreur de connexion indiquant que quelqu'un d'autre est connecté à mon ordinateur*, page 472
- *Sites recatégorisés non filtrés par la catégorie appropriée*, page 472
- *Impossible de créer un protocole personnalisé*, page 472

Les clients gérés ne peuvent pas être supprimés de leur rôle.

Les clients ne peuvent pas être supprimés directement de la liste des clients gérés dans la page Administration déléguée >Modifier le rôle, dans les cas suivants :

- L'administrateur a appliqué une stratégie au client.
- L'administrateur a appliqué une stratégie à un ou plusieurs membres d'un réseau, d'un groupe, d'un domaine ou d'une unité d'organisation.

Des problèmes peuvent également survenir si, lors de la connexion à TRITON - Web Security, le Super administrateur choisit un autre serveur Policy Server que celui qui communique avec le service d'annuaire contenant les clients à supprimer. Dans ce cas, le serveur Policy Server actif et le service d'annuaire ne reconnaissent pas les clients.

Pour plus d'informations sur la suppression de clients gérés, consultez la section *Suppression de clients gérés*, page 345.

Erreur de connexion indiquant que quelqu'un d'autre est connecté à mon ordinateur

Lorsque vous tentez de vous connecter à TRITON - Web Security, il peut arriver que vous receviez l'erreur « Échec de la connexion. Le rôle *nom_du_rôle* est utilisé par *nom_d'utilisateur*, depuis *date*, *heure*, sur l'ordinateur 127.0.0.1 ». L'adresse IP 127.0.0.1 est également appelée adresse de bouclage et désigne généralement l'ordinateur local.

Ce message signifie que quelqu'un est connecté à l'ordinateur d'installation de TRITON - Web Security, dans le rôle même que vous demandez. Vous pouvez alors sélectionner un autre rôle (si vous en administrez plusieurs), vous connecter pour la génération de rapports uniquement, ou attendre que l'autre administrateur se déconnecte.

Sites recatégorisés non filtrés par la catégorie appropriée

Les URL recatégorisées n'affectent que les clients gérés par le rôle dans lequel les URL sont ajoutées. Par exemple, si un Super administrateur ajoute des URL recatégorisées, les clients gérés par les rôles d'administration déléguée continuent à être filtrés selon la catégorie Base de données principale pour ces sites.

Pour appliquer la recatégorisation aux clients d'autres rôles, le Super administrateur peut passer à chaque rôle et recatégoriser leurs sites.

Impossible de créer un protocole personnalisé

Seuls les Super administrateurs peuvent créer des protocoles personnalisés. Les administrateurs délégués peuvent cependant définir des actions de filtrage pour les protocoles personnalisés.

Lorsque des Super administrateurs créent des protocoles personnalisés, ils doivent définir l'action par défaut appropriée pour la plupart des clients. Ils doivent ensuite signaler le nouveau protocole aux administrateurs délégués de sorte qu'ils puissent mettre à jour les filtres de leur rôle, le cas échéant.

Problème de Log Server et de la base de données d'activité

- *Non exécution de Log Server*, page 473
- *Non réception par Log Server des fichiers journaux de Filtering Service*, page 474
- *Espace disque faible dans l'ordinateur Log Server*, page 476
- *Aucun Log Server installé pour un serveur Policy Server*, page 477
- *Non création de la base de données d'activité*, page 479
- *Base de données d'activité non disponible*, page 479
- *Taille de la base de données d'activité retardant la génération des rapports*, page 481
- *Plus de 100 fichiers dans le répertoire du cache de Log Server*, page 481
- *Dernière exécution réussie de la tâche ETL depuis plus de 4 heures*, page 483

- *Configuration de Log Server pour l'utilisation d'un compte de base de données*, page 483
- *Aucun enregistrement de Log Server dans la base de données d'activité*, page 484
- *Mise à jour du compte ou du mot de passe de connexion à Log Server*, page 484
- *Configuration des autorisations d'utilisateur pour Microsoft SQL Server*, page 485
- *Problèmes de connexion de Log Server au service d'annuaire*, page 486
- *Affichage d'une page de rapport incorrecte*, page 486

Non exécution de Log Server

Si Log Server ne s'exécute pas, ou si d'autres composants Websense ne peuvent pas communiquer avec Log Server, les informations relatives à l'utilisation d'Internet ne sont pas stockées. Les graphiques de la page **État > Tableau de bord** ne sont plus mis à jour et il est possible que vous ne puissiez plus générer de rapport.

Log Server peut être indisponible dans les cas suivants :

- 20 tentatives ne lui ont pas permis de contacter la base de données d'activité.

  Vérifiez que l'ordinateur de la base de données d'activité est actif, que Microsoft SQL Server fonctionne correctement et que la communication réseau reliant les ordinateurs Log Server et de la base de données d'activité n'a pas été interrompue.
- L'ordinateur Log Server ne dispose pas de suffisamment d'espace disque.

  Vérifiez la quantité d'espace disque disponible dans Log Server et supprimez au besoin les fichiers devenus inutiles.
- Vous avez modifié le mot de passe Microsoft SQL Server sans mettre à jour la connexion ODBC ou Log Server.

  Pour plus d'informations sur la résolution de ce problème, consultez la section *Mise à jour du compte ou du mot de passe de connexion à Log Server*, page 484.
- Il s'est écoulé plus de 14 jours depuis le dernier téléchargement réussi de la base de données principale.

  Pour plus d'informations sur la résolution de ce problème, consultez les sections *Base de données principale âgée de plus d'une semaine*, page 440, et *Échec du téléchargement de la base de données principale*, page 440.
- Le fichier **logserver.ini** est manquant ou corrompu.

  Naviguez jusqu'au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut) et vérifiez que vous pouvez ouvrir le fichier **logserver.ini** dans un éditeur de texte. Si ce fichier est corrompu, remplacez-le par un fichier de sauvegarde.
- Vous avez arrêté Log Server pour éviter la journalisation des informations de l'utilisation d'Internet.

  Ouvrez la boîte de dialogue Services de Windows pour vérifier que Log Server s'exécute et, si nécessaire, redémarrez le service (voir *Arrêt et démarrage des services Websense*, page 375).

Si aucune de ces procédures ne permet de résoudre ce problème, recherchez les messages d'erreur liés à Log Server dans l'Observateur d'événements de Windows et dans le fichier **websense.log** (voir *Conseils et outils de dépannage*, page 515) pour identifier le problème avec plus de précision.

Non réception par Log Server des fichiers journaux de Filtering Service

Log Server reçoit les informations de Filtering Service sur l'utilisation d'Internet et les enregistre dans la base de données d'activité. Lorsque Log Server ne reçoit pas les fichiers de Filtering Service, aucune donnée n'est enregistrée, les données récentes ne s'affichent pas dans la page **État > Tableau de bord** et vous ne pouvez pas générer de rapports incluant des données récentes sur l'utilisation Internet.

Log Server peut ne pas recevoir les fichiers de Filtering Service dans les cas suivants :

- Filtering Service ne s'exécute pas.

  Pour plus d'informations sur la résolution de ce problème, consultez la section *Dysfonctionnement de Filtering Service*, page 446.

- Ces deux services ne peuvent pas communiquer via le réseau.
  - Vérifiez qu'aucune modification n'a été récemment apportée aux règles du pare-feu, susceptibles d'affecter le trafic entre les ordinateurs via le port 55805 (par défaut) ou le port personnalisé qu'utilise votre organisation.
  - Servez-vous d'un utilitaire tel que **telnet** ou **ping** pour vérifier que ces ordinateurs peuvent communiquer.
  - Vérifiez que l'adresse IP et le port (55805, par défaut) de Log Server sont correctement définis dans la page **Paramètres > Général > Journalisation** de TRITON - Web Security.

    Si l'adresse de bouclage (127.0.0.1) ou « localhost » s'affiche, entrez la véritable adresse IP de l'ordinateur Log Server.
  - Servez-vous du bouton **Vérifier l'état** dans la page Paramètres > Général > Journalisation pour vérifier que la connexion à Log Server est possible.

    Si la vérification de l'état échoue :

    a. Assurez-vous qu'aucun pare-feu ne bloque le port.

    b. Exécutez la commande suivante dans l'ordinateur Log Server pour vérifier que Log Server est bien à l'écoute sur le port :

    ```
    netstat -ban > port.txt
    ```

- Network Agent, Content Gateway ou un produit d'intégration tiers n'est pas configuré correctement et ne reçoit pas le trafic Internet.
  - Pour plus d'informations sur la résolution des problèmes de configuration de Network Agent, consultez les sections *Problèmes liés à Network Agent*, page 450 et *Configuration du réseau*, page 427.
  - Pour plus d'informations sur la résolution des problèmes de configuration de Content Gateway, consultez le Centre Installation et déploiement et l'Aide de Content Gateway.
  - Pour plus d'informations sur les autres intégrations prises en charge, consultez le Centre Installation et déploiement et la documentation de votre fournisseur.

- L'espace disque est insuffisant pour que Log Server crée de nouveaux fichiers de cache.

  Pour plus d'informations sur la résolution de ce problème, consultez la section *Espace disque faible dans l'ordinateur Log Server*, page 476.

- Filtering Service est associé à une instance de Policy Server non configurée pour la journalisation ou envoie les journaux à TestLogServer.

Pour plus d'informations sur la résolution de ce problème, consultez les sections *Aucun Log Server installé pour un serveur Policy Server*, page 477 et *Configuration du mode de journalisation des requêtes filtrées*, page 398.

- Impossible d'écrire les fichiers dans le cache ou dans les dossiers BCP.

  Vérifiez que le chemin d'accès défini pour les fichiers du cache ODBC ou les fichiers BCP dans la page **Paramètres > Génération de rapports > Log Server** est correct, et que le compte utilisé pour exécuter Log Server est autorisé à écrire dans cet emplacement.

- Log Server ne s'est pas installé correctement.

  Exécutez la procédure suivante pour vérifier que le service Log Server s'est correctement enregistré auprès du système d'exploitation Windows :

  1. Utilisez la boîte de dialogue Services de Windows pour arrêter le service Websense Log Server.
  2. Ouvrez une invite de commande (**Exécuter > cmd**) et accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut).
  3. Entrez la commande suivante :

     ```
     LogServer .exe -c
     ```

     - Si aucune erreur ne s'affiche, le service est correctement enregistré.
     - Si des erreurs s'affichent, passez à l'étape suivante.
  4. Pour supprimer le service Log Server, entrez :

     ```
     LogServer.exe -u
     ```
  5. Pour enregistrer le programme exécutable, entrez :

     ```
     LogServer.exe -i
     ```
  6. Une fois encore, entrez la commande suivante. Vérifiez qu'aucune erreur ne s'affiche.

     ```
     LogServer .exe -c
     ```

Si aucune des étapes ci-dessus n'a résolu votre problème :

- Vérifiez que la version exécutable de Log Server correspond à la version du produit installé. Pour identifier la version de Log Server :

  1. Ouvrez une invite de commande Windows dans l'ordinateur Log Server.
  2. Accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut).
  3. Entrez la commande suivante :

     ```
     logserver -v
     ```

  La version doit correspondre à celle indiquée à côté de **Web Security build** dans la page **Aide > About the TRITON Console (À propos de la console TRITON)** de TRITON Unified Security Center.

- Il arrive parfois que Filtering Service, lorsqu'il est installé dans un dispositif Websense, ne redémarre pas comme prévu après modification des paramètres. Lorsque l'instance de Filtering Service installée dans un dispositif ne s'exécute plus, ouvrez la page **État > Modules** et redémarrez le module Websense Web Security dans son intégralité.

- Si Log Server cesse de s'exécuter immédiatement après le redémarrage et que l'erreur d'exécution « C error (Visual C Runtime Error) » s'affiche, supprimez le fichier **LogServer.state** présent dans le dossier Log Server **Cache** (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin\Cache, par défaut), puis redémarrez le service **Websense Log Server**.
- Si vous utilisez TestLogServer, vérifiez que cet outil est configuré pour transmettre les données de journal à Log Server.

  Pour plus d'informations sur TestLogServer, consultez notre portail support.websense.com.

Espace disque faible dans l'ordinateur Log Server

Websense Log Server stocke les enregistrements du filtrage Internet dans des fichiers cache de journal temporaires ou dans des fichiers BCP (Bulk Copy Program) de l'ordinateur Log Server jusqu'à leur traitement dans la base de données d'activité.

Websense surveille l'espace disponible pour le stockage des fichiers cache de journal et des fichiers BCP. Par défaut :

- Les fichiers cache de journal sont stockés dans le répertoire **C:\Program Files** ou **Program Files (x86)\Websense\Web Security\bin\Cache**.
- Les fichiers BCP sont stockés dans le répertoire **C:\Program Files** ou **Program Files (x86)\Websense\Web Security\bin\Cache\BCP**.

L'emplacement des fichiers cache de journal et des fichiers BCP peut être modifié dans la page **Paramètres > Génération de rapports > Log Server** de TRITON - Web Security. Voir *Configuration de Log Server*, page 400.

> **Remarque**
> Lorsque plusieurs instances de Log Server transmettent leurs données à l'instance principale de Log Server, l'espace disque n'est surveillé que pour cette dernière uniquement.

Un message d'alerte d'état s'affiche dans l'onglet Système de la page État > Tableau de bord lorsque l'espace disponible dans l'un de ces emplacements devient trop faible. Lorsque l'espace disque est insuffisant, la journalisation cesse.

- Lorsque l'espace disque disponible descend au-dessous de 10 % du lecteur de stockage des fichiers de cache de journal et des fichiers BCP, un message d'avertissement s'affiche. Bien que la journalisation se poursuive, il est préférable de libérer aussi vite que possible de l'espace disque dans cet ordinateur afin d'éviter toute perte de données.
- Lorsque l'espace disque disponible descend au-dessous de 4 Mo sur le lecteur de stockage des fichiers de cache de journal et des fichiers BCP, un message d'erreur s'affiche.

  Lorsque l'espace disque est inférieur à 4 Mo, la journalisation peut devenir intermittente ou cesser entièrement. Pour réduire les risques de perte de données, libérez aussi vite que possible de l'espace disque sur l'ordinateur Log Server dès que ce message d'erreur s'affiche.

Aucun Log Server installé pour un serveur Policy Server

Websense Log Server collecte des informations sur l'utilisation Internet et les stocke dans la base de données d'activité en vue de leur utilisation dans les rapports d'investigation et de présentation et les graphiques et résumés de la page Tableau de bord de TRITON - Web Security.

Pour pouvoir générer des rapports, Log Server doit être installé.

Ce message peut s'afficher dans les cas suivants :

- Log Server n'est pas installé dans le même ordinateur que Policy Server et l'adresse IP de Log Server n'est pas correctement définie sur localhost dans TRITON - Web Security.
- Vous n'exploitez pas les outils de génération de rapports de Websense.
- Log Server est associé à une autre instance de Policy Server.

Pour vérifier que l'adresse IP de Log Server IP est bien définie dans TRITON - Web Security :

1. Ouvrez l'onglet **Paramètres** dans le panneau de navigation gauche, puis accédez à **Général > Journalisation**.
2. Entrez l'adresse IP ou le nom de l'ordinateur Log Server dans le champ **Adresse IP ou nom de Log Server**.
3. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)**.

Si vous n'exploitez pas les outils de génération de rapports de Websense, ou si Log Server est associé à une instance de Policy Server différente, vous pouvez masquer ce message d'alerte dans TRITON - Web Security.

1. Cliquez sur l'onglet Principal dans le panneau de navigation gauche, puis sur **État > Alertes**.
2. Sous Alertes actives, cliquez sur **Avancé**.
3. Activez l'option **Masquer cette alerte** pour le message « Aucun serveur Log Server installé ».
4. Cliquez sur **Enregistrer maintenant**. Les modifications sont implémentées immédiatement.

Plusieurs instances de Log Server installées pour une seule instance de Policy Server

Chaque instance de Policy Server ne peut se connecter qu'à une seule instance de Web Security Log Server. Lorsque plusieurs instances de Log Server tentent de se connecter à la même instance de Policy Server, les données des journaux ne sont pas enregistrées correctement, ce qui gêne le fonctionnement de plusieurs outils de génération de rapports.

Pour résoudre ce problème :

- Si plusieurs instances actives de Log Server s'exécutent, désinstallez toutes celles qui se connectent à l'instance de Policy Server à l'origine de l'erreur, sauf une.

Pour configurer plusieurs instances de Log Server de sorte qu'elles communiquent avec une instance centrale de Log Server chargée d'enregistrer les données dans la base de données d'activité, consultez la section Extending your Web Security deployment (Extension de votre déploiement de Web Security) dans le Centre Installation et déploiement.

- Si cette erreur s'affiche alors qu'une seule instance de Log Server est active, il est probable que :
  - Policy Server ne s'exécutait pas lorsqu'une instance de Log Server a été désinstallée.
  - L'adresse IP de Policy Server a été modifiée après l'installation de Log Server.
  - Pendant l'installation, Log Server s'est connecté à une instance de Policy Server installée dans un autre ordinateur. Par la suite, une instance de Policy Server a été installée dans l'ordinateur Log Server.

  Dans tous les cas, le moyen le plus sûr pour résoudre ce problème consiste à procéder comme suit :

  1. Désinstallez la ou les instances de Log Server actuellement connectées à l'instance de Policy Server à l'origine de l'erreur.
  2. Arrêtez le service Websense Policy Server (via la boîte de dialogue Services de Windows ou la commande /opt/Websense/WebsenseDaemonControl).
  3. Naviguez jusqu'au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin) et créez une copie de sauvegarde du fichier **config.xml** dans un autre emplacement. **Ne sautez pas cette étape.**
  4. Ouvrez le fichier **config.xml** d'origine dans un éditeur de texte de base (pas dans un éditeur XML ou HTML).
  5. Vers le haut du fichier, localisez le conteneur WebsenseLogServer. Ce dernier contient l'ID de l'instance « fantôme » de Log Server.

     ```
     <container name="WebsenseLogServer">
     ```

  6. Supprimez le conteneur dans son intégralité, y compris sa balise de fermeture. Par exemple :

     ```
     <container name="WebsenseLogServer">
          <data name="0c65012f-93af-11e1-8616-
     f215ee9c7d9d">10.201.136.34</data>
     </container>
     ```

  7. Enregistrez et fermez le fichier **config.xml**.
  8. Supprimez le fichier **config.xml.bak** dans le répertoire **bin** de Websense.
  9. Utilisez la boîte de dialogue Services de Windows ou de la commande /opt/Websense/WebsenseDaemonControl pour démarrer le service Websense Policy Server.

Non création de la base de données d'activité

Lorsque le programme d'installation ne parvient pas à créer la Base de données d'activité, vérifiez les éléments suivants :

- Le compte de connexion utilisé pour l'installation ne dispose pas des autorisations SQL Server adéquates pour créer une base de données. Les autorisations nécessaires dépendent de la version de Microsoft SQL Server :
  - SQL Server Standard ou Enterprise :
    - Membre du rôle serveur **dbcreator**
    - Autorisations **SQLServerAgentReader** requises
  - SQL Server Express : autorisations **sysadmin** requises

  Mettez à jour ce compte de connexion ou connectez-vous avec un compte qui dispose déjà des autorisations requises (voir *Configuration des autorisations d'utilisateur pour Microsoft SQL Server*, page 485), puis réexécutez le programme d'installation.
- Un ou des fichiers existants utilisent les noms de la base de données d'activité par défaut (wslogdb70 et wslogdb70_1), mais les fichiers ne sont pas correctement connectés au moteur de base de données et ne peuvent donc pas être utilisés par le programme d'installation de Websense.

  Pour résoudre ce problème :
  - Si vous ne voulez pas mettre à niveau les fichiers existants de la base de données, supprimez-les ou renommez-les, puis exécutez de nouveau le programme d'installation.
  - Si les fichiers de base de données existants proviennent d'une version pouvant être mise à niveau mais que vous souhaitez continuer à utiliser, servez-vous de SQL Server Management Studio pour associer les fichiers au moteur de base de données, puis réexécutez le programme d'installation.
- Le compte utilisé pour exécuter le programme d'installation ne dispose pas des autorisations adéquates sur le lecteur dans lequel la base de données est installée.

  Actualisez le compte de connexion pour qu'il dispose d'autorisations en lecture et écriture sur l'emplacement d'installation, ou connectez-vous avec un autre compte qui dispose déjà de ces autorisations. Réexécutez ensuite le programme d'installation.
- L'emplacement spécifié ne contient pas suffisamment d'espace disque pour créer et gérer la base de données d'activité.

  Libérez suffisamment d'espace sur le disque sélectionné pour installer et gérer la base de données d'activité. Réexécutez ensuite le programme d'installation. Vous pouvez également choisir un autre emplacement.

Base de données d'activité non disponible

La base de données d'activité Websense stocke les informations sur l'activité Internet en vue de leur utilisation dans les rapports d'investigation et de présentation, et les graphiques et résumés de la page Tableau de bord de TRITON - Web Security.

Si Websense ne peut pas se connecter à la base de données d'activité, commencez par vérifier que le moteur de base de données (Microsoft SQL Server ou Microsoft SQL Server Express) s'exécute dans l'ordinateur de la base de données d'activité.

1. Ouvrez la boîte de dialogue Services de Windows (voir *Boîte de dialogue Services de Windows*, page 515) et vérifiez que le service **MSSQLSERVER** s'exécute :

   Si vous exécutez Microsoft SQL Server Standard ou Enterprise (pas Express), assurez-vous également que le service **SQLSERVERAGENT** s'exécute.

2. Si un service est arrêté, cliquez du bouton droit sur son nom, puis choisissez **Démarrer**.

   Si le service ne redémarre pas, regardez dans l'Observateur d'événements de Windows (voir *Observateur d'événements de Windows*, page 516) si des erreurs et des avertissements sont liés à Microsoft SQL Server.

3. Si vous exécutez Microsoft SQL Server Standard ou Enterprise (pas Express), double-cliquez sur le service SQLSERVERAGENT pour ouvrir la boîte de dialogue Propriétés et vérifiez que le **type de démarrage** est bien défini sur **Automatique**. Vous serez ainsi certain que le service SQL Server Agent redémarre chaque fois que Microsoft SQL Server, ou l'ordinateur du moteur de base de données, redémarre.

   Si le type de démarrage est Manuel ou Désactivé, définissez-le sur **Automatique**, puis cliquez sur **OK**.

Si le moteur de la base de données et les services SQL Server Agent (le cas échéant) s'exécutent :

- Dans la boîte de dialogue Services de Windows, vérifiez que le service **Websense Log Server** s'exécute.
- Si Log Server et la base de données d'activité sont installés dans des ordinateurs différents, assurez-vous que ces deux ordinateurs s'exécutent et que la connexion réseau qui les relie fonctionne.
- Assurez-vous qu'il y ait suffisamment d'espace disque dans l'ordinateur de la base de données d'activité et que suffisamment d'espace disque ait été alloué à celle-ci (voir *Aucun enregistrement de Log Server dans la base de données d'activité*, page 484).
- Vérifiez que le mot de passe SQL Server n'a pas été modifié. Si ce mot de passe a été modifié, vous devez actualiser les informations de mot de passe utilisées par Log Server pour se connecter à la base de données. Voir *Mise à jour du compte ou du mot de passe de connexion à Log Server*, page 484.
- Vérifiez qu'aucune interruption réseau n'empêche TRITON - Web Security de communiquer avec la base de données d'activité.

Après avoir vérifié que le moteur de base de données et les services associés s'exécutent et résolu les éventuels problèmes de réseau, utilisez la boîte de dialogue Services de Windows pour redémarrer le service Websense TRITON - Web Security. Vous serez ainsi certain que le planificateur de rapports de présentation peut enregistrer les définitions des tâches (voir *Aucun Log Server installé pour un serveur Policy Server*, page 477).

Taille de la base de données d'activité retardant la génération des rapports

La taille de la base de données d'activité est toujours problématique. Si vous avez déjà généré des rapports Websense avec succès et que vous remarquez à présent que cette opération est plus longue, ou si votre navigateur Web commence à vous envoyer des messages d'expiration, envisagez de désactiver certaines partitions de la base de données.

1. Dans TRITON - Web Security, sélectionnez **Paramètres** > **Génération de rapports** > **Base de données d'activité**.
2. Localisez la section **Partitions disponibles** de cette page.
3. Cochez la case accolée aux partitions non nécessaires pour les opérations de génération de rapports actuelles, puis cliquez sur **Désactiver**.
4. Cliquez sur **OK**, puis sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Pour plus d'informations sur l'évaluation de la taille de la base de données, consultez la section *Conseils sur le dimensionnement de la base de données d'activité*, page 417.

Plus de 100 fichiers dans le répertoire du cache de Log Server

Habituellement, les fichiers de cache ODBC et les fichiers BCP de Log Server sont régulièrement déplacés vers la Base de données d'activité. Lorsque les fichiers temporaires s'accumulent dans l'ordinateur Log Server, les informations actuelles relatives à l'activité Internet ne sont pas envoyées à la base de données d'activité.

Log Server peut ne pas traiter les fichiers temporaires dans les cas suivants :

- La base de données d'activité ne s'exécute pas, la connexion à l'ordinateur Microsoft SQL Server est hors service ou la base de données est occupée. Voir *Base de données d'activité non disponible*, page 479.
- La base de données d'activité n'est pas installée correctement ou sa version ne convient pas. Voir *Non création de la base de données d'activité*, page 479.
- La tâche ETL ne s'exécute plus et le tampon entrant est saturé.
- La base de données d'activité ne dispose plus d'espace disque. Voir *Aucun enregistrement de Log Server dans la base de données d'activité*, page 484.
- Le chemin de création de la base de données n'est pas valide.
- Aucune partition n'est actuellement active.
- L'insertion BCP présente un problème.
- La taille du fichier **tempdb** présente un problème.

Pour résoudre ce problème :

- Vérifiez que Microsoft SQL Server s'exécute (voir *Base de données d'activité non disponible*, page 479) et qu'aucun autre processus n'utilise abondamment les ressources, par exemple une sauvegarde complète ou une analyse antivirus en exécution.

  Vérifiez également les E/S du disque pour vérifier que l'ordinateur est capable de traiter un taux d'insertion élevé dans la base de données.

- Vérifiez que la version de Microsoft SQL Server que vous utilisez est prise en charge. Les versions prises en charge sont les suivantes :
  - SQL Server 2008 ou 2008 R2 Enterprise ou Standard (32 ou 64 bits)
  - SQL Server 2005 SP 4 Enterprise ou Standard
  - SQL Server 2008 R2 Express (32 ou 64 bits)

    Si vous utilisez SQL Server Express, vous devez choisir le programme d'installation de TRITON Unified pour installer le moteur de base de données.
- Servez-vous de SQL Server Management Studio pour vérifier que la tâche ETL s'exécute.

  Si vous utilisez SQL Server Enterprise ou Standard et que la tâche ETL ne s'exécute pas, vérifiez que le service SQL Server Agent s'exécute bien dans l'ordinateur.

  Si SQL Server Agent s'exécute :
  - Développez la base de données du catalogue (wslogdb70) et vérifiez que la table INCOMINGBUFFER contient des enregistrements. Si le tampon INCOMINGBUFFER est saturé, Log Server ne peut plus ajouter d'autres enregistrements.
  - Si des enregistrements sont présents dans la table INCOMINGBUFFER :
    a. Localisez la table **wse_etl_config**.
    b. Cliquez du bouton droit sur son entrée, puis choisissez **Ouvrir la table**.
    c. Remplacez la valeur de **max_buffer_size** par **40000**.
- Servez-vous de SQL Server Management Studio pour vérifier que l'option **Auto Growth (Croissance automatique)** est bien activée pour la base de données du catalogue.
- Ouvrez la page **Paramètres > Génération de rapports > Base de données d'activité** dans TRITON - Web Security et vérifiez que :
  - Les entrées de **Chemin du fichier** situées sous **Partition Management (Gestion des partitions)** sont valides.
  - Une partition active au moins est répertoriée sous **Partitions disponibles**.
- Si Log Server a été configuré pour utiliser l'insertion BCP mais que les fichiers BCP ne sont pas traités, remplacez la méthode d'insertion par ODBC et voyez si les nouveaux fichiers du cache sont traités :
  1. Sélectionnez Paramètres > Génération de rapports > Log Server dans TRITON - Web Security.
  2. Développez la section **Log Record Creation (Création des enregistrements dans le journal)**.
  3. Activez le bouton radio **ODBC (Open Database Connectivity)**.
  4. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

  Par défaut, les fichiers du cache ODBC sont créés dans le répertoire **C:\Program Files (x86)\Websense\Web Security\bin\Cache**.
- Il est possible que le fichier de journal (ldf) de la base de données **tempdb** soit plein. Redémarrez les services Microsoft SQL Server (MSSQLSERVER) pour effacer la base de données tempdb.

Dernière exécution réussie de la tâche ETL depuis plus de 4 heures

La tâche d'extraction, de transformation et de chargement (ETL, Extract, Transform, and Load) est chargée de traiter les données dans la base de données des partitions. Lorsque cette tâche n'est pas exécutée régulièrement, l'écriture des données dans la base de données d'activité est reportée, et les rapports et les graphiques du Tableau de bord deviennent obsolètes.

En général, la tâche ETL s'exécute rapidement et est programmée pour redémarrer 10 secondes après la fin de son dernier processus. Si cette tâche ne s'est pas exécutée récemment, vérifiez les éléments suivants :

- Vérifiez que Microsoft SQL Server s'exécute (voir *Base de données d'activité non disponible*, page 479) et qu'aucun autre processus n'utilise abondamment les ressources, par exemple une sauvegarde complète ou une analyse antivirus en exécution.

  Vérifiez également les E/S du disque pour vérifier que l'ordinateur est capable de traiter un taux d'insertion élevé dans la base de données.
- Vérifiez que la version de Microsoft SQL Server que vous utilisez est prise en charge. Les versions prises en charge sont les suivantes :
  - SQL Server 2008 ou 2008 R2 Enterprise ou Standard (32 ou 64 bits)
  - SQL Server 2005 SP4 Enterprise ou Standard
  - SQL Server 2008 R2 Express (32 ou 64 bits)

    Si vous utilisez SQL Server Express, vous devez choisir le programme d'installation de TRITON Unified pour installer le moteur de base de données.
- (*Microsoft SQL Server Standard et Enterprise*) SQL Server Agent s'exécute. Utilisez la boîte de dialogue Services de Windows.
- La tâche ETL s'exécute.

  Servez-vous de SQL Server Management Studio pour vérifier que la tâche ETL s'exécute. Si ce n'est pas le cas, cherchez des erreurs dans l'historique de cette tâche, et redémarrez-la ou exécutez-la manuellement.

Configuration de Log Server pour l'utilisation d'un compte de base de données

Lorsque TRITON - Web Security s'exécute dans un dispositif Websense, les composants de génération de rapports ne sont pas disponibles quand Log Server utilise une connexion sécurisée Windows pour accéder à la base de données d'activité.

Pour afficher tous les composants de génération de rapports dans TRITON - Web Security sur un dispositif, configurez Log Server pour qu'il utilise un compte de base de données (par exemple **sa**) pour se connecter à la base de données d'activité. Pour ce faire :

1. Ouvrez TRITON - Web Security, puis la page **Paramètres** > **Génération de rapports** > **Log Server**.
2. Sous **Log Database Connection (Connexion à la base de données d'activité)**, activez le bouton radio **Authentification SQL Server**.

3. Entrez le nom du **Compte** (par exemple **sa**) et le **Mot de passe** d'un compte SQL Server disposant d'autorisations de création, de lecture et d'écriture. Pour plus d'informations, consultez la section *Configuration des autorisations d'utilisateur pour Microsoft SQL Server*, page 485.
4. Cliquez sur **Tester la connexion** pour vérifier que Log Server peut se connecter à la base de données d'activité avec le comte sélectionné et que ce dernier dispose des autorisations appropriées.
5. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.
6. Utilisez la boîte de dialogue Services de Windows pour redémarrer le service **Websense TRITON - Web Security**.

Aucun enregistrement de Log Server dans la base de données d'activité

De façon générale, si Log Server ne peut pas écrire dans la base de données d'activité, c'est que celle-ci ne dispose plus de suffisamment d'espace disque. Cela se produit lorsque le disque est plein ou, dans le cas de Microsoft SQL Server, si une taille maximale a été définie pour la croissance de la base de données.

Si le lecteur qui héberge la base de données d'activité est saturé, vous devez accroître l'espace disque de l'ordinateur pour rétablir la journalisation.

Si votre administrateur de base de données SQL Server a défini une taille maximale de croissance potentielle pour une base de données individuelle dans Microsoft SQL Server, effectuez l'une des opérations suivantes :

- Demandez à votre administrateur de bases de données SQL Server d'augmenter cette taille maximale.
- Identifiez la taille maximale et ouvrez la page **Paramètres** > **Génération de rapports** > **Base de données d'activité** pour configurer la base de données d'activité de sorte qu'elle utilise le remplacement lorsqu'elle atteint environ 90 % de sa taille maximale. Voir *Configuration des options de partition de la base de données*, page 409.

Si votre service informatique a défini une quantité d'espace disque maximale pour les opérations SQL Server, demandez-leur de l'aide.

Mise à jour du compte ou du mot de passe de connexion à Log Server

Pour modifier le compte ou le mot de passe utilisé par Log Server pour se connecter à la base de données d'activité :

1. Connectez-vous à TRITON - Web Security et ouvrez la page **Paramètres** > **Génération de rapports** > **Log Server**.
2. Sous **Log Database Connection (Connexion à la base de données d'activité)**, vérifiez que la base de données appropriée (par défaut, wslogdb70) s'affiche bien dans le champ **Nom de la source de données (DSN)**.

3. Vérifiez que la méthode de connexion sélectionnée est bien l'option **Authentification SQL Server** et qu'un nom de compte valide (par exemple **sa**) s'affiche dans le champ **Compte**.
4. Entrez le mot de passe actuel du compte de connexion.
5. Cliquez sur **Tester la connexion** pour vérifier que Log Server peut utiliser ce compte.
6. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.
7. Utilisez la boîte de dialogue Services de Windows pour redémarrer le service **Websense TRITON - Web Security**.

Configuration des autorisations d'utilisateur pour Microsoft SQL Server

Les éditions Microsoft SQL Server Standard et Enterprise définissent des rôles SQL Server Agent qui régissent l'accès à la structure des tâches. Les tâches SQL Server Agent sont stockées dans la base de données **msdb** de SQL Server.

Pour que Websense Log Server soit bien installé, le compte d'utilisateur qui possède la base de données Websense doit :

1. Être membre de l'un des rôles suivants dans la base de données msdb :
   - Rôle SQLAgentUser
   - Rôle SQLAgentReader
   - Rôle SQLAgentOperator
2. Être membre du rôle **db_datareader**
3. Être membre du rôle de serveur fixe **dbcreator**

Servez-vous de Microsoft SQL Server Management Studio pour accorder les autorisations nécessaires au compte d'utilisateur de base de données et installer correctement Log Server.

1. Dans l'ordinateur SQL Server, sélectionnez **Démarrer > Tous les programmes > Microsoft SQL Server 2005** ou **2008 > Microsoft SQL Server Management Studio**.
2. Sélectionnez l'arborescence **Explorateur d'objets**, puis **Sécurité > Connexions**.
3. Sélectionnez le compte de connexion à utiliser pour l'installation.
4. Cliquez du bouton droit sur le compte de connexion et sélectionnez **Propriétés** pour cet utilisateur.
5. Sélectionnez **Mappage utilisateur** et procédez comme suit :
   a. Sélectionnez **msdb** dans le mappage des bases de données.
   b. Accordez l'appartenance à l'un des rôles suivants :
      - Rôle SQLAgentUser
      - Rôle SQLAgentReader
      - Rôle SQLAgentOperator
   c. Accordez l'appartenance au rôle **db_datareader**.
   d. Cliquez sur **OK** pour enregistrer vos modifications.
6. Sélectionnez **Rôles du serveur**, puis **dbcreator**. Le rôle dbcreator est créé.
7. Cliquez sur **OK** pour enregistrer vos modifications.

Problèmes de connexion de Log Server au service d'annuaire

Si l'une des erreurs énumérées ci-dessous se produit, Log Server ne peut pas accéder au service d'annuaire, alors que cet accès est nécessaire pour la mise à jour des mappages utilisateur/groupe dans les rapports. Ces erreurs s'affichent dans l'Observateur d'événements de Windows (voir *Observateur d'événements de Windows*, page 516).

- EVENT ID:4096 - Impossible d'initialiser le service d'annuaire. Websense Server est peut-être hors service ou inaccessible.
- EVENT ID:4096 - Impossible de se connecter au service d'annuaire. Les groupes de cet utilisateur ne seront pas résolus pour l'instant. Vérifiez que ce processus peut accéder au service d'annuaire.

La cause la plus courante est que Log Server et User Service sont installés de part et d'autre d'un pare-feu qui limite l'accès. Pour résoudre ce problème, configurez le pare-feu de sorte qu'il autorise l'accès via le port 55815.

Les ports utilisés par défaut pour la communication avec le service d'annuaire sont les suivants :

139	Communication NetBIOS : Active Directory
389	Communication LDAP : Active Directory, Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
636	Port SSL : Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
3268	Active Directory
3269	Port SSL : Active Directory

Affichage d'une page de rapport incorrecte

Si vous avez déployé un dispositif V-Series, les paramètres de fuseau horaire définis dans les ordinateurs TRITON - Web Security et Log Server doivent correspondre au fuseau horaire de ce dispositif.

Lorsque les paramètres du fuseau horaire ne sont plus synchronisés, une page incorrecte s'affiche lorsque les administrateurs tentent d'ouvrir la page **Génération de rapports > Rapports d'investigation** de la page **Paramètres > Génération de rapports > Base de données d'activité** dans TRITON - Web Security. Une page de connexion ou un message d'échec de connexion s'affiche alors à la place de la fonctionnalité attendue.

Pour résoudre ce problème, définissez le fuseau horaire des ordinateurs TRITON - Web Security et Log Server sur le fuseau horaire du dispositif, puis redémarrez les services.

Problèmes des rapports d'investigation et de présentation

- *Planificateur de rapports de présentation non connecté à la base de données d'activité*, page 487
- *Espace disque inadéquat pour générer des rapports de présentation*, page 488
- *Échec des tâches planifiées dans les rapports de présentation*, page 488
- *Affichage d'une page de rapport incorrecte*, page 486
- *Bande passante plus importante que prévu*, page 489
- *Absence de journalisation de certaines requêtes de protocoles*, page 490
- *Rapports vides*, page 491
- *Données de rapport manquantes dans le document Microsoft Excel*, page 492
- *Enregistrement du résultat des rapports de présentation au format HTML*, page 493
- *Erreur de génération ou d'affichage des rapports de présentation*, page 493
- *Problèmes de recherche dans les rapports d'investigation*, page 494
- *Problèmes généraux liés aux rapports d'investigation*, page 494

Planificateur de rapports de présentation non connecté à la base de données d'activité

Lorsqu'une alerte d'état indique que le Planificateur de rapports de présentation est déconnecté de la base de données d'activité, ne créez **pas** de tâches planifiées dans les rapports de présentation avant d'avoir résolu ce problème.

Les tâches planifiées créées dans des rapports de présentation alors que cette connexion est rompue ne sont stockées que temporairement et ne peuvent pas être écrites, puis enregistrées définitivement dans la base de données d'activité. En conséquence, les définitions des tâches sont perdues lorsque l'ordinateur TRITON doit être redémarré, ou dès que le service Websense TRITON - Web Security redémarre.

Vérifiez que le moteur de base de données s'exécute et que les éventuels problèmes de réseau ont été résolus. Redémarrez ensuite le service Websense TRITON - Web Security.

1. Dans l'ordinateur TRITON, ouvrez la boîte de dialogue Services de Windows.
2. Dans la liste des services, sélectionnez **Websense TRITON - Web Security**.
3. Cliquez sur le bouton Redémarrer dans la barre d'outils.
4. Après le redémarrage du service, fermez la boîte de dialogue Services.

Espace disque inadéquat pour générer des rapports de présentation

Par défaut, pour générer des rapports de présentation, Websense utilise l'espace disponible dans le dossier suivant de l'ordinateur TRITON :

```
C:\Program Files (x86)\Websense\Web Security\ReportingOutput
```

Lorsque l'espace disponible à cet emplacement est inférieur à 1 Go, un avertissement s'affiche dans le Résumé sur les alertes d'état de l'onglet Système de la page État > Tableau de bord.

Lorsque vous obtenez ce message, libérez de l'espace sur le disque approprié de l'ordinateur TRITON afin d'éviter les problèmes de génération de rapports de présentation ou de performances du système.

Échec des tâches planifiées dans les rapports de présentation

Lorsqu'une ou plusieurs tâches planifiées ne peuvent pas s'exécuter correctement dans les rapports de présentation, le Résumé sur les alertes d'état de l'onglet Système de la page État > Tableau de bord présente un avertissement.

Divers facteurs peuvent être à l'origine des échecs des tâches planifiées, par exemple :

- Les informations du serveur de messagerie n'ont pas été configurées dans la page Paramètres > Génération de report > Préférences. Pour obtenir des instructions, consultez la section *Configuration des préférences de génération de rapports*, page 397.
- L'espace disque disponible dans l'ordinateur TRITON n'est pas suffisant pour générer des rapports de présentation. Pour plus d'informations, consultez la section *Espace disque inadéquat pour générer des rapports de présentation*, page 488.
- La connectivité à la base de données d'activité n'est plus établie. Pour plus d'informations, consultez la section *Aucun Log Server installé pour un serveur Policy Server*, page 477.
- Le serveur de messagerie configuré ne s'exécute pas. Pour résoudre ce problème, contactez votre administrateur système.

Pour identifier la tâche en échec, ouvrez la page **Rapports de présentation > File d'attente de tâches**.

- Si les problèmes connus ont été résolus, cochez la case de la tâche en échec, puis cliquez sur **Exécuter maintenant** pour la relancer.
- Cliquez sur le lien **Détails** de la tâche en échec pour afficher la page Historique de tâches et des informations sur les tentatives d'exécution récentes de la tâche sélectionnée.

Données erronées dans les rapports du temps de navigation sur Internet

N’oubliez pas que la consolidation peut dérégler les données des rapports sur le Temps de navigation sur Internet. Ces rapports indiquent le temps passé par les utilisateurs sur Internet et peuvent détailler le temps consacré à chaque site. Le temps de navigation sur Internet est calculé à partir d’un algorithme spécial et l’activation de la consolidation peut dérégler la précision des calculs pour ces rapports.

Bande passante plus importante que prévu

La plupart des intégrations Websense, mais pas toutes, fournissent des informations sur la bande passante. Si votre intégration n’en fournit pas, vous pouvez configurer Network Agent pour qu’il exécute la journalisation en incluant les données sur la bande passante.

Lorsqu’un utilisateur demande à télécharger un fichier autorisé, le produit d’intégration ou Network Agent envoie la taille complète du fichier, que Websense enregistre sous forme d’octets reçus.

Si l’utilisateur annule ensuite le téléchargement, ou si le fichier n’est pas téléchargé dans son intégralité, la valeur des octets reçus dans la base de données d’activité représente toujours la taille complète du fichier. Dans ce cas, le nombre d’octets rapportés est supérieur au nombre d’octets véritablement reçus.

Cela affecte également les valeurs de bande passante indiquée, qui représentent une combinaison des octets reçus et des octets envoyés.

Absence des données de tendance dans la base de données d’activité

Les données de tendance sont d’abord insérées dans la base de données d’activité par la tâche ETL (qui génère les données de tendance quotidiennes), puis par la tâche trend (qui génère les tableaux hebdomadaires, mensuels et annuels). Ces données sont ensuite utilisées dans les rapports de présentation des tendances.

Si votre base de données ne contient pas de données de tendance ou lorsque certaines données de tendance manquent :

- Assurez-vous d’avoir activé la conservation des données de tendance dans la page Paramètres > Génération de rapports > Base de données d’activité de TRITON - Web Security. Pour que les données de tendance soient générées, puis stockées, l’option **Store trend data (Stocker les données de tendance)** (située sous Trend Data Retention (Conservation des données de tendance)) doit être activée.
- Si vous utilisez Microsoft SQL Server **Standard** ou **Enterprise**, vérifiez que le service SQL Server Agent s’exécute et en tant qu’utilisateur approprié. Voir *Configuration des autorisations d’utilisateur pour Microsoft SQL Server*, page 485, et *Tâche SQL Server Agent*, page 491.

  Dans la boîte de dialogue Services de Windows, vérifiez que le service **SQL Server Agent** s’exécute.

- Vérifiez que les tâches de bases de données **ETL** et **trend** s'exécutent.

  La tâche ETL génère les données de tendance quotidiennes, tandis que la tâche trend s'exécute chaque nuit pour générer les valeurs de tendance hebdomadaires, mensuelles et annuelles. Servez-vous de SQL Server Management Studio pour vérifier que ces deux tâches s'exécutent. Si ce n'est pas le cas, cherchez des erreurs dans l'historique des tâches et redémarrez ces dernières, ou exécutez-les manuellement. Pour plus d'informations, consultez la section *Dernière exécution réussie de la tâche ETL depuis plus de 4 heures*, page 483.

Rapports de tendance vides

Lorsque vous utilisez des rapports de présentation, vous pouvez générer des rapports de tendance pour obtenir des informations de tendance quotidiennes, hebdomadaires, mensuelles ou annuelles. Dans la base de données d'activité, de tables distinctes gèrent les données de tendance de chaque période.

Lorsque les rapports de tendance que vous générez ne contiennent pas de données, commencez par consulter les sections suivantes :

- *Rapports vides*, page 491
- *Erreur de génération ou d'affichage des rapports de présentation*, page 493
- *Absence des données de tendance dans la base de données d'activité*, page 489

Si ces rubriques ne vous permettent pas d'identifier le problème, vérifiez ensuite que :

- Le rapport que vous exécutez est défini pour une période de tendance qui contient des données valides.

  Il existe 4 périodes distinctes pour lesquelles des données de tendance peuvent être stockées et pour lesquelles des rapports peuvent être définis : quotidiennes, hebdomadaires, mensuelles ou annuelles. Vérifiez que des données de tendance existent pour la période sélectionnée pour le rapport de tendance exécuté.

- Les rapports de présentation sont connectés à la base de données d'activité.

  Si la connexion à la base de données d'activité a été interrompue, les outils de rapport de présentation ne peuvent pas créer les rapports. Voir *Base de données d'activité non disponible*, page 479.

- L'espace disque disponible pour la création et le stockage du rapport est suffisant.

  Lorsqu'il génère un rapport, l'outil de rapport de présentation écrit sur le disque. Voir *Espace disque inadéquat pour générer des rapports de présentation*, page 488.

Absence de journalisation de certaines requêtes de protocoles

Quelques protocoles, tels que ceux qu'utilisent ICQ et AOL, invitent les utilisateurs à se connecter à un serveur disposant d'une adresse IP, puis envoient une adresse IP d'identification et un numéro de port différents au client pour la messagerie. Dans ce cas, il est possible que tous les messages envoyés et reçus ne soient pas surveillés et enregistrés par Websense Network Agent, car le serveur de messagerie est inconnu lors de l'échange des messages.

Par conséquent, le nombre de requêtes enregistrées peut ne pas correspondre au nombre de requêtes réellement envoyées. La précision des rapports produits par les outils de Websense en est affectée.

Rapports vides

Si vos rapports ne contiennent aucune donnée, vérifiez les éléments suivants :

- Les partitions de base de données actives comprennent des informations pour les dates incluses dans les rapports. Voir *Partitions de base de données*, page 491.
- La tâche SQL Server Agent est active dans l'ordinateur Microsoft SQL Server. (Ce service n'est pas utilisé avec SQL Server Express.) Voir *Tâche SQL Server Agent*, page 491.
- Log Server est configuré pour recevoir les informations de journal de Filtering Service. Voir *Configuration de Log Server*, page 492.

Partitions de base de données

Tous les enregistrements de journal Websense sont stockés dans des partitions de la base de données. De nouvelles partitions peuvent être créées en fonction de la taille ou de la date, selon votre configuration et votre moteur de base de données.

Vous pouvez activer ou désactiver des partitions individuelles dans TRITON - Web Security. Si vous tentez de générer un rapport à partir des informations stockées dans des partitions désactivées, aucune information n'est détectée et votre rapport sera vide.

Pour vérifier que les partitions de base de données appropriées sont actives :

1. Sélectionnez **Paramètres** > **Génération de rapports** > **Base de données d'activité**.
2. Localisez la section **Partitions disponibles**.
3. Cochez la case **Activer** de chaque partition contenant des données à inclure dans vos rapports.
4. Cliquez sur **Enregistrer maintenant** pour implémenter les modifications.

Tâche SQL Server Agent

Si vous utilisez un ajout Standard ou Enterprise de Microsoft SQL Server, il est possible que la tâche de bases de données SQL Server Agent ait été désactivée. Cette tâche doit s'exécuter pour que les enregistrements de journal soient traités dans la base de données par la tâche de base de données ETL.

1. Sélectionnez **Démarrer** > **Outils d'administration** > **Services**.
2. Vérifiez que les services MSSQLSERVER et SQLSERVERAGENT ont démarré.
3. Vérifiez que le service SQLSERVERAGENT est configuré pour un démarrage **Automatique**. (Double-cliquez sur le nom du service dans la liste Services pour ouvrir la boîte de dialogue Propriétés qui contient les informations sur le **Type de démarrage**.)

   Vous serez ainsi certain que SQL Server Agent redémarre automatiquement à chaque redémarrage de SQL Server ou de l'ordinateur hôte.

Si vous n'avez pas accès à l'ordinateur SQL Server, demandez à votre administrateur de base de données de vérifier que la tâche SQL Server Agent s'exécute et est configurée pour démarrer automatiquement.

Configuration de Log Server

Pour être certain que Log Server reçoive les informations des journaux de Filtering Service, les paramètres de configuration doivent être corrects dans TRITON - Web Security et dans Log Server. Si ce n'est pas le cas, les données de journal ne sont jamais traitées dans la base de données d'activité.

Pour commencer, vérifiez que TRITON - Web Security parvient à se connecter à Log Server.

1. Connectez-vous à TRITON - Web Security avec des autorisations de Super administrateur inconditionnel.
2. Sélectionnez **Paramètres > Général > Journalisation**.
3. Entrez l'adresse IP ou le nom d'hôte de l'ordinateur Log Server.
4. Entrez le port surveillé par Log Server (par défaut, 55805).
5. Cliquez sur **Vérifier l'état** pour vous assurer que TRITON - Web Security peut communiquer avec l'instance de Log Server spécifiée.

   Un message indique si le test de la connexion a réussi. Actualisez l'adresse IP ou le nom d'ordinateur et le port, le cas échéant, jusqu'à ce que ce test réussisse.
6. Lorsque vous avez terminé, 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)**.

Vérifiez ensuite vos paramètres Log Server.

1. Ouvrez la page **Paramètres > Génération de rapports > Log Server**.
2. Sous **Emplacement**, vérifiez que le **Port** correspond à la valeur indiquée dans la page Paramètres > Général > Journalisation.
3. Cliquez sur **OK** pour valider et mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.
4. Si vous avez modifié le paramètre du port de Log Server, utilisez la boîte de dialogue Services de Windows pour redémarrer les services **Websense Log Server** et **Websense TRITON - Web Security**.

Données de rapport manquantes dans le document Microsoft Excel

Le plus grand nombre de lignes pouvant être ouvert dans une feuille de calcul Microsoft Excel est 65 536. Si vous exportez un rapport contenant plus d'enregistrements au format Microsoft Excel, le 65 537ème enregistrement et les suivants ne seront pas disponibles dans la feuille de calcul.

Pour pouvoir accéder à toutes les informations dans le rapport exporté, effectuez l'une des opérations suivantes :

- Dans le cas de rapports de présentation, modifiez le filtre de manière à définir un rapport plus petit, éventuellement en réduisant la plage de dates, en sélectionnant moins d'utilisateurs et de groupes ou en sélectionnant moins d'actions.
- Dans le cas de rapports d'investigation, explorez les données de manière à définir un rapport plus petit.
- Sélectionnez un autre format d'exportation de rapport.

Enregistrement du résultat des rapports de présentation au format HTML

Si vous générez un rapport directement à partir de la page Génération de rapports > Rapports de présentation, vous avez le choix entre 3 formats d'affichage : HTML, PDF et XLS. Si vous choisissez le format HTML, vous pouvez afficher le rapport dans la fenêtre de TRITON - Web Security.

L'impression et l'enregistrement des rapports de présentation à partir du navigateur ne sont pas conseillés. La sortie imprimée comprend l'intégralité de la fenêtre du navigateur et l'ouverture d'un fichier enregistré lance TRITON - Web Security.

Pour imprimer ou enregistrer des rapports plus efficacement, choisissez le format PDF ou XLS. Vous pouvez ouvrir ces types de fichier immédiatement si le logiciel correspondant (Adobe Reader ou Microsoft Excel) est installé dans l'ordinateur local. Vous pouvez également enregistrer le fichier sur le disque (votre seule possibilité si le logiciel correspondant n'est pas disponible).

Après avoir ouvert un rapport dans Adobe Reader ou Microsoft Excel, servez-vous des options d'impression et d'enregistrement de ce logiciel pour obtenir le résultat désiré.

Erreur de génération ou d'affichage des rapports de présentation

Deux options des rapports de présentation permettent d'exécuter immédiatement un rapport : la planification de l'exécution du rapport en arrière plan (par défaut) ou l'exécution du rapport sans planification (si vous avez désactivé l'option par défaut).

Si vous exécutez le rapport sans planification (au premier plan), une fenêtre contextuelle présente l'état du rapport et ce dernier s'affiche. Dans certains cas, au lieu d'afficher un rapport complet :

- Un message d'erreur de génération du rapport s'affiche.
- Un message de rapport terminé apparaît, mais aucun rapport ne s'affiche.

Ce problème survient généralement lorsque l'administrateur a fermé la fenêtre contextuelle contenant les messages de génération de rapport et de rapport terminé en utilisant le bouton de fermeture (X) du navigateur. Pour éviter ce problème, fermez plutôt la fenêtre à l'aide du bouton **Fermer** intégré au menu.

Si vous rencontrez ce problème, quittez la page Rapports de présentation de TRITON - Web Security et réexécutez le rapport. Si cette approche ne fonctionne pas, déconnectez-vous de TRITON - Web Security, puis reconnectez-vous avant de réexécuter le rapport.

Si ce problème persiste, vous pouvez :

- Utiliser l'option **Schedule the report to run in the background (Planifier l'exécution du rapport en arrière-plan)** et ouvrir les rapports via la page Review Reports (Examiner les rapports)
- Utiliser Firefox, plutôt qu'Internet Explorer, pour générer vos rapports

Problèmes de recherche dans les rapports d'investigation

Les champs de recherche situés au-dessus du graphique à barres dans la page principale des Rapports d'investigation vous permettent de rechercher un terme ou une chaîne de texte spécifique dans l'élément graphique sélectionné. Deux problèmes potentiels sont liés à la recherche dans les rapports d'investigation : les caractères ASCII étendus et les correspondances de modèle de recherche.

- Si vous utilisez Mozilla Firefox dans un ordinateur Linux pour accéder à TRITON - Web Security, vous ne pouvez pas saisir de caractères ASCII étendus dans les champs de recherche. Il s'agit d'une limite connue de Firefox sous Linux.

  Si vous devez rechercher une chaîne de texte comprenant des caractères ASCII étendus dans un rapport d'investigation, accédez à TRITON - Web Security à partir d'un ordinateur Windows et utilisez un navigateur pris en charge.
- Il arrive parfois que des rapports d'investigation ne puissent pas trouver les URL associées à un modèle saisi dans les champs de recherche de la page principale des rapports d'investigation. Si cela se produit, et si vous êtes pratiquement certain(e) que ce modèle existe dans les URL rapportées, tentez de saisir un modèle différent qui vous permette également de trouver les URL recherchées.

Problèmes généraux liés aux rapports d'investigation

- Certaines requêtes sont très longues. Vous pouvez dans ce cas obtenir un écran vide ou un message indiquant que votre requête a expiré. Cela peut se produire pour les raisons suivantes :
  - Le serveur Web a expiré.
  - Microsoft SQL Server a expiré.
  - Le serveur proxy ou de mise en cache a expiré.

  Vous devrez peut-être augmenter manuellement le délai d'expiration de ces composants.
- Si les utilisateurs n'appartiennent à aucun groupe, ils n'apparaîtront pas non plus dans un domaine. Les choix Groupe et Domaine seront inactifs.
- Même si Log Server enregistre les visites à la place des accès, les rapports d'investigation appellent ces informations de journal des **Accès**.

Autres problèmes de génération de rapports

- *Mémoire faible dans l'ordinateur Real-Time Monitor*, page 495
- *Non exécution de Real-Time Monitor*, page 495
- *Plus de réponse de Real-Time Monitor*, page 496
- *Impossible d'accéder à certaines fonctions de génération de rapports*, page 496
- *Aucun graphique affiché dans la page État > Tableau de bord*, page 496
- *Problème de configuration des données d'analyse*, page 497
- *Emplacement du référentiel d'analyse inaccessible*, page 497
- *Données d'analyse sur le point de dépasser la limite de taille ou d'âge*, page 498
- *Non exécution ou indisponibilité de Websense Multiplexer*, page 498

Mémoire faible dans l'ordinateur Real-Time Monitor

Cette alerte s'affiche lorsque la mémoire disponible dans l'ordinateur Real-Time Monitor atteint 15 % ou moins de la mémoire totale. Une condition de mémoire faible empêche Real-Time Monitor de recevoir, afficher et stocker tout ou partie des enregistrements du filtrage.

Des différences peuvent alors apparaître dans les données affichées par Real-Time Monitor ou encore, les composants serveur et base de données de Real-Time Monitor peuvent ne pas s'exécuter du tout.

Servez-vous du Gestionnaire des tâches de Windows pour évaluer l'utilisation de la mémoire dans l'ordinateur Real-Time Monitor. Pour résoudre ce problème, vous pouvez :

- Augmenter la quantité de mémoire RAM de l'ordinateur
- Déplacer les applications ou les composants qui sollicitent fortement la mémoire vers un autre ordinateur

Installer Real-Time Monitor dans un ordinateur équipé de plus de mémoire

Non exécution de Real-Time Monitor

Cette alerte s'affiche lorsque le service Websense RTM Server est arrêté.

Utilisez la boîte de dialogue Services de Windows pour vérifier que les 3 services Real-Time Monitor ont démarré et pour démarrer l'un des services suivants éventuellement arrêtés :

- Base de données Websense RTM
- Serveur Websense RTM
- Client Websense RTM

Si l'un de ces services ne démarre pas :

- Dans l'Observateur d'événements de Windows, recherchez des erreurs ou des avertissements provenant éventuellement de Websense RTM Server.
- Dans le fichier **WebsenseRTMMemoryOutput0.log** (situé par défaut dans le répertoire C:\Program Files (x86)\Websense\Web Security\rtm\logs), recherchez des informations sur l'utilisation de la mémoire par Real-Time Monitor.
- Vérifiez que les ressources disponibles (mémoire, disque dur et processeur) sont suffisantes pour l'exécution des services.

Si le service s'exécute alors que l'alerte continue de s'afficher, il est possible que Real-Time Monitor n'ait pas pu s'enregistrer auprès de Policy Server. Vérifiez que l'instance de Policy Server associée à cette instance de Real-Time Monitor s'exécute et que l'ordinateur Real-Time Monitor peut communiquer avec l'ordinateur Policy Server via le port 55836 (communication cryptée) ou 55856 (communication non cryptée).

Si ces services démarrent, assurez-vous qu'ils soient configurés pour un démarrage **Automatique** (non Manuel).

Plus de réponse de Real-Time Monitor

Si Real-Time Monitor n'est pas installé dans le même ordinateur que la console TRITON Unified Security Center, utilisez une commande ping pour vérifier que ces deux ordinateurs peuvent communiquer via le réseau. Vérifiez également que l'ordinateur TRITON peut communiquer avec Real-Time Monitor via le port 9445 (pour l'affichage de l'interface utilisateur).

Real-Time Monitor doit par ailleurs pouvoir communiquer avec :

- Usage Monitor sur le port 55835
- Policy Server sur le port 55836 (communication cryptée) ou 55856 (communication non cryptée)

S'il n'y a pas de problème de communication réseau, il est possible que Real-Time Monitor se heurte à des contraintes de ressources.

- Vérifiez la mémoire, l'utilisation du processeur et l'espace disque disponible dans l'ordinateur Real-Time Monitor.

  Notez qu'au maximum, la base de données RTM peut contenir 10 000 enregistrements, ce qui réduit son impact sur l'espace disque disponible.
- Il est possible que la base de données reçoive trop de requêtes ou ne puisse pas accepter d'autres connexions.

  Si des erreurs de la base de données Websense RTM s'affichent dans l'Observateur d'événements de Windows, vous pouvez résoudre ce problème en redémarrant le service.

  Notez que, lorsque la base de données redémarre, tous les enregistrements sont effacés, ce qui entraîne la perte des anciennes données. Les données non disponibles pour l'affichage dans Real-Time Monitor sont tout de même stockées dans la base de données d'activité et peuvent être consultées dans les rapports d'investigation et de présentation.

Impossible d'accéder à certaines fonctions de génération de rapports

Si les paramètres de blocage des fenêtres contextuelles de votre navigateur Web sont très stricts, ils peuvent bloquer certaines fonctions de la génération de rapports. Pour utiliser ces fonctions, vous devez réduire le niveau de blocage ou désactiver complètement le blocage des fenêtres contextuelles.

Aucun graphique affiché dans la page État > Tableau de bord

Si votre organisation utilise l'administration déléguée, examinez les autorisations de génération de rapports pour le rôle d'administrateur délégué. Si l'option **View dashboard charts (Afficher les graphiques du tableau de bord)** n'est pas activée, ces graphiques ne s'affichent pas pour les administrateurs délégués de ce rôle.

Dans les environnements à plusieurs serveurs Policy Server, TRITON - Web Security ne présente de données de rapports que s'il est connecté au serveur Policy Server également configuré pour communiquer avec Log Server. Vous devez vous connecter à ce serveur Policy Server pour afficher les graphiques dans le tableau de bord ou pour accéder aux autres fonctions de rapports.

Si vous utilisez plusieurs instances de Log Server, des considérations particulières régissent également le déploiement de plusieurs instances de TRITON - Web Security. Dans ces environnements à journalisation distribuée, il est important de n'utiliser qu'une seule instance de TRITON - Web Security pour la génération des rapports. Les administrateurs qui se connectent à l'instance de génération de rapports de TRITON - Web Security peuvent utiliser toutes les fonctionnalités de rapport (y compris les graphiques du tableau de bord). Les administrateurs qui se connectent à d'autres instances de TRITON - Web Security ne disposent pas des fonctionnalités de rapport.

Problème de configuration des données d'analyse

Lorsque la collecte des données d'analyse est activée dans la page **Paramètres > Génération de rapports > Tableau de bord** de TRITON - Web Security, les détails des transactions liées aux tentatives d'envoi de données à l'extérieur de votre réseau et les fichiers de données réellement impliqués sont enregistrés dans un référentiel d'analyse.

Dans de rares cas, les fichiers utilisés pour activer la collecte et le stockage de ces données d'analyse peuvent être endommagés ou corrompus. L'assistance du Support technique de Websense est dans ce cas requise pour résoudre ce problème.

Emplacement du référentiel d'analyse inaccessible

Lorsque la collecte des données d'analyse est activée dans la page **Paramètres > Génération de rapports > Tableau de bord** de TRITON - Web Security, l'administrateur définit l'emplacement (répertoire temporaire ou chemin UNC) de stockage du fichier et fournit les identifiants de connexion d'un compte disposant d'autorisations en lecture, écriture et suppression sur le répertoire spécifié.

Si une alerte d'état signale des problèmes d'accès à l'emplacement du référentiel d'analyse, vérifiez les éléments suivants :

- Les informations de chemin d'accès et d'identification définies dans la page Paramètres > Génération de rapports > Tableau de bord sont correctes.
- Le compte spécifié dispose d'autorisations en lecture, écriture et suppression sur le répertoire.
- Aucun problème réseau n'empêche la communication entre TRITON Management Server et l'ordinateur distant.

Données d’analyse sur le point de dépasser la limite de taille ou d’âge

Lorsque la collecte des données d’analyse est activée dans la page **Paramètres > Génération de rapports > Tableau de bord** de TRITON - Web Security, l’administrateur définit à la fois la taille maximale (en Go) du référentiel et la durée maximale (en jours) de stockage des données d’analyse.

Lorsque la taille du référentiel d’analyse approche la limite définie, une alerte d’état s’affiche. Lorsque la limite est atteinte, les enregistrements les plus anciens sont supprimés, une journée à la fois, jusqu’à ce que la place disponible permette de stocker les nouveaux enregistrements entrants.

Une alerte d’état s’affiche également lorsque la limite de taille n’a pas été atteinte, mais que les enregistrements approchent leur âge maximal. Lorsque cette limite d’âge est atteinte, les enregistrements antérieurs sont supprimés.

Aucune méthode ne permet de récupérer les données d’analyse supprimées.

Non exécution ou indisponibilité de Websense Multiplexer

Lorsque l’intégration SIEM est activée pour des solutions Websense Web Security, Websense Multiplexer transmet les données de l’activité Internet (journaux) de Filtering Service à Log Server et au produit SIEM configuré.

Lorsque Multiplexer ne s’exécute pas ou n’est pas disponible, une fonction de basculement s’assure que Filtering Service transmet les données de journal à Log Server. Les données ne sont toutefois pas envoyées au produit SIEM.

Pour résoudre ce problème dans un déploiement avec dispositif Websense :

1. Si vous n’avez pas activé le service Multiplexer, sélectionnez **Administration > Boîte à outils > Command Line Utility (Utilitaire de ligne de commande)** dans Appliance Manager.

   Sélectionnez **multiplexer**, puis utilisez la commande **enable (activer)**.
2. Si Multiplexer a déjà été activé mais ne s’exécute pas, ouvrez la page **État > Général** dans Appliance Manager et redémarrez le module Websense Web Security.

Pour résoudre ce problème dans un déploiement exclusivement logiciel :

1. Démarrez ou redémarrez le service ou le démon Multiplexer :
   - Sous Windows : utilisez la boîte de dialogue Services pour démarrer (ou redémarrer) le service **Websense Multiplexer**.
   - Sous Linux : utilisez la commande /opt/Websense/**WebsenseDaemonControl** pour démarrer (ou redémarrer) **Multiplexer**.
2. Si le service ne peut pas redémarrer, il est possible que le programme exécutable Multiplexer Controller ne réponde plus.
   - Sous Windows : servez-vous du Gestionnaire des tâches pour arrêter le processus **MuxCtrl.exe**, puis de la boîte de dialogue Services pour démarrer **Websense Multiplexer**.
   - Sous Linux : arrêtez le processus (commande Kill) **MuxCtrl**, puis servez-vous de la commande /opt/Websense/**WebsenseDaemonControl** pour démarrer **Multiplexer**.

Problèmes d'interopérabilité

- *Non exécution de Content Gateway*, page 499
- *Indisponibilité de Content Gateway*, page 500
- *Alertes non critiques de Content Gateway*, page 500
- *Accès impossible de l'administrateur aux autres modules TRITON*, page 503
- *Indisponibilité de Sync Service*, page 503
- *Problème de téléchargement des fichiers journaux par Sync Service*, page 504
- *Problème d'envoi des données de Sync Service à Log Server*, page 505
- *Données du filtrage hybride manquantes dans les rapports*, page 505
- *Espace disque faible dans l'ordinateur Sync Service*, page 506
- *Fichier de configuration de Sync Service*, page 506
- *Non exécution de Directory Agent*, page 507
- *Impossibilité pour Directory Agent de se connecter au contrôleur de domaine*, page 508
- *Service d'annuaire non pris en charge par Directory Agent*, page 509
- *Fichier de configuration de Directory Agent*, page 510
- *Paramètres de ligne de commande de Directory Agent*, page 511
- *Envoi d'alertes par le service hybride*, page 512
- *Impossible de se connecter au service hybride*, page 513
- *Problème d'authentification des connexions du service hybride*, page 513
- *Absence d'informations essentielles dans la configuration hybride*, page 514
- *Suppression du proxy de basculement hybride dans les listes de proxy explicites*, page 514

Non exécution de Content Gateway

Lorsqu'une instance de Content Gateway s'enregistre auprès de Policy Server, cette connexion est surveillée dans TRITON - Web Security. Les informations relatives à l'instance de Content Gateway s'affichent dans la page Paramètres > Général > Content Gateway Access (Accès à Content Gateway) et dans le Résumé du Filtering Service de l'onglet Système de la page État > Tableau de bord.

Lorsque l'instance enregistrée s'arrête, ou est supprimée, un message d'alerte d'état s'affiche dans TRITON - Web Security.

- Si l'instance s'est arrêtée inopinément, recherchez des informations sur l'origine de la défaillance dans le fichier **syslog** de l'ordinateur Content Gateway.
- Si vous avez déplacé Content Gateway vers une autre adresse IP ou un autre ordinateur physique, ou si vous avez supprimé une instance devenue inutile, vous pouvez supprimer l'instance manuellement dans la page Paramètres > Général > Content Gateway Access (Accès à Content Gateway) pour interrompre l'affichage de cette alerte d'état.

Indisponibilité de Content Gateway

Lorsqu'une instance de Content Gateway s'enregistre auprès de Policy Server, cette connexion est surveillée dans TRITON - Web Security. Les informations relatives à l'instance de Content Gateway s'affichent dans la page Paramètres > Général > Content Gateway Access (Accès à Content Gateway) et dans le Résumé du Filtering Service de l'onglet Système de la page État > Tableau de bord.

Lorsque des composants de Web Security ne peuvent plus communiquer avec l'instance enregistrée, un message d'alerte d'état s'affiche dans TRITON - Web Security.

- Vérifiez que l'ordinateur Content Gateway est actif et que Content Gateway s'exécute.
- Cette alerte peut indiquer un problème réseau. Vérifiez que Content Gateway peut communiquer avec les ordinateurs Policy Server (ports 55806 et 55880) et Filtering Service (port 15868).

Alertes non critiques de Content Gateway

Lorsqu'une notification vous signale qu'une instance de Content Gateway a envoyé des alertes non critiques, l'une des erreurs ou conditions suivantes peut s'être produite. Pour identifier l'erreur en question, consultez le Content Gateway Manager associé à l'instance de Content Gateway concernée.

Servez-vous du tableau ci-dessous pour obtenir une présentation de la condition d'erreur. Des informations plus détaillées sont également disponibles dans les fichiers journaux système, d'erreurs et d'événements de l'ordinateur Content Gateway.

Alerte	Description
Réinitialisation du processus Content Gateway	Un problème a entraîné le redémarrage de Content Gateway. Consultez le fichier syslog de Content Gateway pour plus d'informations sur la cause de cette réinitialisation.
Problème de configuration du cache	Content Gateway n'a pas pu configurer un cache. Pour plus d'informations, consultez la section « Configuration du cache » dans l'Aide de Content Gateway Manager.
Impossible de créer une partition pour le cache	Une erreur s'est produite pendant la configuration du cache. Consultez la section « Configuration du cache » dans l'Aide de Content Gateway Manager.
Impossible d'initialiser le cache	Une défaillance du cache s'est produite. Content Gateway tolère les défaillances des disques de cache. En cas de panne complète d'un disque, Content Gateway le désigne comme endommagé et continue à utiliser les disques restants. Consultez la section « Configuration du cache » dans l'Aide de Content Gateway Manager.

Alerte	Description
Impossible d'ouvrir un fichier de configuration	Un fichier de configuration présente un problème. • Pour plus d'informations sur le fichier affecté, consultez le journal système. • Les autorisations du fichier ou du répertoire peuvent avoir été modifiées. • Si le fichier a été modifié hors de Content Gateway Manager, il est possible que des problèmes de syntaxe non valide ou autres perturbent la lecture du fichier.
Champs non valides dans un fichier de configuration	Un ou plusieurs paramètres ou valeurs de paramètre d'un fichier de configuration sont incorrects. Pour plus d'informations sur le fichier affecté, consultez le journal système.
Impossible de mettre un fichier de configuration à jour	Un problème empêche l'enregistrement d'un fichier de configuration. Pour plus d'informations sur le fichier affecté, consultez le journal système.
Non-correspondance du système d'exploitation dans les pairs d'un cluster	Les nœuds d'un cluster doivent être homogènes et utiliser la même : • Plateforme matérielle • Version de système d'exploitation
Impossible d'activer l'adressage IP virtuel	Content Gateway a tenté d'activer le basculement des adresses IP virtuelles, mais a échoué. Ce problème survient lorsque l'adresse IP virtuelle désignée est déjà utilisée dans le réseau. Comme toutes les adresses IP, les adresses IP virtuelles doivent être réservées au préalable, avant de pouvoir être affectées à Content Gateway.
Limitation de connexions trop élevée	Un événement de limite de connexions se produit lorsque les connexions des clients ou des serveurs d'origine atteignent 90 % de la moitié de la limite configurée (45 000 par défaut). Si vous augmentez la limite de connexions, le système doit disposer de suffisamment de mémoire pour gérer le nombre de connexions requises pour les clients. Tout système dont la mémoire RAM est limitée doit avoir une limite de connexions inférieure à la valeur par défaut.

Alerte	Description
Hôte de base de données désactivé	La base de données des hôtes stocke les entrées DNS (Domain Name Server) des serveurs d'origine auxquels le proxy se connecte. Elle surveille : • Les informations DNS (pour une conversion rapide des noms d'hôte en adresses IP) • La version HTTP de chaque hôte (de sorte qu'il soit possible d'utiliser les fonctionnalités de protocole avancées avec les hôtes qui exécutent des serveurs modernes) • Les informations de fiabilité et de disponibilité des hôtes (pour éviter les attentes liées aux serveurs non fonctionnels)
Erreur de la configuration de la journalisation	Content Gateway peut être configuré pour enregistrer les transactions, les erreurs ou les deux, à l'emplacement que vous définissez. Pour plus d'informations sur la journalisation, consultez la section « Utilisation des fichiers journaux » dans l'Aide de Content Gateway.
Impossible d'ouvrir Content Gateway Manager	Content Gateway ne parvient pas à configurer un socket pour gérer les appels d'API de gestion et démarrer l'interface Web.
Échec de l'écho ICMP pour la passerelle par défaut	Un nœud Content Gateway ne parvient pas à contacter sa passerelle par défaut lors de l'affectation des adresses IP virtuelles dans un cluster. Ce nœud va se fermer.
Surcharge du serveur HTTP d'origine	Lorsque Content Gateway est déployé sous forme de cache de proxy Web, les requêtes de contenu Web des utilisateurs passent par Content Gateway avant de parvenir au serveur Web de destination (serveur d'origine). Lorsqu'un client demande un objet HTTP présent dans le cache mais périmé, Content Gateway valide à nouveau cet objet en interrogeant le serveur d'origine pour savoir si l'objet n'a pas été modifié. Si le serveur d'origine est surchargé (ne peut pas accepter les connexions supplémentaires) et ne répond pas à la demande de revalidation, le proxy n'effectue aucune validation, mais envoie à l'utilisateur l'objet périmé présent dans le cache.

Alerte	Description
Résolution de la surcharge du serveur HTTP d'origine	Un serveur d'origine qui refusait auparavant les tentatives de connexion les accepte à présent de nouveau.
Analyse du contenu ignorée	Content Gateway n'a pas pu analyser le contenu d'un site demandé qu'il aurait habituellement analysé. Cela peut se produire lorsque Content Gateway fait face à un trop grand nombre de connexions ou lorsque les ressources du système sont insuffisantes (processeur et mémoire).
Erreur de configuration WCCP	Pour plus d'informations sur les paramètres de configuration, consultez la section « Configuration WCCP » dans l'Aide de Content Gateway Manager.

Accès impossible de l'administrateur aux autres modules TRITON

Si vous obtenez une erreur lorsque vous cliquez sur **Data Security** ou **Email Security** dans TRITON - Web Security, il est possible que le compte local ou réseau que vous avez utilisé pour vous connecter à TRITON ne dispose pas des autorisations d'accès à Data Security ou Email Security.

Pour qu'un administrateur puisse passer d'un module TRITON à l'autre, un Administrateur de sécurité globale doit accorder un accès administrateur à chaque module dans la page Paramètres > Administrateurs de TRITON.

Le compte d'administrateur TRITON Unified Security Center par défaut (**admin**) dispose d'un accès total à tous les modules installés.

Pour plus d'informations, consultez l'Aide de la console TRITON Unified Security Center (disponible via le menu Aide de toute page des Paramètres TRITON).

Indisponibilité de Sync Service

Dans les déploiements Websense Web Security Gateway Anywhere, Websense Sync Service est chargé de la communication entre les services sur site et hybrides. Sync Service :

- Envoie les données de configuration des stratégies au service hybride
- Envoie les informations d'utilisateur collectées par Directory Agent au service hybride
- Reçoit les enregistrements de journal pour les rapports, du service hybride

Si vous n'avez pas encore activé le filtrage hybride, ou si vous avez tenté de l'activer sans y parvenir, notez que vos composants Websense locaux doivent pouvoir communiquer avec Sync Service pour que la connexion au service hybride puisse être créée.

Pour résoudre ce problème, assurez-vous que :

- Sync Service est en cours d'exécution.
- Sync Service parvient à s'associer à l'adresse IP et au port corrects.

- L’adresse IP et le port que Sync Service tente d’utiliser sont répertoriés dans le fichier **syncservice.ini**, situé dans le répertoire **bin** de Websense sur l’ordinateur Sync Service.
- L’adresse IP et le port indiqués dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées) de TRITON - Web Security doivent correspondre à ceux répertoriés dans le fichier **syncservice.ini**. Si vous actualisez le fichier de configuration, actualisez également manuellement la page Paramètres.
- L’adresse IP et le port indiqués dans le fichier **syncservice.ini** doivent correspondre aux valeurs de l’adresse IP et du port de Sync Service indiquées dans le fichier **das.ini** (situé dans le répertoire **bin** de Websense dans l’ordinateur Directory Agent).

Vérifiez qu’aucun autre service de l’ordinateur Sync Service ne soit associé à l’adresse IP et au port que Sync Service tente d’utiliser. Si vous pensez que Sync Service ne peut pas s’associer à l’adresse IP et au port corrects, arrêtez le service, ouvrez une invite de commande et essayez de démarrer le service en mode console :

```
syncservice -c
```

En mode console, Sync Service affiche l’adresse IP et le port qu’il utilise, ou présente une erreur lorsqu’il ne peut pas s’y associer.

- L’ordinateur Sync Service peut communiquer avec l’ordinateur Policy Broker via le port 55880.
- L’ordinateur Sync Service peut se connecter à l’ordinateur Policy Server via les ports 55806 et 40000, et recevoir les données de Policy Server sur les ports 55830 et 55831.
- L’ordinateur TRITON - Web Security peut créer une connexion HTTP à l’ordinateur Sync Service via le port 55832.

Regardez également dans l’Observateur d’événements de Windows ou dans le fichier **websense.log** si des messages d’erreur sont liés à Sync Service.

Problème de téléchargement des fichiers journaux par Sync Service

Sync Service tente de se connecter au service hybride pour télécharger les fichiers journaux destinés aux rapports selon l’intervalle que vous avez configuré (voir *Planification de la communication avec le filtrage hybride*, page 227). Lorsque Sync Service ne peut pas établir cette connexion, ou si Sync Service ne peut pas récupérer les fichiers journaux après la connexion, les problèmes suivants peuvent se produire :

- Le service hybride stocke les fichiers journaux pendant 14 jours seulement. Une fois cette période écoulée, les fichiers journaux sont supprimés et ne peuvent plus être récupérés. Dans ce cas, votre organisation ne peut plus générer de rapports sur l’activité du filtrage hybride enregistrée dans ces journaux.
- Selon le volume d’activité Internet envoyé par votre organisation via le service hybride, les fichiers journaux des rapports peuvent croître rapidement. Si Sync Service ne peut pas télécharger les fichiers journaux une fois par jour au moins, la bande passante requise pour les télécharger et l’espace disque requis pour les stocker temporairement peuvent être relativement importants.

Pour résoudre ce problème, ouvrez la page **État > Hybrid Service (Service hybride)** afin de vous assurer que Sync Service peut se connecter au filtrage hybride. D'autres conseils de dépannage sont disponibles dans la section *Impossible de se connecter au service hybride*, page 513.

Si Sync Service peut se connecter au service hybride, mais ne peut pas récupérer les enregistrements de journal, ouvrez la page **État > Alertes** pour consulter les informations issues du service hybride. Vérifiez également l'adresse électronique administrative associée à votre compte de filtrage hybride.

Problème d'envoi des données de Sync Service à Log Server

Après avoir téléchargé les fichiers journaux du service hybride, Sync Service les transmet à Log Server de sorte qu'ils soient traités dans la base de données d'activité et inclus dans les rapports. Lorsque Sync Service ne peut pas transmettre ces données à Log Server, les fichiers journaux s'accumulent dans l'ordinateur Sync Service et peuvent monopoliser une grande quantité d'espace disque.

- Servez-vous de la commande **telnet** pour vérifier que l'ordinateur Sync Service peut se connecter à l'ordinateur Log Server via le port **55885**.
- Vérifiez que Log Server s'exécute et qu'aucune erreur de Log Server ne s'affiche dans la page État > Alertes.

Données du filtrage hybride manquantes dans les rapports

Lorsque les informations surl'activité Internet des utilisateurs filtrés par le service hybride ne s'affichent pas dans les rapports, commencez par vérifier les éléments suivants :

- Un port de journalisation hybride est configuré dans la page Paramètres > Général > Journalisation. Voir *Configuration du mode de journalisation des requêtes filtrées*, page 398.
- La case à cocher **Have the hybrid service collect reporting data for the clients it filters (Le service hybride doit collecter les données de rapports des clients qu'il filtre)** est activée dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Scheduling (Planification). Voir *Planification de la communication avec le filtrage hybride*, page 227.
- La page **État > Hybrid Service (Service hybride)** indique que Sync Service a bien réussi à se connecter au service hybride et récupéré les enregistrements de journal. Voir *Surveillance de la communication avec le service hybride*, page 233.
- Aucune alerte d'état ne s'affiche dans l'onglet Système de la page **État > Tableau de bord** et ne signale des problèmes de communication avec Sync Service ou des erreurs de Log Server. Voir *Problème d'envoi des données de Sync Service à Log Server*, page 505.

Si votre déploiement utilise une journalisation distribuée au sein de laquelle plusieurs instances de Log Server distantes envoient des données à une instance de Log Server centralisée, assurez-vous également que Sync Service soit configuré pour communiquer avec cette instance de Log Server centrale. Les instances distantes de Log Server ne peuvent pas transmettre les données de la journalisation hybride à l'instance centrale de Log Server.

Espace disque faible dans l'ordinateur Sync Service

Lorsque Sync Service ne peut pas transmettre les fichiers journaux de rapport collectés par le service hybride à Log Server, ces fichiers s'accumulent dans l'ordinateur Sync Service et peuvent monopoliser une grande quantité d'espace disque. Pour éviter ce problème :

- Vérifiez que Sync Service collecte bien les données des journaux du service hybride à l'intervalle défini. Plus l'activité Internet envoyée par votre organisation via le service hybride est importante, plus les fichiers journaux doivent être téléchargés fréquemment pour éviter tout retard.
- Vérifiez que l'ordinateur Sync Service peut se connecter à l'ordinateur Log Server via le port **55885**.
- Allouez suffisamment de ressources au traitement des données de rapport dans l'ordinateur Sync Service.

Fichier de configuration de Sync Service

Utilisez le fichier **syncservice.ini** pour configurer les différents aspects du comportement de Sync Service que TRITON - Web Security ne permet pas de configurer.

Le fichier **syncservice.ini** est situé dans le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin, par défaut).

- Utilisez un éditeur de texte pour modifier le fichier.
- Lorsque vos modifications sont terminées, enregistrez et fermez le fichier, puis redémarrez Sync Service. Les modifications ne sont prises en compte qu'après le redémarrage du service.

Le fichier contient les informations suivantes :

- **SyncServiceHTTPAddress** : adresse IP utilisée par Sync Service pour communiquer avec Directory Agent et TRITON - Web Security. Cette adresse doit correspondre à l'adresse IP de Sync Service indiquée dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées) de TRITON - Web Security.
- **SyncServiceHTTPPort** : port sur lequel Sync Service est à l'écoute des communications de Directory Agent et TRITON - Web Security (par défaut, 55832). Ce port doit correspondre au port de Sync Service indiqué dans la page Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées) de TRITON - Web Security.
- **UseSyncServiceProxy** : indique si Sync Service passe par un proxy pour se connecter au service hybride. Les valeurs disponibles sont **true** ou **false**.
  - **SyncServiceProxyAddress** : adresse IP du proxy par l'intermédiaire duquel Sync Service se connecte au service hybride.
  - **SyncServiceProxyPort** : port du proxy par l'intermédiaire duquel Sync Service se connecte au service hébergé.
  - **SyncServiceProxyUsername** : nom d'utilisateur (si nécessaire) utilisé par Sync Service pour se connecter au proxy et contacter le service hybride.
  - **SyncServiceProxyPassword** : mot de passe (si nécessaire) utilisé par Sync Service pour se connecter au proxy et contacter le service hybride.

Non exécution de Directory Agent

Dans les déploiements Websense Web Security Gateway Anywhere, Websense Directory Agent collecte les informations relatives aux utilisateurs auprès de votre service d'annuaire et les envoie au service hybride afin de les exploiter pour imposer des stratégies de filtrage.

Lorsque Directory Agent n'est pas disponible, les données d'utilisateur du service hybride peuvent devenir obsolètes.

Vérifiez que Directory Agent est installé (logiciel) ou activé (dispositif) et que le service ou le démon s'exécute.

- Dispositif : ouvrez la page **État > Général** dans Appliance Manager et vérifiez que le service Websense Directory Agent s'exécute.
  - Si Directory Agent est répertorié en tant que service désactivé (gris clair), ouvrez la page **Administration > Boîte à outils > Utilitaire de ligne de commande** et sélectionnez **directory-agent-service**, puis **activer**.
  - Si Directory Agent est activé mais ne s'exécute pas, redémarrez le module Websense Web Security.
- Sous Windows : utilisez la boîte de dialogue Services de Windows (**Démarrer > Outils d'administration > Services**) pour démarrer le service ou vérifier qu'il s'exécute.
- Sous Linux : servez-vous de la commande **/opt/Websense/WebsenseDaemonControl** pour démarrer le démon ou vérifier qu'il s'exécute.

Si Directory Agent s'exécute alors que le message d'alerte continue de s'afficher, vérifiez les éléments suivants :

- L'ordinateur Directory Agent peut communiquer avec l'ordinateur Policy Server (ports 40000 et 55806).
- L'ordinateur Directory Agent peut communiquer avec l'ordinateur Sync Service (port 55832).
- Le pare-feu autorise la communication sur le port de Directory Agent (55900).

Si le service démarre, mais ne poursuit pas son exécution :

- Recherchez des erreurs éventuelles dans la page Administration > Logs (Journaux) (Dispositif), l'Observateur d'événements (Windows) ou dans le fichier websense.log (Linux).
- Dans le cas des installations logicielles, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) et vérifiez que le fichier **das.ini** existe et n'est pas corrompu ni tronqué.
- Assurez-vous qu'il y ait suffisamment d'espace disque dans l'ordinateur Directory Agent pour stocker un instantané complet de votre annuaire. Par exemple, l'instantané d'un annuaire de 200 000 utilisateurs requiert 100 Mo d'espace disque environ.
- Assurez-vous qu'il y ait suffisamment de mémoire disponible pour que Directory Agent puisse comparer les instantanés actuel et précédent. Par exemple, la comparaison des instantanés d'un annuaire de 200 000 utilisateurs requiert 100 Mo de mémoire environ.

Impossibilité pour Directory Agent de se connecter au contrôleur de domaine

Pour collecter les informations des utilisateurs auprès du service d'annuaire, Directory Agent doit pouvoir se connecter au contrôleur de domaine. En cas de problème de communication entre l'ordinateur Directory Agent et le contrôleur de domaine, les données des utilisateurs du service hybride peuvent devenir obsolètes et entraîner un filtrage incorrect.

Pour résoudre ce problème :

- Vérifiez que l'ordinateur Directory Agent est lié au domaine et que le pare-feu autorise la communication via le port du service d'annuaire.

Port	Utilisé pour :
139	Communication NetBIOS : Active Directory
389	Communication LDAP : Active Directory, Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
636	Port SSL : Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
3268	Active Directory
3269	Port SSL : Active Directory

- Ouvrez la page **Paramètres > Général > Services d'annuaire** dans TRITON - Web Security et vérifiez que la configuration de votre service d'annuaire n'a pas été modifiée depuis que vous avez mis à jour vos paramètres Directory Agent.
- Ouvrez la page **Paramètres > Hybrid Configuration (Configuration hybride) > Shared User Data (Données utilisateur partagées)** et vérifiez que Directory Agent tente de rechercher un contexte valide (chemin) pour les informations relatives aux utilisateurs et aux groupes. Pour ce faire :
  - Si vous utilisez Windows Active Directory, cliquez sur le nom ou l'adresse IP d'un serveur d'annuaire, puis sur Tester le contexte. Répétez cette procédure pour chaque serveur de catalogue global.
  - Si vous utilisez Oracle (anciennement Sun Java) Directory Server ou Novell eDirectory, cliquez sur Tester le contexte.
- Dans la page Shared User Data (Données utilisateur partagées), vérifiez également que le contexte est non seulement valide, mais aussi approprié. Le contexte doit être limité pour inclure uniquement les utilisateurs et les groupes filtrés par le service hybride.
- Toujours dans la page Shared User Data (Données utilisateur partagées), vérifiez que l'option Directory Search (Recherche d'annuaire) est correctement définie, de sorte que Directory Agent n'effectue de recherche que dans la partie adéquate de votre service d'annuaire.
- Vérifiez qu'il est possible de se connecter à l'adresse IP et au port du service d'annuaire à partir de l'ordinateur Directory Agent.

Problèmes de communication de Directory Agent

Lorsque Directory Agent ne peut pas communiquer avec le service d'annuaire pour récupérer les informations sur les utilisateurs, ou lorsque Directory Agent ne peut pas se connecter à Sync Service, les mises à jour apportées aux informations des utilisateurs et des groupes ne peuvent pas être envoyées au service hybride.

Des problèmes de communication surviennent dans les cas suivants :

- Le réseau présente un problème.
- Les ports utilisés pour le service d'annuaire (voir le tableau) ou Sync Service (55832) sont bloqués entre l'ordinateur Directory Agent et l'ordinateur cible.

Port	Utilisé pour :
139	Communication NetBIOS : Active Directory
389	Communication LDAP : Active Directory, Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
636	Port SSL : Novell eDirectory, Oracle (auparavant Sun Java) Directory Server
3268	Active Directory
3269	Port SSL : Active Directory

- Directory Agent utilise des identifiants de connexion incorrects ou le service cible ne peut pas authentifier la connexion.
- Un service n'est pas disponible, par exemple lors du redémarrage d'un service ou d'un ordinateur.

Pour identifier l'origine de ce problème de communication, recherchez des informations détaillées dans l'Observateur d'événements de Windows ou dans le fichier **websense.log**.

Service d'annuaire non pris en charge par Directory Agent

Directory Agent peut récupérer les informations des utilisateurs et des groupes à partir de services d'annuaire de type LDAP uniquement. Windows Active Directory (Mode mixte) n'est pas pris en charge. Les services d'annuaire pris en charge incluent :

- Windows Active Directory (en mode natif)
- Oracle (auparavant Sun Java System) Directory
- Novell eDirectory
- Si vous n'utilisez pas un service d'annuaire pris en charge, le filtrage hybride peut tout de même s'appliquer aux emplacements filtrés. Par contre, le filtrage basé sur les utilisateurs et les groupes ne peut pas être effectué.

Fichier de configuration de Directory Agent

Servez-vous du fichier **das.ini** pour configurer les différents aspects du comportement de Directory Agent que TRITON - Web Security ne permet pas de configurer. Cela inclut la quantité maximale de mémoire que l'agent peut utiliser, le nombre maximal de threads qu'il peut créer, le répertoire dans lequel il doit stocker les instantanés des informations des utilisateurs, etc.

Le fichier **das.ini** est situé dans le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).

- Utilisez un éditeur de texte pour modifier le fichier.
- Dans le cas des paramètres qui acceptent plusieurs valeurs, servez-vous du symbole pipe (« | ») pour séparer les entrées.
- Dans le cas des paramètres activés ou désactivés, les seules valeurs valides sont **0** (désactivé) et **1** (activé). Dans ce fichier, les valeurs « on » et « off » ne peuvent pas être utilisées.
- Lorsque vos modifications sont terminées, enregistrez, puis fermez le fichier, puis redémarrez le service ou le démon Directory Agent. Les modifications ne sont prises en compte qu'après le redémarrage du service.

Les principales valeurs configurables dans ce fichier incluent :

- La quantité maximale de mémoire utilisable par Directory Agent, en méga-octets (Mo). Si Directory Agent est configuré pour collecter un très grand nombre d'entrées d'annuaire (plus de 200 000 définitions d'utilisateurs ou de groupes), vous pouvez envisager d'augmenter ce chiffre.

  ```
  MaxMemory=100
  ```

- Le chemin de répertoire complet indiquant où Directory Agent stocke les instantanés du service d'annuaire (vues complètes de l'annuaire servant à identifier ce qui a été modifié entre deux requêtes)

  ```
  SnapshotDir=./snapshots/
  ```

  Ce chemin relatif est converti en C:\Program Files\Websense\bin\snapshots (Windows) ou /opt/Websense/bin/snapshots/ (Linux).

- Le chemin de répertoire complet indiquant où Directory Agent stocke les fichiers LDIF que Sync Service envoie au filtrage hybride

  ```
  DiffDir=./diffs/
  ```

- L'expression régulière utilisée par Directory Agent pour valider les adresses électroniques dans les enregistrements LDAP. Les enregistrements dont les adresses électroniques ne correspondent pas au modèle sont abandonnés. Par exemple, [a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?

  Si vous ne voulez pas que Directory Agent valide les adresses électroniques, ne renseignez pas le paramètre (par défaut).

  ```
  EmailValidateRegex=
  ```

- Nombre de tentatives de Directory Agent après un échec de connexion à Sync Service. Ce paramètre accepte un entier compris entre 1 et 65535.

  ```
  SyncServiceRetryCount=5
  ```

- Nombre de secondes pendant lequel Directory Agent doit patienter entre les nouvelles tentatives lorsqu'il se connecte à Sync Service. Ce paramètre accepte un entier compris entre 1 et 65535.

  ```
  SyncServiceRetryDelay=60
  ```

- Nombre de tentatives de Directory Agent après un échec de connexion au service d'annuaire. Ce paramètre accepte un entier compris entre 1 et 65535.

  ```
  DirServiceRetryCount=5
  ```

- Nombre de secondes pendant lequel Directory Agent doit patienter entre les nouvelles tentatives lorsqu'il se connecte au service d'annuaire. Ce paramètre accepte un entier compris entre 1 et 65535.

  ```
  DirServiceRetryDelay=60
  ```

- Nombre de secondes pendant lequel le sous-système de sauvegarde de Directory Agent doit patienter entre les différentes tentatives de reconnexion à Sync Service. Le sous-système de sauvegarde est chargé de vérifier que les données des utilisateurs ont bien été reçues par Sync Service et envoyées au service hybride. En cas de défaillance, ce sous-système de sauvegarde s'assure que le fichier LDIF qui n'a pas pu être envoyé est préservé en vue d'une tentative ultérieure.

  Ce paramètre accepte un entier compris entre 1 et 65535.

  ```
  BackupPollPeriod=60
  ```

- Nombre de tentatives du sous-système de sauvegarde de Directory Agent pour se reconnecter à Sync Service afin de déterminer l'état de la dernière transaction. Ce paramètre accepte un entier compris entre 1 et 65535.

  ```
  BackupRetryCount=60
  ```

- Paramètres de configuration permettant d'envoyer les informations des utilisateurs et des groupes au service hybride si vous utilisez Sun Java System Directory ou Oracle Directory Server. Pour activer ces paramètres, supprimez le symbole # présent au début des lignes.

  ```
  # GroupMembershipAttribute=uniqueMember
  # MemberOfAttribute=memberOf
  ```

- Si Directory Agent respecte ou non les références LDAP. Ce paramètre accepte les valeurs 1 (activé) et 0 (désactivé).

  ```
  EnableLDAPReferrals=1
  ```

Paramètres de ligne de commande de Directory Agent

L'interface de ligne de commande de Directory Agent vous permet au besoin d'installer, de désinstaller, de démarrer et d'arrêter l'agent. Vous pouvez également imprimer les informations de version et d'utilisation de l'agent.

Pour démarrer Directory Agent en mode console (en tant qu'application), ouvrez une invite de commande, accédez au répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut) et saisissez la commande suivante :

```
DAS.exe -c
```

Directory Agent accepte les paramètres de ligne de commande suivants. Notez que certains paramètres ne peuvent être utilisés que dans les environnements Microsoft Windows.

Paramètre	Description
-i	Installe le service Directory Agent. S'inscrit lui-même auprès du système d'exploitation (Windows uniquement).
-u	Désinstalle le service Directory Agent. (Windows uniquement).
-c	Exécute Directory Agent en mode console.
-r	Exécute Directory Agent en tant que démon ou service.
-s	Arrête le service Directory Agent. (Windows uniquement).
-v	Imprime les informations relatives à la version du service Directory Agent.
-h -? -help <sans option>	Imprime les informations relatives à l'utilisation du service Directory Agent.

Envoi d'alertes par le service hybride

Lorsque le service hybride fait face à un problème susceptible d'affecter votre organisation, il envoie une alerte à votre installation de Sync Service. Des alertes sont envoyées pour les problèmes qui affectent le filtrage hybride dans son intégralité ou qui sont propres à votre compte. Lorsque l'alerte est reçue :

- Une alerte générale s'affiche sous Alertes d'état dans l'onglet Système de la page État > Tableau de bord de TRITON - Web Security.
- Une alerte plus spécifique s'affiche dans la page État > Alertes, sous Hybrid Filtering Alerts (Alertes du filtrage hybride).

Si vous pouvez prendre les mesures nécessaires pour résoudre le problème (par exemple, demander à Directory Agent de renvoyer les informations des utilisateurs ou cliquer sur Save and Deploy (Enregistrer et déployer) pour demander à Sync Service de renvoyer les informations des stratégies), ces informations sont incluses dans le message d'alerte détaillé affiché dans la page État > Alertes.

Dans la plupart des cas, les alertes du filtrage hybride sont informatives et visent à vous prévenir qu'un problème temporaire peut empêcher la réception des informations sur les utilisateurs ou les stratégies, ou l'envoi des données des rapports. Aucune action n'est nécessaire de votre part pour résoudre de tels problèmes.

Lorsque la condition à l'origine du problème a été résolue, les alertes affichées dans le tableau de bord Système et dans la page État > Alertes disparaissent.

Impossible de se connecter au service hybride

Pour garantir la cohérence du filtrage et des rapports précis, les parties locales et hybrides de votre solution Websense Web Security Gateway Anywhere doivent communiquer régulièrement.

Certains problèmes réseau, affectant des connexions Internet ou des connexions réseau internes, peuvent empêcher Sync Service d'accéder au service hybride.

- Servez-vous d'un navigateur ou de l'utilitaire **ping** pour vérifier que l'ordinateur Sync Service peut se connecter à Internet.
- Vérifiez qu'il est possible d'établir une connexion HTTPS à Internet depuis l'ordinateur Sync Service. Sync Service utilise le port 443 pour se connecter au service hybride.
- Vérifiez que Sync Service peut communiquer avec les autres composants locaux du réseau via les ports 55830 et 55831.

Vérifiez également qu'aucun problème n'empêche le service hybride d'accepter la connexion à Sync Service.

- Recherchez des informations sur le service hybride dans le tableau Hybrid Filtering Alerts (Alertes du filtrage hybride) de la page État > Alertes.
- Assurez-vous que les administrateurs ont surveillé le compte de messagerie fourni en tant qu'adresse de contact dans la page Paramètres > Général > Compte, afin de lire les messages éventuellement envoyés par le service technique de Websense.

Problème d'authentification des connexions du service hybride

Dans les environnements de filtrage hybride, Sync Service fournit un identifiant de compte chaque fois qu'il se connecte au service hybride pour envoyer ou récupérer des informations. Cet identifiant est propre à votre organisation et est actualisé à chaque changement du mot de passe du compte **admin**.

Dans de rares cas, impliquant éventuellement un problème grave de la base de données des stratégies, la connexion établie entre votre logiciel sur site et le service hybride peut être perdue. Dans ce cas, vous devez demander un jeton de sécurité servant à générer un nouvel identifiant pour votre compte de filtrage hybride. Ce jeton de sécurité est envoyé à l'**adresse électronique de contact** définie dans la page Paramètres > Général > Compte de TRITON - Web Security.

Pour demander un nouveau jeton :

1. Cliquez sur le bouton **Get Token (Obtenir un jeton)** qui s'affiche à côté de l'alerte « Impossible d'authentifier la connexion » dans la page État > Alertes de TRITON - Web Security.
2. Vérifiez que vous avez reçu un message indiquant que la requête a bien été envoyée au service hybride.
3. Surveillez le compte de messagerie d'administration associé à votre compte de filtrage hybride. Le traitement de la demande d'un nouveau jeton de sécurité peut prendre un certain temps.
4. Lorsque vous recevez le message électronique envoyé par le service hybride, ouvrez la page Paramètres > Général > Compte de TRITON - Web Security.

5. Faites défiler l'écran jusqu'à la section Hybrid Filtering (Filtrage hybride) de la page et saisissez le **jeton de sécurité** fourni dans le message.
6. Cliquez sur **Connecter**.

Après vérification, le jeton temporaire est utilisé pour rétablir la communication entre Sync Service et le service hybride.

Absence d'informations essentielles dans la configuration hybride

Dans les environnements de filtrage hybride, Sync Service fournit un identifiant de compte chaque fois qu'il se connecte au service hybride pour envoyer ou récupérer des informations. Cet identifiant est propre à votre organisation et est actualisé à chaque changement du mot de passe du compte **admin**.

Dans de rares cas, impliquant éventuellement un problème grave de la base de données des stratégies, la connexion établie entre votre logiciel sur site et le service hybride peut être perdue. Dans ce cas, vous devez demander un jeton de sécurité servant à générer un nouvel identifiant pour votre compte de filtrage hybride. Ce jeton de sécurité est envoyé à l'**adresse électronique de contact** définie dans la page Paramètres > Général > Compte.

Si vous recevez le message d'alerte « Missing configuration information; connection to hybrid filtering lost (Informations de configuration manquantes ; connexion au filtrage hybride interrompue) », aucune adresse électronique de contact n'a été fournie ou cette adresse n'est plus valide.

Dans ce cas, pour renforcer au maximum la sécurité des données confidentielles de votre organisation, contactez directement le *Support technique de Websense* pour mettre à jour votre compte de filtrage hybride.

Suppression du proxy de basculement hybride dans les listes de proxy explicites

Dans la version 7.6 de Websense Web Security Gateway Anywhere, le basculement vers le service hybride était configuré via l'ajout manuel de l'adresse du proxy hybride dans la liste des proxy explicites, puis l'inclusion de ce proxy en tant que dernier proxy explicite de la liste pour un emplacement filtré. Dans la version 7.7, le basculement est configuré différemment, ce qui signifie que le proxy hybride est retiré de la liste des proxy explicites lors de la mise à niveau.

Le basculement vers le proxy hybride doit à présent être activé pour chaque emplacement filtré, puis approuvé par le service hybride. Voir *Configuration du basculement vers le service hybride*, page 211.

Conseils et outils de dépannage

- *Boîte de dialogue Services de Windows*, page 515
- *Observateur d'événements de Windows*, page 516
- *Fichier journal Websense*, page 516

Emplacement du répertoire « bin » de Websense

La plupart des fichiers exécutables et de configuration de Websense Web Security sont installés dans le répertoire **bin** de Websense. Lorsqu'une procédure de dépannage vous invite à accéder à ce répertoire, l'emplacement précis dépend de votre système d'exploitation et des composants installés.

Plateformes Linux

Pour tous les systèmes d'exploitation Linux pris en charge, le chemin par défaut est le suivant :

```
/opt/Websense/bin/
```

Plateformes Windows

Le chemin par défaut est soit :

```
C:\Program Files\Websense\Web Security\bin
C:\Program Files (x86)\Websense\Web Security\bin
```

Boîte de dialogue Services de Windows

Dans les ordinateurs Microsoft Windows, Filtering Service, Network Agent, Policy Server, User Service et les autres composants Web Security s'exécutent en tant que services. Vous pouvez donc utiliser la boîte de dialogue Services de Windows pour vérifier leur état de fonctionnement.

1. Dans le Panneau de configuration de Windows, ouvrez le dossier **Outils d'administration**.
2. Double-cliquez sur **Services**.
3. Parcourez la liste des services pour localiser le service que vous souhaitez dépanner.

   L'entrée du service comprend son nom, une brève description, son état (démarré ou arrêté), comment le service démarre et le compte utilisé par le service pour effectuer ses tâches.
4. Double-cliquez sur un nom de service pour ouvrir une boîte de dialogue de propriétés présentant davantage d'informations sur ce service.

Observateur d’événements de Windows

L’Observateur d’événements de Windows enregistre les messages d’erreur relatifs aux événements Windows, y compris les activités des services. Ces messages peuvent vous aider à identifier des erreurs de réseau ou de service à l’origine de problèmes de filtrage Internet ou d’identification des utilisateurs.

1. Dans le Panneau de configuration de Windows, ouvrez le dossier **Outils d’administration**.
2. Double-cliquez sur **Observateur d’événements**.
3. Dans l’Observateur d’événements, cliquez sur **Application** pour obtenir la liste des erreurs, des avertissements et des messages d’information.
4. Parcourez la liste pour identifier les erreurs ou les avertissements provenant de services Websense.

Fichier journal Websense

Websense inscrit ses messages d’erreur dans le fichier **websense.log**, situé dans le répertoire **bin** de Websense (C:\Program Files *ou* Program Files (x86)\Websense\Web Security\bin ou /opt/Websense/bin/, par défaut).

Les informations de ce fichier sont comparables à celles de l’Observateur d’événements de Windows. Dans les environnements Windows, l’Observateur d’événements présente les messages de façon plus conviviale. Le fichier **websense.log**, toutefois, est disponible dans les systèmes Linux et peut être envoyé au support technique de Websense si vous avez besoin d’aide pour résoudre un problème.

Index

A

abonnements, 24
  dépassés, 24
  périmés, 24
  portail MyWebsense, 24
accès
  définition, 405
Accès à l'URL, outil, 283
accès à TRITON - Web Security, 18, 334
accès des utilisateurs au filtrage hybride, 214
accès et visites, 405
  impact sur la taille de la base de données, 417
accès Internet en fonction du temps, 58
accès par mot de passe, 84
  dans un environnement à plusieurs serveurs Policy Server, 363
  plusieurs instances de Filtering Service, 366
actions, 57
  Autoriser, 57
  blocage en fonction de la bande passante, 57
  Bloquer, 57
  Bloquer des mots-clés, 58
  Bloquer des types de fichiers, 58
  Confirmer, 57
  Contingent, 58
  sélection pour les rapports de présentation, 138
Active Directory
  configuration hybride, 221
  mode natif, 76
Activité utilisateur par mois, rapport, 165
Add Chart (Ajouter un graphique), 34
admin, 19
  suppression, 324
  utilisateur, 324
administrateurs, 324
  accès à TRITON - Web Security, 351
  accès simultané au même rôle, 329
  affichage de la définition du rôle, 348
  ajout dans un rôle, 337, 340
  autorisations, 326
  autorisations Accès direct à Content Gateway, 327
  autorisations de génération de rapports, 327, 339
  autorisations exceptions only (exceptions uniquement), 327
  autorisations full policy (stratégie complète), 326
  autorisations inconditionnelles pour les stratégies, 326
  autorisations Real-Time Monitor, 327
  autorisations, configuration, 338, 341
  dans plusieurs rôles, 329, 340
  impossible de passer d'un module à l'autre, 503
  notification des responsabilités, 334
  présentation, 325
  rapports, 348
  retrait du rôle, 337
  suivi des modifications apportées, 373
  Super administrateur, 326
  tâches des administrateurs délégués, 346
  tâches du Super administrateur, 330
  Verrouillage du filtre, effets, 331
administration déléguée
  accès aux rapports, 395
  ajout d'administrateurs, 340
  ajout de rôles, 335, 336
  application des stratégies, 346
  auditeurs, 328
  autorisations, 326
  autorisations Accès direct à Content Gateway, 327
  autorisations de génération de rapports, 327
  autorisations exceptions only (exceptions uniquement), 327
  autorisations full policy (stratégie complète), 326
  autorisations pour les stratégies, 326

autorisations Real-Time Monitor, 327
conflits entre les rôles, 343
modification des rôles, 337
notification des administrateurs, 334
préparation, 330
présentation, 323
retrait de clients des rôles, 345
suppression de rôles, 335
suppression de rôles, effets, 345
utilisation, 335
adresse électronique
contact associé au filtrage hybride, 204
adresses IP
filtrage par, 73
adresses IP privées
et filtrage hybride, 205
affichage, options
rapports d'investigation, 423
Afficher les modifications en attente, 23
agents utilisateurs, 229
agrégation des données, 371
ajout
à des protocoles définis par Websense, 270
clients, 81
contextes racine du service hybride, 224
destinations non filtrées, 212
domaines de messagerie (hybride), 216
emplacements filtrés, 206
entrées des listes Toujours analyser ou Ne jamais analyser, 194
filtres d'accès limité, 249
filtres de catégories, 61
filtres de protocoles, 63
proxy explicite, 210
stratégies, 92
types de fichiers, 279
Ajouter
filtre de catégories, 61
filtre de protocoles, 63
ajouter
filtre d'accès limité, 249
groupes LDAP personnalisés, 81
mots-clés, 259
stratégies, 92
alertes, 385
activité suspecte, 378
configuration des limites, 379
configuration des méthodes, 379
filtrage hybride, 512
fonctionnement de Websense, 385
messagerie, 379
méthodes d'envoi, 378
Mises à jour de sécurité en temps réel, 385
mises à jour en temps réel de la base de données, 385
prévention des excès, 378
résumé du fonctionnement, 43
SNMP, 379
système, 377
système, configuration, 380
utilisation de catégorie, ajout, 382
utilisation de catégories, 378
utilisation de catégories, configuration, 381
utilisation de protocole, ajout, 383
utilisation de protocoles, 378
utilisation de protocoles, configuration, 382
alertes d'activité suspecte, 378
alertes d'utilisation, 378
catégorie, ajout, 382
catégorie, configuration, 381
journalisation des catégories, 398
non générées, 469
protocole, ajout, 383
protocole, configuration, 382
alertes d'utilisation de catégories
ajout, 382
configuration, 381
et journalisation, 398
suppression, 381
alertes d'utilisation de protocoles
ajout, 383
configuration, 382
alertes de fonctionnement, 385
description, 466
résumé, 43
solutions, 468
alertes de gravité, 378
alertes par e-mail, 379
alertes SNMP, 379

alertes système, 377
  configuration, 380
  Content Gateway, 380
  Web Security, 380
analyse
  activation, 183
  clé d'abonnement, 183
  enregistrements du journal, 197
  exceptions, 182
  mises à jour de la base de données, 195
  paramètres, 183
  présentation, 181
analyse des applications, 188
analyse des fichiers
  définition de la taille maximale, 192
  expiration de l'analyse, 191
  extensions de fichier, 189
analyse des menaces, 187
analyse en temps réel, voir analyse, 181
Analyser l'utilisateur, outil, 283
anonyme, journalisation, 399
applets
  temps contingenté, 59
Appliquer aux clients, 93
Appliquer une stratégie à des clients, 95
arrêt
  démons Linux, 376
  services Websense, 375
authentification
  applications Internet, 229
  sélective, 289
authentification hybride
  ajout de règles personnalisées, 230
  modification des règles personnalisées, 231
authentification manuelle, 287
  activation, 289
authentification personnalisée
  ajout de règles, 230
  modification des règles, 231
authentification sélective, 289
auto-enregistrement, 243
  ajout de domaines, 216
  modification des domaines, 216
autorisations
  accès direct à Content Gateway, 327
  administrateur, 326
  auditeur, 328
  configuration, 338, 339, 341
  DC Agent, 455, 460
  full policy (stratégie complète), 326
  gestion des stratégies et génération de rapports, 327
  inconditionnelles pour les stratégies, 326
  lecteur d'installation, 479
  libération des stratégies, 335
  Logon Agent, 460
  plusieurs rôles, 329
  rapports, 327, 351
  rapports d'investigation, 328
  Real-Time Monitor, 327
  SQL Server, 479, 485
  User Service, 460
autorisations Accès direct à Content Gateway, 327
autorisations d'auditeur, 328
autorisations des administrateurs
  exceptions only (exceptions uniquement), 327
autorisations exceptions only (exceptions uniquement), 327
autorisations full policy (stratégie complète), 326
autorisations pour les stratégies
  inconditionnel, 326
  libération, 335
autorisations Real-Time Monitor, 327
Autoriser, 57
autoriser des URL pour tous les utilisateurs (hybride), 212

B

bande passante
  configuration des limites, 272
  gérée par Content Gateway, 271
  gérée par Network Agent, 271
  gestion, 270
  journalisée pour les requêtes bloquées, 155
  plus importante que prévu, 489
  utilisée par les catégories, 270
  utilisée par les protocoles, 270, 271
bande passante journalisée, requêtes bloquées, 163
bannière, 21

bannière TRITON, 21
base de données
  base de données d'activité, 406
  base de données des stratégies, 360
  Base de données principale, 27
  catalogue, 406
  mises à jour en temps réel de la base de données, 28
  partitions de la base de données d'activité, 406
  pour l'analyse, 195
  Real-Time Security Updates, 28
  tâche de maintenance, 412
  tâches de la base de données d'activité, 407
base de données d'activité, 357, 395
  active, 408
  administration, 396, 408
  base de données de catalogue, 406
  connexion pour les rapports d'investigation, 421
  consolidation des enregistrements de journal, 403
  création de partitions, 409
  maintenance, 412
  non créée, 479
  non disponible, 479
  paramètres, 408
  partitions de la base de données, 406
  pas d'enregistrement des données, 484
  présentation, 406
  réindexation, 412
  sélection de partitions pour les rapports, 411
  suppression des erreurs, 413
  tâche AMT, 408
  tâche de maintenance, 407, 412
  tâche IBT, 130, 407
  tâche trend, 408
  tâches, 407
  taille, 417, 481
  taux de croissance et taille, 418
base de données de filtrage initiale, 439
base de données des stratégies, 354, 360
  ne démarre pas, 470
base de données initiale, 27
Base de données principale, 27, 355
  amélioration, 30
  catégories, 50
  de plus d'une semaine, 440
  état du téléchargement, 366
  initiale, 439
  mise à jour, 440
  mises à jour en temps réel, 28
  planning de téléchargement, 28
  problèmes de téléchargement, 440
  protocoles, 51
  Real-Time Security Updates, 28
  reprise du téléchargement, 367
  serveurs de téléchargement, 441
  téléchargement, 27
Base de données principale Websense, 27
BCP
  pour l'insertion des enregistrements de journal, 402
bin, répertoire, 515
blocage
  contenu intégré, 117
  par mot-clé, 259
  protocoles, 265
  publications destinées à certains sites, 263
  types de fichiers, 273
blocage des fenêtres contextuelles
  accès aux rapports, 496
blocage par mots-clés
  dépannage, 448
BlockMessageBoardPosts, 263
Bloquer, 57
  en fonction de la bande passante, 57
  Mots-clés, 58
  Types de fichiers, 58
bloqués et verrouillés, 332
  catégories, 332
  mots-clés, 332
  protocoles, 333
  types de fichiers, 333
boîte à outils, 282
boîte de dialogue Services, 515
bouton Continuer, 57

C

calcul des économies de bande passante, 46

calcul du temps économisé, 46
caractères ASCII étendus
  dans le nom de l'ordinateur DC Agent, 296
  recherche dans les rapports d'investigation, 494
caractères ASCII, étendus
  recherche dans les rapports d'investigation, 494
carte réseau de blocage, 432
carte réseau de surveillance, 432
catalogue
  base de données, 406
  rapport, 131
catalogue de rapports, 131
  nom, 139
catalogue global, 76
catégorie confidentielle, 199
Catégorie d'URL, outil, 282
catégorie Largeur de bande, 52
catégorie Productivité, 52
catégorie Sécurité, 53
catégories
  ajout à la base de données principale, 52
  ajout de catégories personnalisées, 257
  définition, 27, 50
  Événements spéciaux, 52
  journalisation, 398
  Largeur de bande, 52
  liste exhaustive, 51
  modification des catégories personnalisées, 254
  personnalisées, 254
  Productivité, 52
  Protection étendue, 53
  renommer une catégorie personnalisée, 256
  Sécurité, 53
  sélection pour les rapports de présentation, 137
  utilisation de la bande passante, 270
  verrouillage pour tous les rôles, 332
catégories personnalisées, 254
  ajout, 257
  création, 253
  modification, 254
  renommer, 256
catégorisation du contenu, 184
certificat SSL
  filtrage hybride, 218
changement de rôle, 327
Check Point
  requête FTP non bloquée, 449
classes de risque, 395, 396
  attribution de catégories, 396
  dans la génération de rapports, 396
classes de risques, 54
  Perte de bande passante réseau, 54, 55
  Perte de productivité, 54, 55
  Responsabilité légale, 54
  Risques de sécurité, 55
  sélection pour les rapports d'investigation, 162
  sélection pour les rapports de présentation, 137
  Utilisation professionnelle, 55
clé, 24
clé d'abonnement, 24
  non valide ou arrivée à expiration, 438
  non vérifiée, 438
  saisie, 25
  vérification, 441
clé d'abonnement à Websense Web Security Gateway, 183
Client Remote Filtering, 356
client Remote Filtering, 238
  fichier journal, 239, 241
clients, 71
  ajout, 81
  annuaire, 71
  application des stratégies, 71
  attribution de stratégies, 93, 95
  déplacer vers le rôle, 86
  gestion, 72
  groupes, 74
  groupes LDAP personnalisés, 73
  modification, 83
  ordinateurs, 71, 73
  réseaux, 71, 73
  sélection pour les rapports de présentation, 136
  utilisateurs, 74
clients de l'annuaire, 71
clients gérés, 324
  ajout dans des rôles, 346
  application des stratégies, 350
  attribution à des rôles, 338, 342, 348

attribution à un rôle, 338, 342
chevauchement des rôles, 343
dans plusieurs rôles, 342, 349
déplacement vers un rôle, 86
suppression dans des rôles, 338, 345
clients gérés, suppression, 471
colonnes
des rapports d'investigation détaillés, 161
combinaison
filtrages hybride et sur site, 203
commandes
WebsenseAdmin, 376
WebsenseDaemonControl, 376
composants, 354
base de données d'activité, 357
base de données des stratégies, 354
Base de données principale, 355
Client Remote Filtering, 356
client Remote Filtering, 238
DC Agent, 358
Directory Agent, 359
eDirectory Agent, 358
Linking Service, 359
Log Server, 357
Logon Agent, 358
Multiplexer, 357
Network Agent, 355
Plug-in de filtrage, 359
Policy Broker, 354
Policy Server, 355
RADIUS Agent, 359
Real-Time Monitor, 357
Serveur Remote Filtering, 238, 356
Service de filtrage, 355
State Server, 356
Sync Service, 359
TRITON - Web Security, 356
Usage Monitor, 356
User Service, 358
Websense Content Gateway, 356
composants de filtres, 253
compte de base de données
utilisé par Log Server, 483
comptes d'administrateur
affichage, 336
comptes d'utilisateur
admin, 324
configuration
Log Server, 400
configuration de carte réseau
blocage, 432
paramètres, 431
surveillance, 432
configuration de DC Agent, 296
configuration des stratégies
restauration des paramètres par défaut, 67
Confirmer, 57
dans un environnement à plusieurs serveurs Policy Server, 363
plusieurs instances de Filtering Service, 366
connexion, 19
connexion à la base de données d'activité
DSN, 401
connexion, erreur, 472
console de gestion, 18
console TRITON, 18
impossible de passer d'un module à l'autre, 503
consolidation
et journalisation des URL complètes, 414
et temps de navigation sur Internet, 489
consolidation des enregistrements de journal, 403
impact sur la taille de la base de données, 417
contacter le support technique, 24
Content Gateway, 356, 372
accès depuis la console TRITON, 372
alertes non critiques, 500
alertes système, 380
clé d'abonnement, 183
ne s'exécute pas, 499
non disponible, 500
page Content Gateway Access (Accès à Content Gateway), 372
contenu
analyse des menaces, 187
blocage du contenu intégré, 117
catégorisation, 184
contenu actif
retrait, 192
contenu ActiveX

retrait, 192
contenu dynamique
catégorisation, 184
contenu JavaScript
retrait, 192
contenu, découpage, 192
Contingent, 58
contournement du décryptage, 198
contournement du décryptage SSL, 198
catégorie confidentielle, 199
présentation, 182
contrôle des flux des alertes, 378
copie
filtres d'accès limité, 60
filtres de catégories, 60
filtres de protocoles, 60
rapports de présentation, 132
copier
rapports de présentation, 132
Copier dans le rôle, 252
filtres, 60
stratégies, 91
correctifs, 24
correspondance des catégories
Détails de l'activité utilisateur, rapport, 166
couleur rouge, rapports d'investigation, 156
courrier électronique
personnalisation pour les rapports d'investigation, 173
personnalisation pour les rapports de présentation, 148
création
filtres d'accès limité, 93
filtres de catégories, 93
filtres de protocoles, 94
stratégies, 92

D

das.ini, 510
DC Agent, 295, 358
autorisations, 460
autorisations insuffisantes, 455
configuration, 296
dc_config.txt, fichier, 456, 457
fichier requis manquant, 456
déblocage des URL (hybride), 212
découpage du contenu actif, 192
définition des options d'analyse, 183
définition des stratégies
planification, 93
délai d'expiration
désactivation pour TRITON - Web Security, 46
demandes d'authentification
rapport, 229
démarrage
démons Linux, 376
services Websense, 375
déplacement de sites vers une autre catégorie, 260
déplacer vers le rôle, 86
clients, 86
destinations non filtrées
ajout, 212
définition, 212
fichier PAC, 212
messagerie Web, 212
modification, 213
syntaxe, 213
Détail de l'activité utilisateur par jour, rapport, 164
correspondance des catégories, 166
détails des incidents suspects, 37
détection de contenu malveillant avancé, 35
détection des protocoles, 186
détection des protocoles mis en tunnel, 186
didacticiels
Démarrage rapide, 19
didacticiels Démarrage rapide, 19
démarrage, 19
Directory Agent, 220, 359
ajout de contextes, 224
et utilisateurs hors site, 220, 243
exclure des contextes, 226
fichier de configuration, 510
impossible de se connecter au contrôleur de domaine, 508
informations sur l'état, 233
ne s'exécute pas, 507
problèmes de communication, 509
service d'annuaire non pris en charge, 509
Directory Agent, interface de ligne de commande, 511

dissimulation des noms d'utilisateur
  rapports d'investigation, 157
données d'analyse
  des incidents suspects, 38
données de tendance
  impact sur la taille de la base de données, 418
  non disponible, 489
  stockage, 416
données des journaux
  envoi à l'intégration SIEM, 371
données envoyées par WebCatcher, 30
durées de navigation
  détaillé, 415
  sur Internet (IBT), 130, 414

E

échec de fermeture
  délai d'expiration, 239, 240
  logiciel Remote Filtering, 239
échec de l'ouverture
  logiciel Remote Filtering, 239
économies de bande passante
  tableau de bord, 45, 46
économies de temps
  tableau de bord, 45, 46
eDirectory, 78
eDirectory Agent, 304, 358
  configuration, 305
eimserver.ini
  BlockMessageBoardPosts, paramètre, 263
  SecurityCategoryOverride, paramètre, 262
emplacements filtrés
  ajout, 206
  définition, 205
  modification, 208
  proxy explicites, 209
endpoint
  mot de passe d'anti-altération, 315
enregistrement des rapports de présentation, 143
enregistrements de journaux hybrides
  collecte, 228
  non envoyés à Log Server, 505
  non téléchargés, 504
enregistrements du journal, 196
  ODBC ou BCP, 402
  pour l'activité d'analyse, 198
  Sync Service ne peut pas télécharger, 504
espace disque
  des rapports de présentation, 145
  requis pour le téléchargement de la base de données, 443
Estimations de l'utilité
  calculs, 45
État
  Alertes, 385
  Journal d'audit, 373
  Tableau de bord, 33
état
  filtrage hybride, 233
  service hybride, 233
état de Websense, 385
  Alertes, 385
  Journal d'audit, 373
état du système
  surveillance, 46
ETL, tâche, 407
évaluation des stratégies de filtrage, 129
Événements spéciaux, 52
Event Details (Détails de l'événement), 37
  données d'analyse, 38
  personnalisation, 38
exceptions
  définition, 103
  gestion, 103
  recherche, 105
exceptions à l'identification des utilisateurs, 288
exceptions aux stratégies, 103
  gestion, 103
exceptions d'authentification, 289
exécution de TRITON - Web Security, 18
Exemple - Utilisateur standard, stratégie, 89
exemples
  filtres de catégories et de protocoles, 65
  stratégies, 89
expiration
  rapports, 481
expiration des sessions, 19
Explorateur d'ordinateur, service
  activation, 459
expressions régulières, 253, 281

dans un filtre d’accès limité, 251
recatégorisation des URL, 255
extensions de fichier
ajout à un type de fichiers, 280
ajout à un type de fichiers prédéfini, 279
dans les types de fichiers prédéfinis, 276
filtrage par, 273
pour l’analyse, 189

F

favoris
rapports d’investigation, 153, 170, 171, 172
rapports de présentation, 132, 139, 141
fichier de configuration automatique des proxy (PAC), 214
configuration du navigateur, 219
définition, 219
destinations non filtrées, 212
fragment personnalisé, 219
informations sur l’état, 233
par défaut, 219
personnalisation, 219
fichier journal, 516
client Remote Filtering, 241
fichier PAC. Voir Fichier de configuration automatique des proxy (PAC).
fichiers
blocage de l’accès, 273
fichiers de sauvegarde
appellation, 386
stockage, 391
fichiers, analyse, 188
file d’attente des tâches
rapports d’investigation, 153, 174
rapports de présentation, 133
Filtering Service
alerte d’utilisation intensive du processeur, 447
mise à jour de l’ID unique, 451
modification de l’adresse IP, 451
ne s’exécute pas, 446
filtrage
actions, 57
boîte à outils, 282
combinaison de solutions, 203
diagramme, 98
ordre, 95
par mots-clés, 258
présentation des composants, 353
priorité, 98
priorité, URL personnalisées, 261
processus, 98
protocoles, 265
recherche d’images, 59
types de fichiers, 273
utilisateurs distants ou itinérants, 237
filtrage de la recherche, 59
filtrage hybride, 203
absent dans les rapports, 505
accès utilisateur, 214
adresse électronique de contact, 204
alertes, 512
authentification impossible, 513
authentification personnalisée, 229
auto-enregistrement, 215, 243
certificat SSL, 218
compte, 204
configuration d’Active Directory, 221, 222
configuration d’Oracle Directory Server, 223
configuration de Novell eDirectory, 224
contexte racine d’Active Directory, 222
contexte racine d’Oracle Directory Server, 223
contexte racine de Novell eDirectory, 224
destinations non filtrées, 212
emplacements filtrés, 205
enregistrement des domaines, 216
état, 233
exclure des contextes, 226
fichier PAC, 214
filtres de recherche des utilisateurs et des groupes, 226
formulaire d’authentification sécurisée, 312
identification des utilisateurs, 311, 313
Identification NTLM, 312
identification transparente, 311
informations de configuration manquantes, 514
mots de passe des utilisateurs hors site, 220
pages de blocage personnalisées, 215, 217
perte de connexion, 513

planification de la synchronisation des enregistrements de stratégies, d'utilisateurs et de journaux, 227
Service d'authentification, 317
services d'annuaire pris en charge, 220
utilisateurs hors site, 205, 216, 242
Web Endpoint, 314
filtrage par réputation, 53
filtre Autoriser tout
et priorité du filtrage, 98
filtre Bloquer tout, 66
et priorité du filtrage, 99
filtre des rapports de présentation, 132, 135
confirmation, 141
sélection de catégories, 137
sélection de classes de risques, 137
sélection de protocoles, 138
sélection des actions, 138
sélection des clients, 136
filtres, 60
accès limité, 60, 248
catégorie, 49, 60
copier dans le rôle, 252
création pour un rôle, 350
détermination de l'utilisation, 94
modification de l'élément actif, 94
modification pour le rôle, 349
protocole, 49, 60
rapports de présentation, 132
restauration des paramètres par défaut, 67
filtres Autoriser tout, 66
filtres d'accès limité, 60, 248
ajout, 93
création, 249
expressions régulières, 251
priorités du filtrage, 248
renommer, 250
URL non autorisées, 449
filtres de catégories, 60
ajout, 93
création, 61
définition, 49
duplication, 60
modèles, 61, 66
modification, 61
renommer, 61
filtres de protocoles, 60
ajout, 94
création, 63
définition, 49
modèles, 63, 66
modification, 64
renommer, 64
filtres de recherche
filtrage hybride, 226
filtres de recherche des groupes, 226
filtres de recherche des utilisateurs, 226
format Excel
journal d'audit, 373
rapports d'investigation, 153, 174
rapports de présentation, 142, 145, 148
rapports incomplets, 492
rapports sur l'authentification du service hybride, 235, 236
format HTML
enregistrement des rapports de présentation, 493
rapports de présentation, 145
format HTML, rapports de présentation, 142
format PDF
rapports d'investigation, 153, 174, 176
rapports de présentation, 142, 145, 148
rapports sur l'authentification du service hybride, 235, 236
format XLS
journal d'audit, 373
rapports d'investigation, 153, 176
rapports de présentation, 142, 145
formulaire d'authentification sécurisée
filtrage hybride, 312

G

gestion des catégories, 253
gestion des protocoles
Network Agent, 432
gestion des stratégies et génération de rapports
autorisations, 327
type de rôle, 324
gestion du délai du contenu, 192
gestion du trafic crypté, 198

graphique à barres, 156
graphique Activité utilisateur : Zoom Trend (Tendance - Zoom), 43
graphique en secteurs, 156
graphiques
  30-Day Risk Trends (Tendance des risques sur 30 jours), 42
  activité utilisateur, 43
  ajout au tableau de bord, 44
  Filtering Service Status (État du service de filtrage), 44
graphiques des tableaux de bord
  période maximale, 418
  présentation, 129
groupes, 74
  LDAP personnalisés, 73
Groupes de protocoles de sécurité, 57
groupes LDAP personnalisés, 80
  ajout, 81
  modification, 81

I

identifiants réseau
  accès à TRITON - Web Security, 351
identificateurs
  protocole, 266
identificateurs de protocole, 266
  adresses IP, 267
  ports, 267
identification des utilisateurs
  dépannage, 453
  filtrage hybride, 311
  manuelle, 287
  rapports sur les utilisateurs hybrides, 234
  Service d'authentification, 317
  transparente, 286
  utilisateurs distants, 286
  Web Endpoint, 314
Identification des utilisateurs, page, 288
identification hybride des utilisateurs
  Active Directory, 221
  Novell eDirectory, 224
  Oracle Directory Server, 223
Identification NTLM
  filtrage hybride, 312
identification transparente
  filtrage hybride, 311
identification transparente des utilisateurs, 286
  agents, 286
  configuration, 288
  DC Agent, 295
  eDirectory Agent, 304
  exceptions, 288
  Logon Agent, 301
  RADIUS Agent, 303
  utilisateurs non identifiés, 289
impossible de
  ajouter des utilisateurs et des groupes, 457
impression
  graphiques des tableaux de bord, 385
  rapports d'investigation, 176
  rapports de présentation, 143
  tableau de bord, 34
Imprimer les stratégies dans un fichier, 91
informations de configuration de Websense, 360
informations sur le compte
  configuration, 25
  filtrage hybride, 204
informations sur les utilisateurs, journalisation, 398
intégration SIEM, 371
interface de ligne de commande de Directory Agent, 511

J

jeu de caractères
  MBCS, 439
jeux de caractères
  utilisés avec LDAP, 79
journal
  audit, 373
  client Remote Filtering, 239
journal d'audit, 373
journal d'erreurs
  Observateur d'événements, 516
  suppression pour la base de données d'activité, 413
  Websense.log, 516
journalisation
  accès, 405

anonyme, 399
catégorie sélective, 399
catégories, 398
comparaison des options d'analyse et de filtrage, 197
configuration, 398
plusieurs serveurs Policy Server, 398
définition, 395
informations sur les utilisateurs, 398
options d'analyse, 196
URL complètes, 404, 413
journalisation des protocoles
pour tous les rôles, 333
journalisation des URL complètes, 404, 413
impact sur la taille de la base de données, 417
journalisation sélective des catégories, 399
et taille de la base de données, 417

L

LDAP
groupes personnalisés, 80
jeux de caractères, 79
libérer les autorisations de stratégie, 335
limitation du temps d'accès, 58
Linking Service, 359
liste des tâches planifiées
rapports d'investigation, 174
rapports de présentation, 133
listes blanches, 103
gestion, 103
listes noires, 103
gestion, 103
localisation des informations sur le produit, 24
Log Server, 357
compte de base de données, 483
configuration, 396, 400, 492
connexion au service d'annuaire, 486
espace disque faible, 476
mise à jour de la connexion, 484
mises à jour des utilisateurs et des groupes, 405
ne s'exécute pas, 473
non installé, 477
logiciel Remote Filtering, 238
à l'extérieur du réseau, 239
au sein du réseau, 238
communication, 239
échec de fermeture, 239
échec de l'ouverture, 239
filtrage basé sur la bande passante, 238
ignorer le trafic FTP, 241
ignorer le trafic HTTPS, 241
intervalle d'expiration, 239
modification de l'intervalle de pulsations, 242
protocoles pris en charge, 238
pulsation, 238
logiciel Websense
composants, 354
logo
modification dans la page de blocage du filtrage hybride, 217
modification sur la page blocage, 123
rapports de présentation, 135
logo dans les rapports de présentation, 140
logo personnalisé
pages de blocage, 123
pages de blocage du filtrage hybride, 217
rapports de présentation, 135, 140
Logon Agent, 301, 358
autorisations, 460
configuration, 301
lots ayant échoué, 413

M

mémoire requise
téléchargement de la base de données, 444
Menaces
Event Details (Détails de l'événement), 37
menaces
dans les fichiers, 188
dans les pages Web, 187
identification, 35
message de blocage de protocole
à la place de la page de blocage, 465
messagerie
diffusion des rapports, 397
messages d'erreur
alertes de fonctionnement, 466
emplacement, 466
messages de blocage

création d'un élément personnalisé, 121
création d'un message alternatif, 125
des types de fichiers, 276, 278
modification de la taille des cadres, 122
personnalisation, 119
protocole, 118
messages de blocage alternatifs, 125
messages de blocage de protocole, 118
non affichage, 464
messages de blocage personnalisés, 121
méthodes de filtrage
combinaison, 205, 243
Microsoft Excel
rapports incomplets, 492
mise à jour de la base de données d'analyse, 195
mise à niveau
utilisateurs manquants, 439
mise en tunnel HTTP, 186
exceptions, 187
mises à jour
Base de données principale, 440
mises à jour de la base de données, 27
analyse, 195
en temps réel, 28, 385
sécurité en temps réel, 28, 385
Mises à jour de sécurité en temps réel, 385
mises à jour en temps réel de la base de données, 28, 385
mode mixte
Active Directory, 76
mode natif
Active Directory, 76
mode Status Monitor (Moniteur d'état), 46
modèle de recherche
rapports d'investigation, 494
modèles, 66
filtre de catégories, 61, 66
filtre de protocoles, 63, 66
modèles de filtres, 66
modification
contextes racine du service hybride, 225
destinations non filtrées, 213
domaines de messagerie (hybride), 216
emplacements filtrés, 208
filtres d'accès limité, 250
filtres de catégories, 61
filtres de protocoles, 64
paramètres des clients, 83
proxy explicite, 210
stratégies, 93
modification d'une catégorie d'URL, 260
modification de l'adresse IP
Policy Server, 363
modifications
enregistrement, 23
mise en cache, 23
revue, 23
modifications mises en cache, 22
modifier
filtre de catégories, 61
groupe LDAP personnalisé, 81
Modifier les catégories, bouton, 253
Modifier les protocoles, bouton, 253
mot de passe
réinitialisation, 470
mot de passe d'anti-altération, 315
mots-clés, 253, 258
blocage, 58
définition, 259
non bloqués, 448
verrouillage pour les rôles, 332
Multiplexer, 357

N

navigation dans TRITON - Web Security, 20
Ne jamais analyser, liste, 184
ajout de sites, 194
suppression des entrées, 194
NetBIOS
activation, 456
Network Agent, 355, 427
carte réseau de blocage, 432
carte réseau de surveillance, 432
communication avec Filtering Service, 451
configuration de carte réseau, 431
gestion des protocoles, 432
mémoire insuffisante, 452
ne s'exécute pas, 450
non installé, 450

non surveillance, 451
paramètres globaux, 429
paramètres locaux, 430
plus de 2 cartes réseau, 451
utilisation intensive du processeur, 452
nom de la source de données (DSN)
configuration, 401
nom du fichier
rapport de présentation planifié, 144
Novell eDirectory, 78
configuration hybride, 224

O

Observateur d'événements, 516
ODBC
pour l'insertion des enregistrements de journal, 402
onglet Paramètres, 22
onglet Principal, 22
optimisation des résultats des recherches, 226
options d'analyse, 187, 196
catégorisation du contenu, 184
découpage du contenu, 192
enregistrement des modifications, 195
rapports, 196
options d'analyse en temps réel
analyse des fichiers, 188
options de sortie
rapports d'investigation, 423
options des rapports d'investigation, 153
Oracle Directory Server
configuration hybride, 223
ordinateurs
clients, 71
ordre
filtrage, 98
outils
Accès à l'URL, 283
Analyser l'utilisateur, 283
Catégorie d'URL, 282
Rechercher un utilisateur, option, 284
Tester le filtrage, 283
Vérifier la stratégie, 282
outils de dépannage
boîte de dialogue Services, 515
Observateur d'événements, 516
websense.log, 516

P

page de blocage blanche, 117
page de blocage vide, 117
page vide à la place de la page de blocage, 464
pages de blocage, 115
accès par mot de passe, 84
affichage d'un message d'erreur, 463
bouton Continuer, 57
bouton Utiliser du temps contingenté, 58
changement de logo, 123
fichiers source, 119
filtrage hybride, 215
non affichée pour le blocage de type de fichier, 463
page blanche vide, 464
partielles, 117
personnalisation pour le service hybride, 217
publicités, 117, 464
réinitialisation des pages par défaut, 125
remplacement de compte, 84
variables du contenu, 123
pages de blocage du filtrage hybride
logo, 217
personnalisation, 217
texte, 217
paramètre du proxy
téléchargement de la base de données, 442
vérification, 442
paramètres
Alertes, 379
Authentification personnalisée, 229
base de données d'activité, 408
Compte, 25
Données utilisateur partagées, 221, 223, 224
Filtered Locations (Emplacements filtrés), 205
filtrage, 67
Identification des utilisateurs, 288
Identification hybride des utilisateurs, 311, 313
Network Agent, 429
Planification, 227
Policy Server, 361

Remote Filtering, 240
services d'annuaire, 75
tableau de bord, 418
Téléchargement de la base de données, 28
paramètres de contournement de catégories, 198
paramètres de filtrage
configuration, 67
paramètres de l'annuaire
avancés, 78
paramètres du pare-feu
téléchargement de la base de données, 442
paramètres du service d'annuaire
dépannage, 457
paramètres du tableau de bord, 418
partitions
base de données d'activité, 406
création, 410
options de remplacement, 409
sélection pour les rapports, 411
suppression, 411
partitions de base de données
activation ou désactivation, 491
partitions de la base de données
création, 410
options de remplacement, 409
sélection pour les rapports, 411
suppression, 411, 412
password
anti-altération, 315
période
graphiques des tableaux de bord, 418
personnaliser
fichier de configuration automatique des proxy (PAC), 219
messages de blocage, 119
pages de blocage du filtrage hybride, 217
plage de dates
tâche planifiée de rapports d'investigation, 174
tâche planifiée de rapports de présentation, 147
Planificateur de rapports de présentation
non connecté, 487
Planificateur, rapports de présentation, 144
planification
acheminement du trafic via un proxy ou un pare-feu, 228
arrêt des sauvegardes planifiées, 393
définition des stratégies, 93
sauvegardes, 388
synchronisation des annuaires hybrides, 227
synchronisation des enregistrements de journaux hybrides, 228
synchronisation des stratégies hybrides, 227
planification de la communication avec le service hybride, 227
Plug-in de filtrage, 359
plusieurs rôles, autorisations, 329
plusieurs serveurs Policy Server, 363
plusieurs stratégies
priorités du filtrage, 71
Policy Broker, 354
et la base de données des stratégies, 360
Policy Server, 355, 361
arrêt inopiné, 471
et la base de données des stratégies, 360
et TRITON - Web Security, 361
gestion des connexions à TRITON - Web Security, 362
modification de l'adresse IP, 363
plusieurs instances, 363
plusieurs instances, configuration de la journalisation, 398
suppression dans TRITON - Web Security, 362
portail MyWebsense, 24
préférences des rapports, 397
priorité
filtrage, 98
rôle d'administration déléguée, 343
stratégie de filtrage, 71
priorité des rôles, 336, 343
prise en charge TCP et UDP, 65
Protection étendue, 53
protocole
définitions, 264
gestion, 253
protocoles
ajout à la base de données principale, 52
collecte des informations d'utilisation, 26
création, 266
définition, 27, 51
définition d'éléments personnalisés, 253
définitions, 264

filtrage, 64, 265
Groupes de protocoles de sécurité, 57
journalisation pour tous les rôles, 333
liste exhaustive, 51
modification des protocoles définis par Websense, 270
non journalisés, 490
prise en charge TCP et UDP, 65
renommer un protocole personnalisé, 267
sélection pour les rapports d'investigation, 162
sélection pour les rapports de présentation, 138
utilisation de la bande passante, 270
verrouillage pour tous les rôles, 332, 333
protocoles personnalisés, 264
création, 268
identificateurs, 266
impossible de créer, 472
modification, 266
renommer, 267
proxy explicites
ajout, 210
filtrage hybride, 209
modification, 210
proxy Websense, 372
publicités bloquées, 117
publicités, blocage, 117
pulsation
logiciel Remote Filtering, 238
modification de l'intervalle, 242

R

RADIUS Agent, 303, 359
configuration, 303
rapport sur activité propre, 177, 342
activation, 397
configuration, 425
notification des utilisateurs, 425
rapport User Agents by Volume (Agents utilisateurs par volume), 229
rapport Volume par agent utilisateur, 235
rapports
absence des données du filtrage hybride, 505
accès, 395
Activité utilisateur par mois, 165
administrateur, 348
affichage des rapports de présentation planifiés, 151
authentification des agents utilisateurs hybrides, 235
authentification du service hybride, 234
autorisations, 327, 339, 351
autorisations, configuration, 339
blocage des fenêtres contextuelles, 496
configuration des rapports d'investigation, 421
configuration des rapports sur activité propre, 425
configuration du serveur de messagerie, 397
conservation, 144
d'investigation, 129
Détail de l'activité utilisateur par jour, 164
diffusion par e-mail, 397
expiration, 481
graphiques des tableaux de bord, 129
incomplets, 492
informations sur l'analyse, 197
modification, 132
options d'analyse, 196
page Review Reports (Examiner les rapports), 151
préférences, 397
présentation, 129
rapport sur activité propre, 342
Real-Time Monitor, 130, 178
récupération des données hybrides, 228
utilisation, 129
vides, 491
rapports Cas particuliers, 153, 175
rapports d'investigation, 152
activité utilisateur, 153
Activité utilisateur par mois, 165
affichage, options, 423
anonymes, 157
autorisations, 328
cas particuliers, 153, 175
choix d'une base de données d'activité, 421
configuration, 421
couleur rouge, 156
définition du planning des, 173

Détail de l'activité utilisateur par jour, 164
dissimulation des noms d'utilisateur, 157
enregistrement des Favoris, 170
favoris, 153, 170, 171
file d'attente des tâches, 153, 174
format Excel, 153, 174, 176
format PDF, 153, 174, 176
format XLS, 176
graphique à barres, 156
graphique en secteurs, 156
impression, 176
modèles de recherche, 494
options, 153
options de sortie, 423
paramètres par défaut, 422
personnalisation du courrier électronique, 173
présentation, 129
problèmes généraux, 494
rapport sur activité propre, 177, 425
récapitulatif, 154
récapitulatifs multi-niveaux, 158
recherche, 157, 494
standard, 153, 168
tâches planifiées, 153, 172
temps de navigation détaillé, 415
type de rôle, 324
vue détaillée, 159, 160, 161
rapports d'investigation, exploration, 154
rapports de présentation
affichage des rapports planifiés, 151
catalogue de rapports, 131
confirmation du filtre de rapport, 141
conservation, 144
copie, 132
définition d'une plage de dates pour une tâche, 147
échec des tâches planifiées, 488
en exécution, 142
enregistrement, 143
erreurs, 493
espace disque faible, 488
favoris, 132, 139, 141
file d'attente des tâches, 133, 149
filtre de rapport, 132, 135
format de sortie, 148
format Excel, 142, 143, 148
format HTML, 142, 145
format PDF, 142, 145, 148
format XLS, 142, 145
historique des tâches, 150
impression, 143
logo personnalisé, 135, 140
nom du catalogue de rapports, 139
nom du fichier, 144
non affichage, 493
page Review Reports (Examiner les rapports), 151
personnalisés, 132
planification, 133, 144, 145
présentation, 129
Review Reports (Examiner les rapports), 133
utilisation de l'espace disque, 145
rapports de présentation, titre, 139
rapports de tendances
activation, 416
vides, 490
rapports récapitulatifs
multi-niveaux, 158
rapports d'investigation, 154
rapports standard d'investigation, 153, 168
Real-Time Monitor, 178, 357
démarrage et arrêt, 375
mémoire faible, 495
ne s'exécute pas, 495
pas de données, 469
plusieurs serveurs Policy Server, 180
présentation, 130
sans réponse, 496
Real-Time Security Updates, 28
activation, 29
recherche
clients de l'annuaire, 82
dans la barre d'adresse, 448
rapports d'investigation, 157, 494
recherche d'utilisateur, 82
référentiel d'analyse, 420
configuration de la taille, 420
emplacement, 497

erreurs, 497
expiration des données, 498
réindexation de la base de données d'activité, 412
Remote Filtering, paramètres, 240
Bloquer toutes les requêtes, 240
intervalle d'expiration, 240
remplacement de compte, 84
dans un environnement à plusieurs serveurs Policy Server, 363
plusieurs instances de Filtering Service, 366
remplacement des partitions de base de données, options, 409
remplacer une action
catégories, 256
protocoles, 267
renommer
catégorie, 256
filtres d'accès limité, 250
filtres de catégories, 61
filtres de protocoles, 64
protocole personnalisé, 267
stratégies, 93
répertoire bin de Websense, 515
répertoires d'installation, 377
répliques du serveur eDirectory
configuration, 306
requêtes bloquées
bande passante journalisée, 155
requêtes bloquées, bande passante journalisée, 163
réseaux
clients, 71
restauration des données Websense, 386, 391
restauration, utilitaire, 386
exécution, 391
références des commandes, 393
résumé sur les alertes d'état, 43
retrait
contenu actif, 192
contenu VB Script, 192
entrées des listes Toujours analyser ou Ne jamais analyser, 194
instances de Policy Server via TRITON - Web Security, 362
Review Reports (Examiner les rapports), 151
rapports de présentation, 133
Risques de sécurité
filtrage des sites, 262
risques de sécurité
analyse des, 187
rôles
administrateurs attribués à plusieurs rôles, 340
administratifs, 324
affichage de la définition, 348
ajout, 335, 336
ajout d'administrateurs, 337, 340
ajout de clients gérés, 338, 342, 346, 348
application des stratégies, 346, 350
changement, 327
chevauchement de clients, 349
clients dans plusieurs rôles, 343
création de filtres, 350
création de stratégies, 350
gestion des stratégies et génération de rapports, 324
modification, 337
modification des filtres, 349
modification des stratégies, 349
noms, 335
priorité, 336, 343
rapports d'investigation, 324
retrait de clients, 338
Super administrateur, 324
suppression, 335
suppression d'administrateurs, 337
suppression du Super administrateur, 324, 345
suppression, effets, 345
verrouillage de catégories, 332
verrouillage des protocoles, 333
Verrouillage du filtre, effets, 331
rôles d'administration, 324

S

sauvegarde des données Websense, 386
sauvegarde, utilitaire, 386
arrêt des sauvegardes planifiées, 393
exécution, 390
fichier de configuration, 391
planification des sauvegardes, 388
références des commandes, 393

Save and Deploy (Enregistrer et déployer), 22
securewispproxy.ini, fichier, 241, 242
Security Events by Type (Événements de sécurité par type), 35
SecurityCategoryOverride, 262
serveur d'interruption
  configuration d'alertes SNMP, 379
serveur proxy
  configuration du téléchargement de la base de données, 29
Serveur Remote Filtering, 238, 356
service d'annuaire
  problèmes de configuration, 457
Service d'authentification
  définition, 317
  déploiement, 318
Service de filtrage, 355, 365
  connexions à Content Gateway, 366
  graphique d'état, 44
  informations sur la version, 366
  page de détails, 366
  téléchargement de la base de données, 366
services
  arrêt et démarrage, 375
services d'annuaire
  configuration, 75
  configuration pour la connexion à TRITON - Web Security, 352
  connexion de Log Server, 486
  pris en charge pour le filtrage hybride, 220
  recherche, 82
  Windows Active Directory (en mode mixte), 76
session
  délai d'expiration, 46
  navigation, 415
session de navigation, 415
signatures des fichiers
  filtrage par, 273
sites HTTPS
  filtrage personnalisé, 449
SQL Server
  autorisations, 479, 485
  compte de base de données, 483
SQL Server Agent
  tâche, 491
SQL Server Agent, tâche, 485
State Server, 356
Status Monitor (Moniteur d'état), 34
stockage des données d'analyse, 420
stockage des fichiers de sauvegarde, 391
stratégie non limitée, 89
stratégie Par défaut, 90
stratégies
  affichage, 91
  ajout, 91, 92
  application aux clients, 93, 95
  application aux clients gérés, 346, 350
  application aux utilisateurs et aux groupes, 74
  copie vers des rôles, 91, 344
  copier dans le rôle, 252
  création pour un rôle, 350
  définition, 49, 89
  dépannage des clients de l'annuaire, 449
  dépannage des clients distants, 449
  descriptions, 92
  détermination de l'application, 95
  Exemple - Utilisateur standard, 89
  illimitées, 89
  imposer, 95
  imprimer dans un fichier, 91
  lorsque l'utilisateur n'est pas identifié, 289
  modification, 91, 93
  modification pour le rôle, 349
  Par défaut, 90
  plusieurs groupes, 96
  priorités du filtrage, 98
  renommer, 93
stratégies de plusieurs groupes, 96
suivi
  activité Internet, 377
  modifications du système, 373
Sun Java System Directory, 78
Super administrateur
  admin, 19
  ajout de clients au rôle, 344
  autorisations, 326
  autorisations conditionnelles, 326
  changement de rôle, 327
  déplacement de clients depuis un rôle, 86

inconditionnel, 327
rôle, 324
suppression du rôle, 324, 345
Verrouillage du filtre, effets, 331
super administrateur inconditionnel, 326
super administrateurs conditionnels
autorisations, 326
support client, 31
support technique, 31
suppression d'entrées des listes Toujours analyser et Ne jamais analyser, 196
surveiller l'activité Internet, 178
Suspicious Event Summary (Résumé des événements suspects), 35
colonnes, 37
filtres, 36
Sync Service, 220, 359
configuration, 227
espace disque faible, 506
fichier de configuration, 506
impossible de se connecter à Log Server, 505
impossible de se connecter au service hybride, 513
impossible de télécharger les journaux, 504
informations sur l'état, 233
non disponible, 503
syncservice.ini, 506
BlockMessageBoardPosts, paramètre, 264
SecurityCategoryOverride, paramètre, 263

T

tableau de bord, 33
Add Chart (Ajouter un graphique), 34
ajout d'éléments, 44
calcul des économies de bande passante, 46
calcul des estimations de l'utilité, 45
calculs des économies de temps, 46
graphiques non affichés, 496
impression, 34
Menaces, 35
personnalisation des onglets, 44
Risques, 33, 42
Status Monitor (Moniteur d'état), 34
surveillance, 46
Système, 33, 34, 43
Téléchargement de la base de données, 34
Usage, 33, 42
tableau de bord Risques, 42
tableau de bord Système, 43
Tableau de bord Threats (Menaces), 35
filtres, 35
tableau de bord Usage, 42
Tableau de bord Web Security
graphiques non affichés, 496
tâche AMT
base de données d'activité, 408
tâche de maintenance
base de données d'activité, 407, 412
configuration, 412
tâche ETL (Extract, Transform, and Load), 407
tâche trend
base de données d'activité, 408
tâches
base de données d'activité, 407
ETL, 407
IBT, 407
maintenance de la base de données d'activité, 407
rapports d'investigation planifiés, 172, 174
rapports de présentation planifiés, 144, 149
SQL Server Agent, 491
tâche AMT de la base de données d'activité, 408
tendances de la base de données d'activité, 408
tâches de base de données
AMT, 408
ETL, 407
maintenance, 407
SQL Server Agent, 491
Temps de navigation Internet (IBT), 407
tendance, 408
tâches planifiées
activation, 150
désactivation, 150
échec pour les rapports de présentation, 488
format de sortie, 148
historique des tâches, 150
nom des fichiers de rapport, 144
perdues, 487

personnalisation du courrier électronique, 148, 173
plage de dates, 147, 174
planification, 145, 173
rapports d'investigation, 153, 172
rapports de présentation, 144, 147, 149
suppression, 150
taille de la base de données d'activité, 417
taille maximale d'analyse des fichiers, 192
Technologies de l'information
catégorisation inappropriée des sites, 448
Téléchargement de la base de données, 34
téléchargement de la base de données, 27
analyse, 195
configuration, 28
dépannage, 440
espace disque nécessaire, 443
état, 366
mémoire requise, 444
mises à jour en temps réel, 28
problèmes d'abonnement, 441
problèmes d'applications restrictives, 444
Real-Time Security Updates, 28
reprise, 367
vérification de l'accès Internet, 441
via un serveur proxy, 29
temps contingenté, 58
applets, 59
application aux clients, 58
dans un environnement à plusieurs serveurs Policy Server, 363
plusieurs instances de Filtering Service, 366
sessions, 58
temps de navigation détaillé, 415
impact sur la taille de la base de données, 417
temps de navigation du dernier site, 415
Temps de navigation Internet (IBT)
configuration, 414
définition, 130
dernier site, 415
et consolidation, 489
rapports, 414
tâche de base de données, 130
temps par site, 415
temps de navigation moyen, 415
Tendance des risques sur 30 jours, 42
Tester le filtrage
Rechercher un utilisateur, 284
Tester le filtrage, outil, 283
titre des rapports de présentation, 139
Top Security Destinations (Principales destinations de sécurité), 35
Toujours analyser, liste
ajout de sites, 194
suppression des entrées, 194
TRITON - Web Security, 18, 356
accès avec un compte réseau, 351
accès simultané des administrateurs, 329
connexion, 19
connexions à Policy Server, 361
désactivation de l'expiration, 46
expiration des sessions, 19
gestion des connexions à Policy Server, 362
navigation, 20
types de fichiers, 253
ajout, 279
blocage, 58
modification, 279
verrouillage pour les rôles, 333

U

URL de sécurité
suivi, 26
URL non catégorisées
rapports, 26
URL non filtrées
pour le filtrage hybride, 212
remplacement, 103
URL personnalisées
définition, 260
non filtrées correctement, 449
priorités du filtrage, 261
URL recatégorisées, 260
ajout, 260
définition, 253
modification, 260
non appliquées, 472
Usage Monitor, 356
ne s'exécute pas, 469

non disponible, 469
User Service, 74, 358
autorisations, 460
non disponible, 446
paramètres WINS, 461
ports de communication de l'annuaire, 458
sous Linux, 461
utilisateur par défaut, 324
suppression, 324
Utilisateur par jour/mois, rapports, 153, 163
utilisateurs, 74
authentification manuelle, 287
identification, 285
identification transparente, 286
utilisateurs distants
filtrage, 237
filtrage incorrect, 462
problèmes d'authentification manuelle, 462
utilisateurs hors site
activation du filtrage hybride pour, 216
auto-enregistrement (hybride), 243
configuration du logiciel Remote Filtering, 238
identification (hybride), 220, 243
options de filtrage, 237
utilisateurs itinérants
filtrage, 237
utilisateurs manquants
après une mise à niveau, 439
utilisateurs mobiles
filtrage, 237
utilisateurs non identifiés, 289
Utiliser des filtres personnalisés, 79
utiliser du temps contingenté, 58
bouton de la page de blocage, 58
Utiliser le blocage le plus restrictif, 248
avec les filtres d'accès limité, 248
utilitaires
configuration de Log Server, 400

V

Vérifier la stratégie
Rechercher un utilisateur, 284
Vérifier la stratégie, outil, 282
Verrouillage du filtre
configuration, 330
création, 326, 332
effet sur les rôles, 350
journalisation des protocoles, 333
verrouillage de catégories, 332
verrouillage des mots-clés, 332
verrouillage des protocoles, 333
verrouillage des types de fichiers, 333
vue détaillée
colonnes, 161
configuration des paramètres par défaut, 422
modification, 160
rapports d'investigation, 159

W

Web Endpoint
définition, 314
déploiement, 314
Web Security
alertes système, 380
répertoires d'installation, 377
WebCatcher, 26, 30
données envoyées, 30
méthode d'envoi des données, 30
websense.log, 516
WebsenseAdmin, commande, 376
WebsenseDaemonControl, commande, 376
Windows
boîte de dialogue Services, 515
Observateur d'événements, 516
Windows Active Directory (en mode mixte), 76
Windows Active Directory (en mode natif), 76
WINS
activation, 461
configuration des paramètres de User Service, 461