AUTHORIZED DOCUMENTATION

Aide de la console de gestion

August 1, 2008

Novell®
ZENworks Endpoint Security Management

3.5

www.novell.com

Mentions légales

Novell, Inc. n'accorde aucune garantie, explicite ou implicite, quant au contenu et à l'utilisation de cette documentation, y compris toute garantie de bonne qualité marchande ou d'aptitude à un usage particulier. Novell se réserve en outre le droit de réviser cette publication à tout moment et sans préavis de ces modifications à quiconque.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans préavis de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous vous engagez à respecter toutes les réglementations de contrôle des exportations et à vous procurer les licences et classifications nécessaires pour exporter, réexporter ou importer des produits livrables. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes noires d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous à la page Web des services de commerce international de Novell (http://www.novell.com/info/exports/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.

Novell, Inc. dispose de droits de propriété intellectuelle sur la technologie intégrée dans le produit décrit dans ce document. En particulier et sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains mentionnés sur le site Web Novell relatif aux mentions légales (http://www.novell.com/company/legal/patents/) (en anglais) et un ou plusieurs brevets supplémentaires ou en cours d'homologation aux États-Unis et dans d'autres pays.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

Documentation en ligne : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site Novell de documentation (http://www.novell.com/documentation).

Marques de Novell

Pour connaître les marques commerciales de Novell, reportez-vous à la liste des marques commerciales et des marques de service de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Éléments tiers

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.

Tables des matières

1 Utilisation de la console de gestion ZENworks Endpoint Security Management

La console de gestion est le point central d'accès et de commande du service de gestion Novell® ZENworks® Endpoint Security Management.

Pour ouvrir la fenêtre de login de la console de gestion, cliquez sur *Démarrer* > *Tous les programmes* > *Novell* > *Console de gestion ESM* > *Console de gestion*. Loguez-vous à la console en spécifiant le nom et le mot de passe de l'administrateur. Le nom d'utilisateur entré doit être un utilisateur autorisé pour le service de gestion (reportez-vous à la rubrique Section 1.3, « Utilisation des paramètres d'autorisations », page 10).

Remarque : Nous vous recommandons de fermer ou de réduire la console lorsque vous ne l'utilisez pas.

1.1 Utilisation de la barre des tâches

La barre des tâches à gauche donne accès aux tâches de la console de gestion. Si la barre des tâches n'est pas visible, cliquez sur le bouton *Tâches* du côté gauche de la console.

Les sections suivantes contiennent un complément d'informations sur les tâches que vous pouvez effectuer à l'aide de la barre prévue à cet effet :

- Section 1.1.1, « Tâches Stratégie », page 8
- Section 1.1.2, « Ressources », page 8
- Section 1.1.3, « Configuration », page 8
- Section 1.1.4, « Audit du noeud d'extrémité », page 9

1.1.1 Tâches Stratégie

La fonction primaire de la console de gestion est de créer et d'appliquer des stratégies de sécurité aux périphériques du noeud d'extrémité géré. Les tâches Stratégie guident l'administrateur dans la création et l'édition de stratégies de sécurité que ZENworks Security Client utilise pour appliquer la sécurité gérée de façon centrale à chaque noeud d'extrémité.

Les tâches Stratégie sont les suivantes :

- **Stratégies actives :** affiche une liste des stratégies actuelles pouvant être révisées et modifiées. Cliquez sur une stratégie pour l'ouvrir.
- **Créer une stratégie :** démarre l'assistant de création de stratégie qui vous permet de créer une stratégie de sécurité.
- **Importer la stratégie :** affiche une boîte de dialogue Importer une stratégie qui vous permet d'importer des stratégies créées avec d'autres services de gestion. Pour plus d'informations, reportez-vous à Section 2.3.1, « Importation de stratégies », page 111.

Le fait de cliquer sur une tâche Stratégie réduit la barre des tâches. Cliquez sur le bouton *Tâches* sur le côté gauche pour la rouvrir.

Reportez-vous à la rubrique Chapitre 2, « Création et distribution des stratégies de sécurité », page 47 pour plus d'informations sur les tâches Stratégie et sur la création et la gestion des stratégies de sécurité.

1.1.2 Ressources

La liste des tâches Ressources affiche le support technique et les ressources d'aide disponibles :

- **Contacter le support :** lance un navigateur et affiche la page de contact et de bureaux Novell®.
- **Support technique en ligne :** lance un navigateur et affiche la page de support et de formation Novell.
- **Aide de la console de gestion :** lance l'aide en ligne de ZENworks® Endpoint Security Management.

1.1.3 Configuration

La fenêtre de configuration du service de gestion fournit des commandes tant pour l'infrastructure du serveur ZENworks® Endpoint Security Management que pour la surveillance d'autres services Annuaire d'entreprise. Pour plus d'informations, reportez-vous à Section 1.4, « Utilisation de la

fenêtre de configuration », page 14. Cette commande n'est pas disponible lorsque la console de gestion est exécutée en mode autonome. Pour plus d'informations, reportez-vous au *Guide d'installation de ZENworks Endpoint Security Management*.

1.1.4 Audit du noeud d'extrémité

La fenêtre Audit du noeud d'extrémité vous permet d'accéder aux fonctionnalités de rapport et d'alerte de ZENworks® Endpoint Security Management.

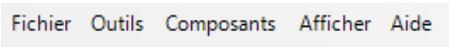
Génération de rapports : la création de rapport est essentielle à l'évaluation et à la mise en œuvre de stratégies de sécurité efficaces. Pour accéder aux rapports, cliquez sur *Rapports* dans la console de gestion. Les informations de sécurité du noeud d'extrémité rassemblées et communiquées sont également entièrement configurables et peuvent être collectées par domaine, groupe ou utilisateur individuel. Pour plus d'informations, reportez-vous à Section 1.6, « Utilisation du service de création de rapport », page 29.

Alertes : la surveillance des alertes garantit la consignation dans la console de gestion de toutes les tentatives de corruption des stratégies de sécurité de l'entreprise. Les alertes avertissent l'administrateur ZENworks Endpoint Security Management des problèmes potentiels, lequel peut prendre les actions correctives qui s'imposent. Totalement configurable, le tableau de bord des alertes permet de contrôler le moment et la fréquence de déclenchement des alertes. Pour plus d'informations, reportez-vous à Section 1.5, « Utilisation de la surveillance des alertes », page 25.

1.2 Utilisation de la barre de menus

La barre de menus ZENworks® Endpoint Security Management permet d'accéder à toutes les fonctions de la console de gestion.

Les options disponibles sont les suivantes :



- **Fichier :** le menu Fichier permet de créer et de gérer des stratégies de sécurité.
  - **Créer une nouvelle stratégie :** lance l'assistant de création de stratégie qui vous permet de créer une stratégie de sécurité.
  - **Rafraîchir la liste des stratégies :** met à jour la liste de stratégies pour afficher toutes les stratégies actives
  - **Supprimer la stratégie :** supprime la stratégie sélectionnée.
  - **Importer la stratégie :** permet d'importer une stratégie dans la console de gestion.
  - **Exporter une stratégie :** permet d'exporter une stratégie et le fichier `setup.sen` requis vers un emplacement spécifié à l'extérieur de la base de données du service de gestion.
  - **Quitter :** ferme le logiciel de la console de gestion et délogue l'utilisateur.
- **Outils :** le menu Outils permet de contrôler les autorisations, les clés de codage et la configuration du service de gestion.
  - **Configuration :** ouvre la fenêtre de configuration.
  - **Exporter les clés de codage :** ouvre la boîte de dialogue Exporter les clés de codage dans laquelle vous indiquez les clés à exporter et le mot de passe.

- **Importer des clés de codage :** ouvre la boîte de dialogue Importer les clés de codage dans laquelle vous indiquez les clés à importer et le mot de passe.
- **Générer la clé :** génère une clé de codage à utiliser pour la protection des données.
- **Autorisations :** ouvre la fenêtre des autorisations.

- **Afficher :** le menu Afficher permet d'exécuter des tâches Stratégie clés sans utiliser la barre des tâches.
  - **Stratégie :** lorsqu'une stratégie est ouverte, fait basculer l'affichage vers cette stratégie.
  - **Stratégies actives :** affiche la liste des stratégies.
  - **Alertes :** affiche le tableau de bord des alertes.
  - **Génération de rapports :** affiche le tableau de bord des rapports.
- **Aide :** affiche l'outil d'aide de la console de gestion et à la fenêtre À propos de.
  - **Aide :** lance l'aide en ligne de la console de gestion qui peut vous guider dans la création de stratégies ainsi que dans les tâches de la console de gestion. L'aide est également disponible en appuyant sur la touche F1 de votre clavier.
  - **À propos de la console de gestion :** ouvre la fenêtre du même nom, qui affiche le type d'installation (ZENworks Endpoint Security Management ou UWS) et le numéro de version actuel de la console de gestion. C'est également dans cette fenêtre que l'utilisateur entre la clé de licence si elle est achetée après l'installation.

1.3 Utilisation des paramètres d'autorisations

Figurant dans le menu Outils, cette option n'est accessible que par l'administrateur principal du service de gestion et par tout autre administrateur à qui celui-ci a accordé des « autorisations ». Cette commande n'est pas disponible lorsque la console de gestion est exécutée en mode autonome.

Les paramètres des autorisations définissent quel utilisateur ou groupe d'utilisateurs est autorisé à accéder à la console de gestion, aux autorisations administratives ou aux paramètres de publication.

Pendant l'installation du serveur de gestion, un nom de compte de ressource ou d'administrateur pour l'utilisateur de la ressource est entré dans l'écran de configuration (reportez-vous au *guide d'installation de ZENworks Endpoint Security Management*). Une fois le test réussi et les informations utilisateur enregistrées, toutes les autorisations sont automatiquement accordées à cet utilisateur.

Dès que la console de gestion est installée, l'utilisateur de la ressource est le seul utilisateur à disposer d'autorisations complètes, même si tous les groupes d'utilisateurs au sein du domaine ont accès à la console de gestion. L'utilisateur de la ressource doit supprimer l'accès de tous les groupes ou utilisateurs ne devant pas disposer d'un accès. L'utilisateur de la ressource peut définir d'autres autorisations pour les utilisateurs désignés.

Au lancement de la console de gestion, les autorisations sont récupérées de la table des autorisations. Ces autorisations indiquent à la console si l'utilisateur dispose des droits nécessaires pour se loguer à la console, pour créer ou supprimer des stratégies, pour modifier des paramètres d'autorisations et s'il peut éventuellement publier des stratégies et pour qui.

Les paramètres d'accès disponibles sont les suivants :

- **Accès à la console de gestion :** l'utilisateur peut consulter des stratégies et des composants et éditer des stratégies existantes. Les utilisateurs ayant uniquement obtenu ce privilège ne sont pas autorisés à ajouter ou supprimer des stratégies ; les options relatives à la publication et aux autorisations ne sont pas disponibles.
- **Publier des stratégies :** l'utilisateur ne peut publier des stratégies que pour des utilisateurs ou groupes assignés.
- **Modifier des autorisations :** l'utilisateur peut accéder aux autorisations d'autres utilisateurs ayant déjà été définis et les modifier ou encore en octroyer à de nouveaux utilisateurs.
- **Créer des stratégies :** l'utilisateur peut créer de nouvelles stratégies dans la console de gestion.
- **Supprimer des stratégies :** l'utilisateur peut supprimer n'importe quelle stratégie dans la console de gestion.

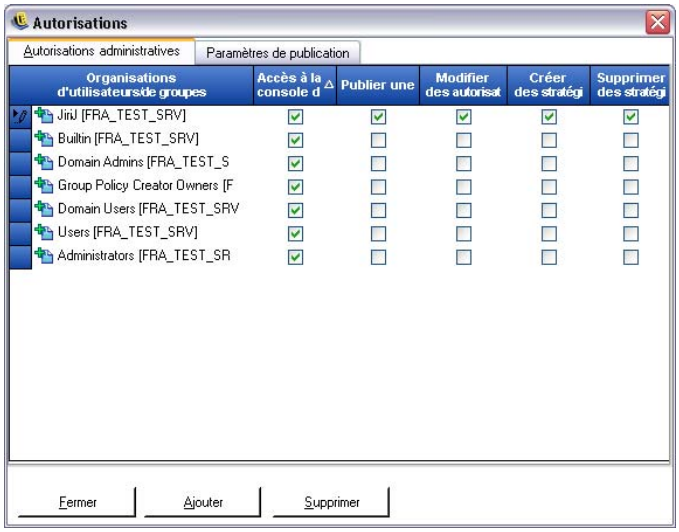
Remarque : Pour des raisons de sécurité, il est recommandé que seul l'utilisateur de la ressource ou un nombre limité d'administrateurs se voient accorder les autorisations de modification des autorisations et de suppression des stratégies.

1.3.1 Autorisations administratives

Pour définir des autorisations administratives :

1 Cliquez sur *Outils* > *Autorisations*.

Les groupes associés au domaine s'affichent.

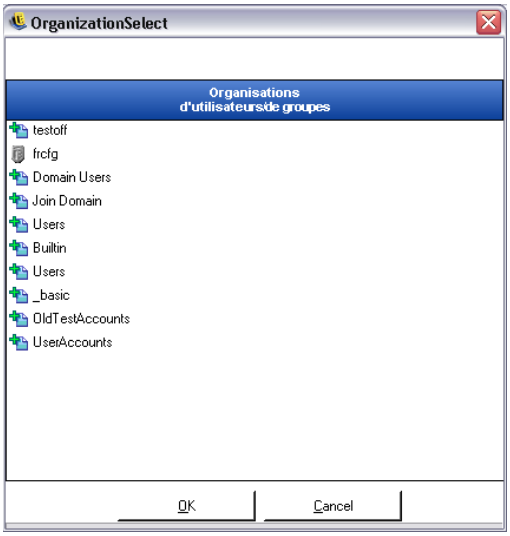


Remarque : Tous les groupes se voient par défaut accorder l'accès à la console de gestion sans pour autant pouvoir exécuter de tâches Stratégie. L'accès à la console peut être supprimé en désélectionnant l'autorisation.

---

2 Pour ajouter des utilisateurs/groupes à cette liste :

2a Cliquez sur le bouton *Ajouter* au bas de l'écran.



2b Sélectionnez les utilisateurs ou groupes appropriés dans la liste. Pour sélectionner plusieurs utilisateurs, sélectionnez-les un à un en maintenant la touche Ctrlenfoncée, ou par groupe, en sélectionnant le premier utilisateur souhaité, puis en maintenant la touche Maj enfoncée et en sélectionnant le dernier utilisateur souhaité.

2c Une fois tous les utilisateurs/groupes sélectionnés, cliquez sur le bouton *OK*.

3 Assignez des autorisations (voire toutes) aux utilisateurs ou groupes disponibles.

Pour supprimer un utilisateur ou groupe sélectionné, sélectionnez son nom, puis cliquez sur *Supprimer*. Le nom sélectionné est replacé dans la table organisationnelle.

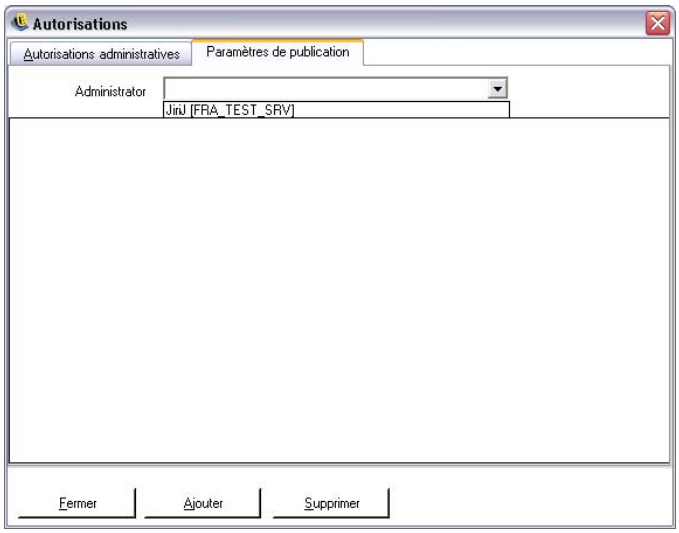
1.3.2 Paramètres de publication

Les utilisateurs ou groupes pour lesquels l'option *Publier des stratégies* est cochée doivent se voir assigner des utilisateurs ou des groupes pour qui publier.

Pour définir les paramètres de publication :

1 Cliquez sur l'onglet *Paramètres de publication*.

2 Sélectionnez dans la liste déroulante les utilisateurs ou groupes ayant reçu l'autorisation de publication.



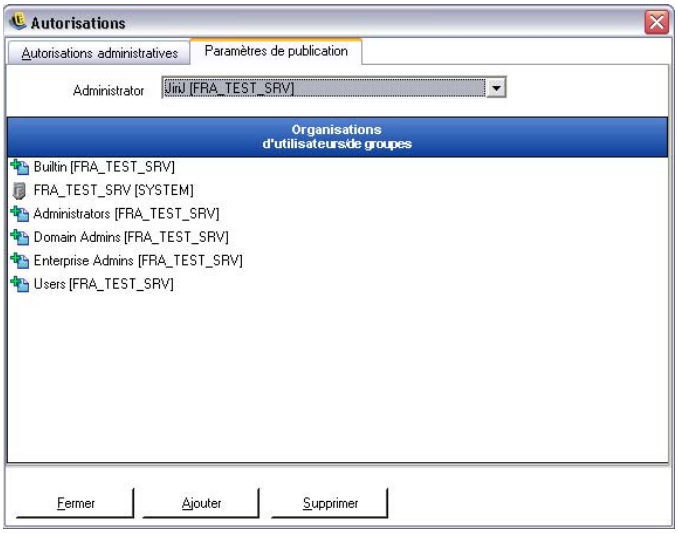
3 Assignez des utilisateurs ou groupes à cet utilisateur/groupe :

3a Cliquez sur le bouton *Ajouter* au bas de l'écran pour afficher la table organisationnelle.

3b Sélectionnez les utilisateurs ou groupes appropriés dans la liste. Vous pouvez utiliser les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs.

3c Lorsque tous les utilisateurs ou groupes ont été sélectionnés, cliquez sur le bouton *OK* pour ajouter les utilisateurs et groupes à la liste de publication

.



Les paramètres d'autorisations sont immédiatement mis en œuvre.

4 Pour supprimer un utilisateur ou groupe sélectionné, sélectionnez son nom, puis cliquez sur *Supprimer*.

5 Cliquez sur *Fermer* pour accepter les modifications et revenir à l'éditeur.

Le nom sélectionné est replacé dans la table organisationnelle.

En cas d'ajout d'un nouveau service Annuaire (voir « Annuaires d'authentification » page 16), le compte de ressource entré se voit accorder des paramètres d'autorisations complètes, comme décrit ci-dessus.

1.4 Utilisation de la fenêtre de configuration

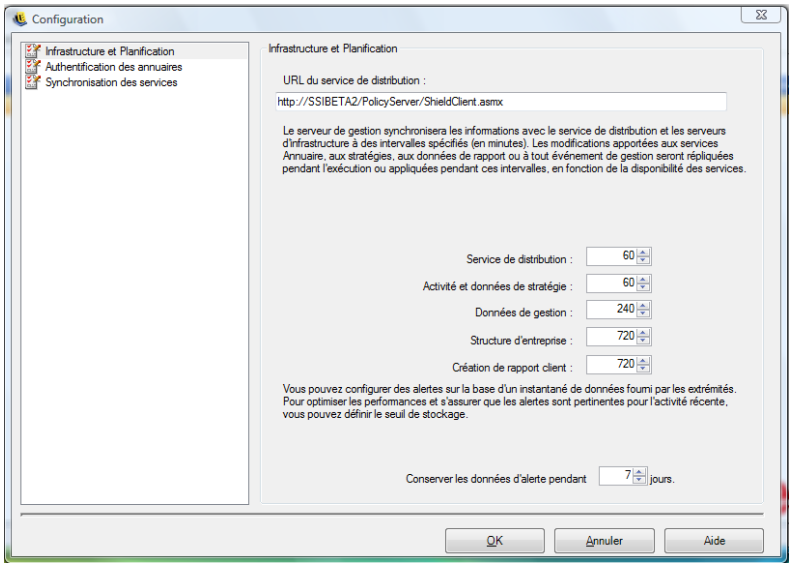
La fenêtre de configuration permet à l'administrateur ZENworks® Endpoint Security Management d'accéder aux commandes *Infrastructure et planification*, *Annuaires d'authentification* et *Synchronisation des services*. Cliquez sur le lien *Configuration* sur la page principale ou cliquez sur le menu *Outils*, puis sur *Configuration*. La fenêtre de configuration s'affiche.

Remarque : Cette fonction n'est pas disponible avec une console de gestion en mode autonome.

Les sections suivantes contiennent davantage d'informations :

1.4.1 Infrastructure et planification

Le module Infrastructure et planification permet à l'administrateur ZENworks Endpoint Security Management de désigner et de modifier l'URL du service de distribution de stratégies et de contrôler les intervalles de synchronisation des composants ZENworks Endpoint Security Management.



Les sections suivantes contiennent davantage d'informations :

URL du service de distribution

Le paramètre *URL du service de distribution* met à jour l'emplacement du service de distribution de stratégies tant pour le service de gestion que pour tous les clients ZENworks Security Client (sans nécessiter leur réinstallation) lorsque le service de distribution de stratégies est déplacé vers un nouveau serveur. L'URL du serveur actuel figure dans la zone de texte.

Si vous devez changer de serveur, ne modifiez que son nom et faites-le pointer vers le nouveau serveur. Ne modifiez aucune information après le nom du serveur.

Par exemple, si l'URL actuelle est `http:\\ACME\PolicyServer\ShieldClient.asmx` et que le service de distribution de stratégies est installé sur un nouveau serveur, ACME 43, l'URL doit être remplacée par : `http:\\ACME43\PolicyServer\ShieldClient.asmx`

Une fois l'URL mise à jour, cliquez sur *OK* pour mettre à jour toutes les stratégies et envoyer une mise à jour automatique du service de distribution de stratégies. Cette opération permet également de mettre à jour le service de gestion.

Lors de la modification de l'URL du serveur, il est recommandé de ne pas arrêter l'ancien service de distribution de stratégies tant que les stratégies mises à jour n'affichent pas un niveau d'adhésion total (reportez-vous à la section Section 1.6, « Utilisation du service de création de rapport », page 29).

Planification

Les composants de planification permettent à l'administrateur ZENworks Endpoint Security Management de définir à quel moment le service de gestion se synchronise avec d'autres composants ZENworks Endpoint Security Management, afin de garantir que toutes les données et que tous les travaux en attente reflètent les activités récentes et de planifier les travaux de maintenance SQL. Tous les incréments horaires sont exprimés en minutes.

Le processus de planification comprend les éléments suivants :

- **Service de distribution :** planification de la synchronisation avec le service de distribution de stratégies.
- **Activité et données de stratégie :** planification de la synchronisation avec les mises à jour de stratégies.
- **Données de gestion :** synchronisation des stratégies avec le service de gestion.
- **Structure d'entreprise :** planification de la synchronisation avec le service Annuaire de l'entreprise (eDirectory™, Active Directory*, Domaine NT* et/ou LDAP). Les changements au niveau du service Annuaire de l'entreprise sont contrôlés de manière à détecter les modifications correspondantes des assignations des stratégies utilisateur et à les envoyer au service de distribution de stratégies à des fins d'authentification client.
- **Rapports client :** fréquence à laquelle le service de gestion interroge et télécharge des données de rapport du service de distribution de stratégies.
- **Conserver les données d'alerte pendant :** vous pouvez configurer des alertes sur la base d'un instantané de données signalé par les noeuds d'extrémité. Pour optimiser les performances et veiller à la pertinence des alertes par rapport aux activités récentes, vous pouvez définir le niveau de stockage en fonction d'un nombre de jours.

1.4.2 Annuaires d'authentification

Après avoir installé ZENworks® Endpoint Security Management, vous devez créer et configurer un service Annuaire avant de pouvoir gérer les périphériques de votre système.

L'assistant de nouvelle configuration du service Annuaire permet de créer une configuration de service Annuaire qui définit la portée de vos installations du client ZENworks Endpoint Security Management. La nouvelle configuration utilise votre service Annuaire existant pour définir la limite logique à appliquer à vos installations du client basées sur les utilisateurs ou sur les ordinateurs.

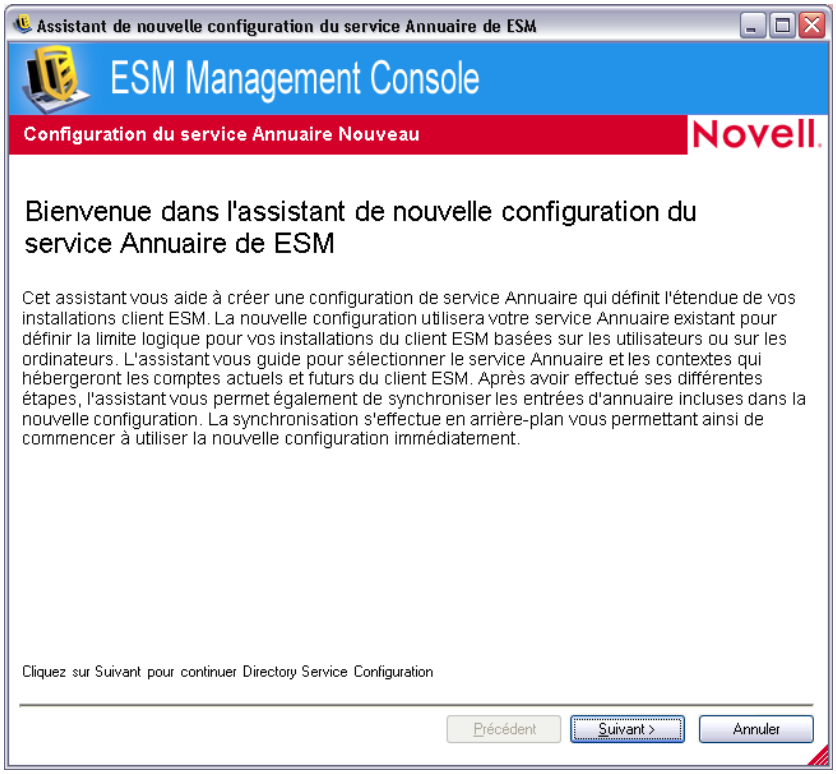
L'assistant vous guide pour sélectionner le service Annuaire et les contextes qui hébergeront les comptes actuels et futurs du client.

L'assistant vous permet également de synchroniser les entrées d'annuaire présentes dans la nouvelle configuration. Cette synchronisation s'effectue en arrière-plan, vous permettant ainsi de commencer à utiliser la nouvelle configuration sans plus tarder.

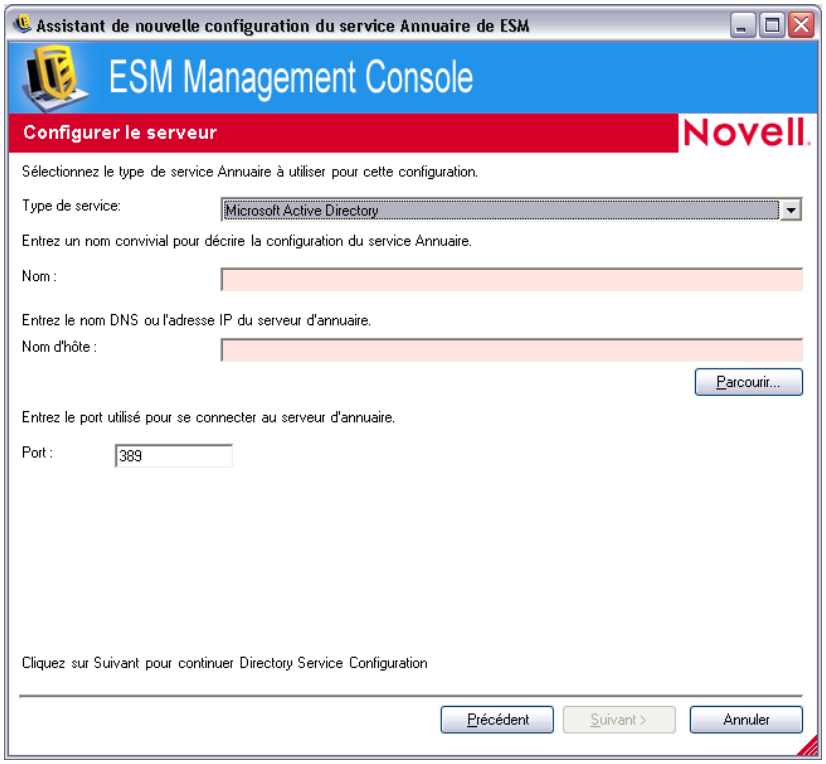
Dès que vous avez installé ZENworks Endpoint Security Management, l'assistant de nouvelle configuration du service Annuaire s'affiche automatiquement. Si vous venez d'installer le produit et que la page d'accueil s'affiche, passez à l'Étape 4 dans la procédure suivante.

Pour configurer le service Annuaire :

1. Dans la console de gestion, cliquez sur *Outils* > *Configuration*.
2. Cliquez sur *Annuaires d'authentification*.
3. Cliquez sur *Nouveau* pour lancer l'assistant de nouvelle configuration du service Annuaire.



4. Cliquez sur *Suivant* pour afficher la page Configurer le serveur.

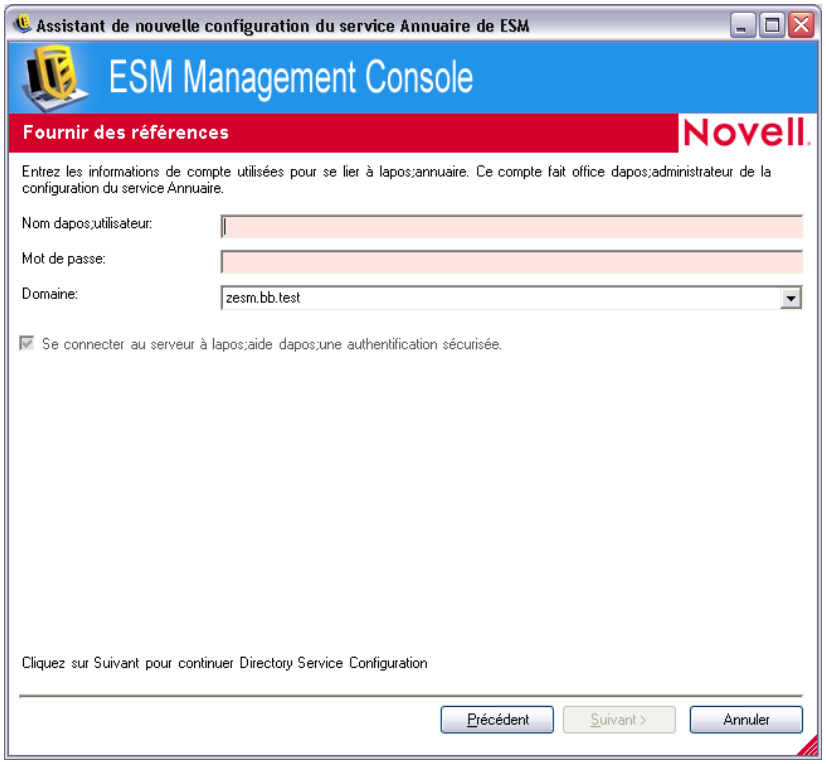


5 Renseignez les champs :

- **Type de service :** Sélectionnez un type de service dans la liste déroulante *Type de service* :
  - Microsoft Active Directory
  - Novell eDirectory
- **Nom :** Entrez un nom convivial pour décrire la configuration du service Annuaire.
- **Nom d'hôte :** Spécifiez ou recherchez le nom DNS ou l'adresse IP du serveur d'annuaire.
- **Port :** Spécifiez le port utilisé pour se connecter au serveur d'annuaire.

  Le port par défaut est le 389. Si vous utilisez un autre port pour vous connecter au serveur d'annuaire, vous pouvez le spécifier.

6 Cliquez sur *Suivant* pour afficher la page Fournir des références.



7 Renseignez les champs :

- **Nom d'utilisateur :** Spécifiez l'administrateur de comptes à lier à l'annuaire.

  Ce compte fait office d'administrateur de la configuration du service Annuaire. Le nom de login doit être un utilisateur qui a l'autorisation d'afficher toute l'arborescence Annuaire. Il est recommandé que cet utilisateur soit l'administrateur de domaine ou un administrateur OU. En cas de configuration pour eDirectory, utilisez un format LDAP, tel que : `cn=admin,o=acmeserver` dans lequel `cn` est l'utilisateur et `o` l'objet où est stocké le compte utilisateur..

- **Mot de passe :** Spécifiez le mot de passe de l'administrateur de comptes.

  Ce compte fait office d'administrateur de cette configuration du service Annuaire.

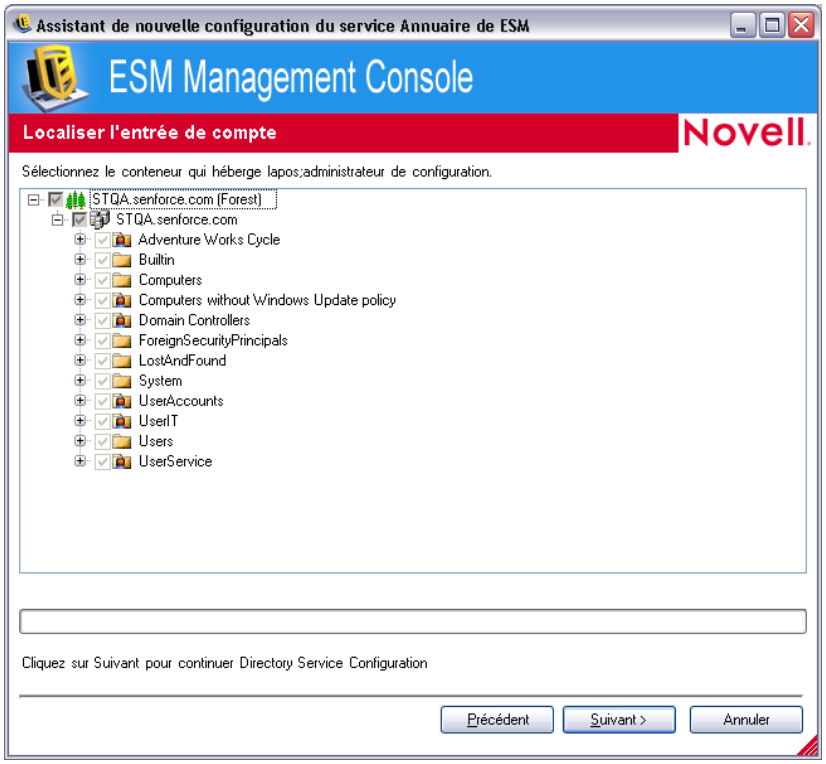
  Le mot de passe doit être configuré de sorte à ne jamais expirer, de même que ce compte ne devra jamais être désactivé.

- **Domaine :** Spécifiez le domaine auquel l'administrateur de comptes appartient.

- **Se connecter au serveur à l'aide d'une authentification sécurisée :** Désélectionnez cette option si vous ne souhaitez pas utiliser d'authentification sécurisée. Cette option est activée par défaut.

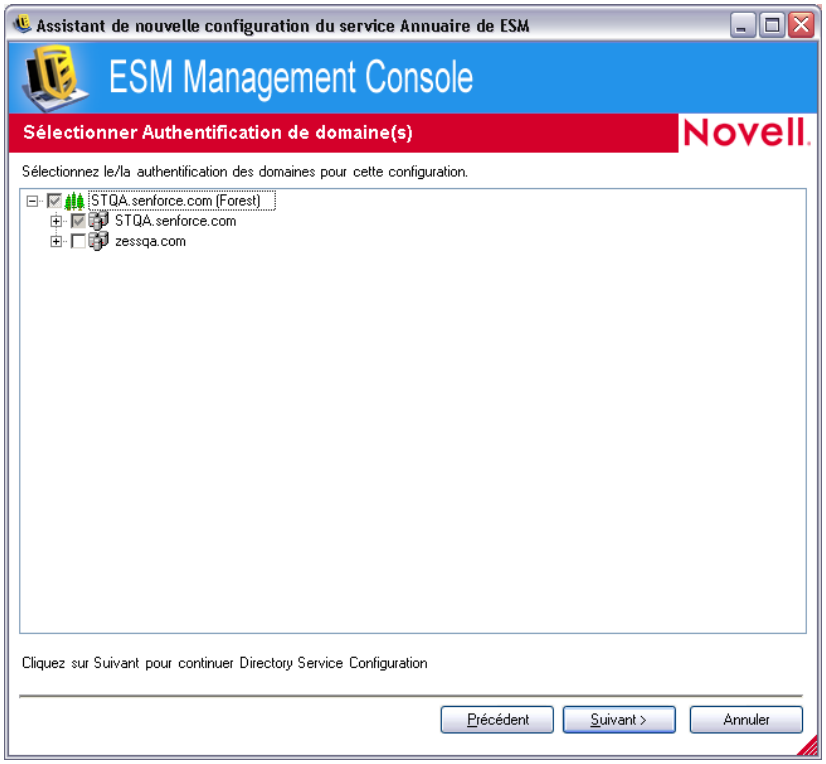
8 Cliquez sur *Suivant* pour continuer.

9 Si l'administrateur de configuration spécifié à l'Étape 7 n'a pas pu être trouvé dans le domaine, la page Localiser l'entrée de compte s'affiche.



Spécifiez dans quel conteneur se trouve l'administrateur, puis cliquez sur *Suivant*.

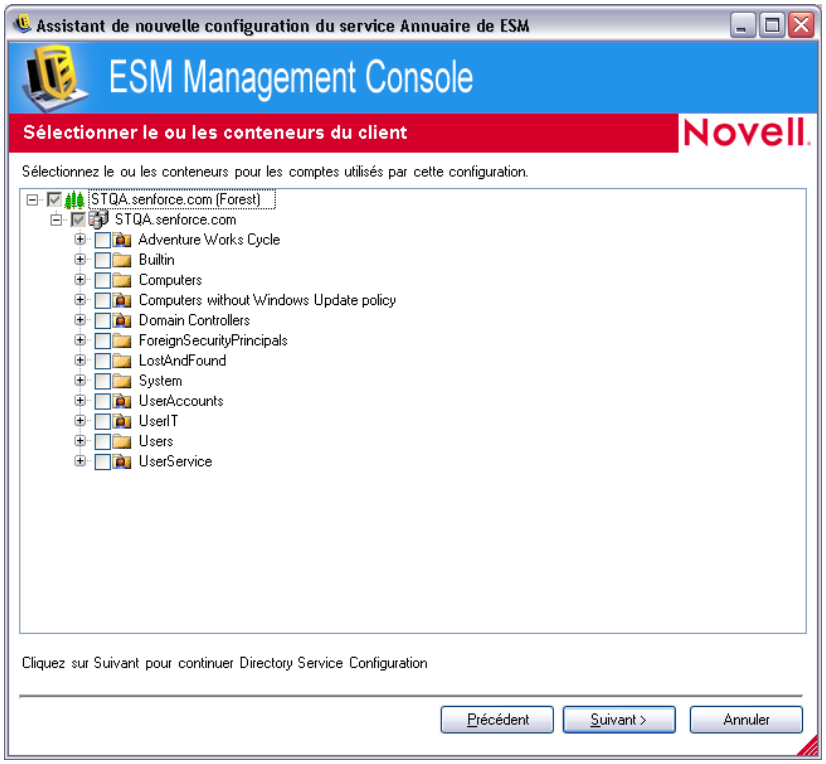
10 Sur la page Sélectionner un ou plusieurs domaines d'authentification, parcourez l'arborescence pour sélectionner les domaines à utiliser pour authentifier les utilisateurs et les ordinateurs de cette configuration.



Le domaine qui contient l'administrateur spécifié à l'Étape 7 est sélectionné et ne peut pas être désélectionné.

Toute tentative d'enregistrement de l'installation du client auprès du serveur de gestion échoue s'il n'appartient pas à l'un des domaines sélectionnés dans la configuration.

11 Cliquez sur *Suivant* pour afficher la page Sélectionner le ou les conteneurs du client, puis sélectionnez les conteneurs des comptes utilisés par cette configuration.

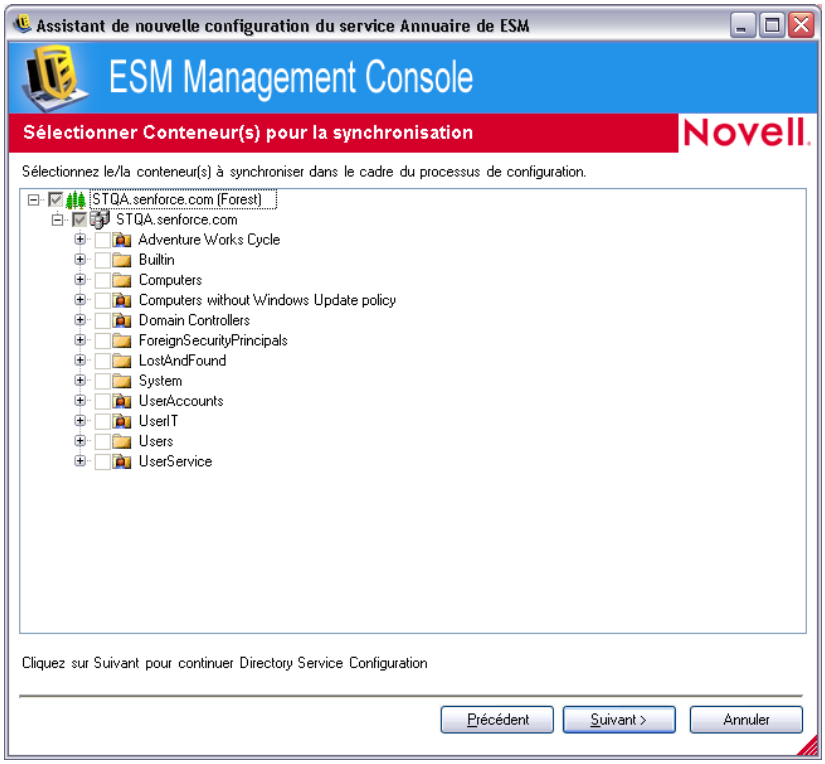


Le conteneur qui contient l'administrateur spécifié à l'Étape 7 est sélectionné et ne peut pas être désélectionné.

Afin d'optimiser les performances, la page Sélectionner le ou les conteneurs du client vous permet de ne faire porter la recherche que sur les conteneurs qui hébergent des utilisateurs et ordinateurs gérés.

Toute tentative d'enregistrement de l'installation du client auprès du serveur de gestion échoue si son compte ne réside pas dans l'un des conteneurs sélectionnés dans la configuration.

12 Cliquez sur *Suivant* pour afficher les conteneurs de la page de synchronisation.



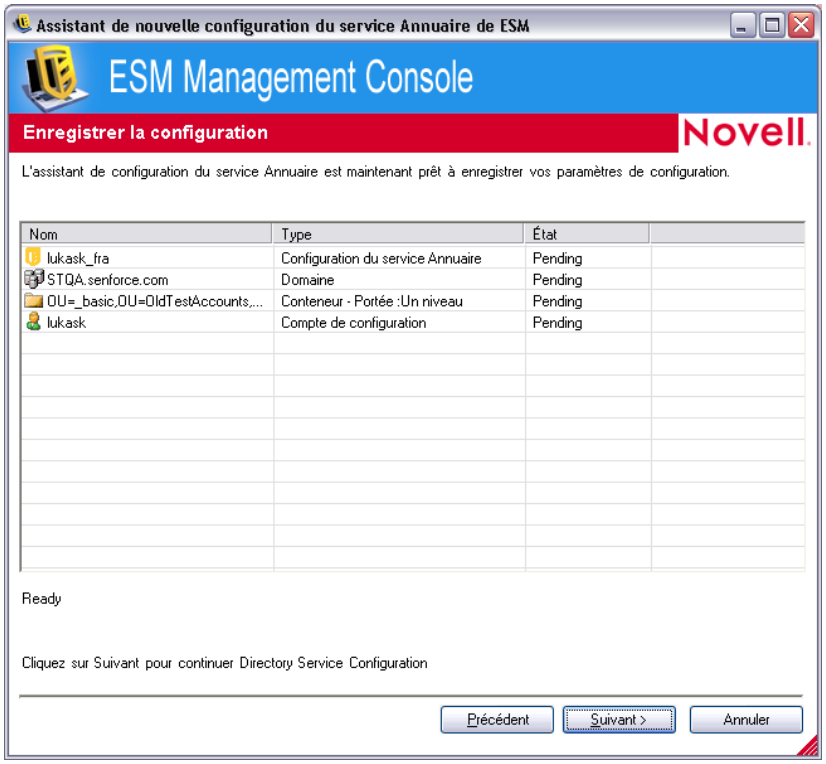
13 (Facultatif) Sélectionnez les conteneurs à synchroniser dans le cadre du processus de configuration.

La synchronisation s'effectue en arrière-plan, vous permettant ainsi de commencer à utiliser la nouvelle configuration sans plus tarder. Une opération de synchronisation d'un nombre important d'utilisateurs et d'ordinateurs peut prendre quelques heures.

Si vous ne spécifiez aucun conteneur à synchroniser, les données relatives à ces utilisateurs et ordinateurs sont renseignées dans la console de gestion lorsque ceux-ci s'enregistrent.

Une synchronisation des conteneurs renseigne au préalable les données relatives à ces utilisateurs et ordinateurs dans la console de gestion, vous permettant ainsi d'effectuer immédiatement des opérations telles que créer des stratégies de sécurité. Lorsque les utilisateurs ou ordinateurs s'enregistrent auprès du système, ces stratégies sont distribuées, puis appliquées. Si vous avez préalablement renseigné des données dans la console de gestion, vous pouvez créer immédiatement des stratégies spécifiques à des ordinateurs ou utilisateurs individuels, au lieu de créer une stratégie qui s'applique à tous les utilisateurs et ordinateurs du conteneur. Si vous n'avez pas synchronisé le conteneur, vous devez attendre que ces utilisateurs et ordinateurs s'enregistrent auprès du système avant de pouvoir créer des stratégies qui leur sont propres.

14 Cliquez sur *Suivant* pour afficher la page Enregistrer la configuration.

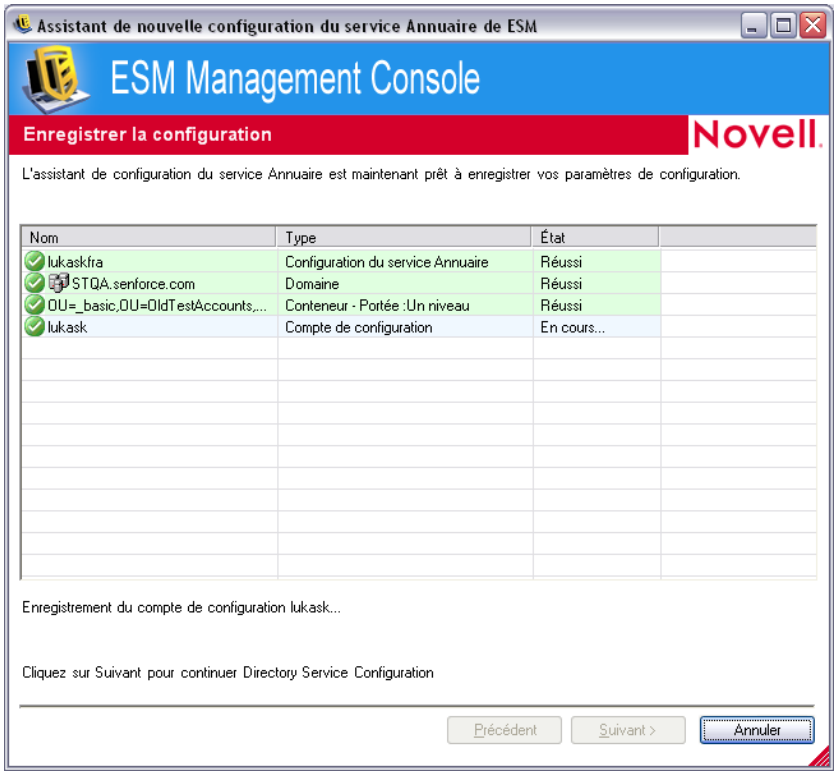


15 Passez en revue les informations, puis cliquez sur *Suivant* pour enregistrer la configuration.

Au besoin, vous pouvez cliquer sur *Précédent* pour modifier certains paramètres.

16 Cliquez sur *Terminer*.

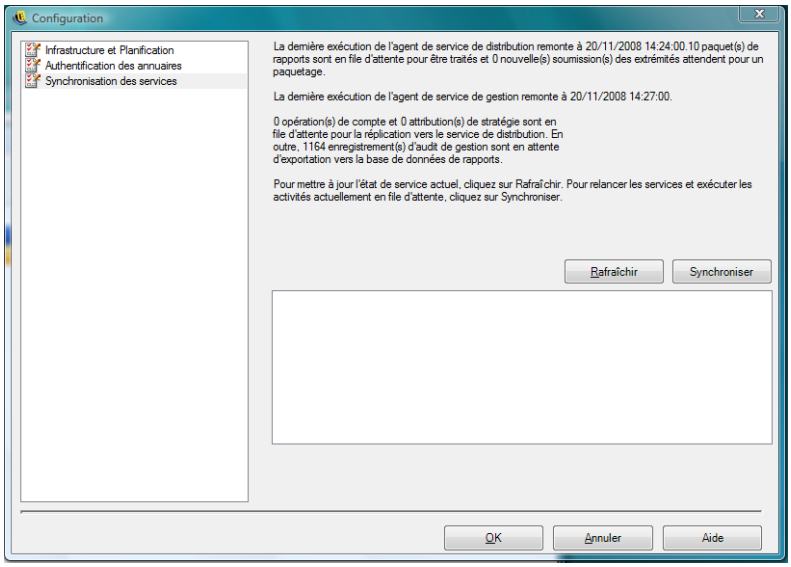
Lorsque vous cliquez sur *Terminer*, l'icône s'affiche dans votre zone de notification Windows et la synchronisation démarre. Vous pouvez double-cliquer sur l'icône pour afficher la boîte de dialogue Synchronisation des services Annuaire.



La synchronisation s'effectue en arrière-plan. Elle s'arrête si vous quittez la console de gestion. Lorsque vous rouvrez cette dernière, la synchronisation reprend là où elle s'était arrêtée.

1.4.3 Synchronisation des services

La commande Synchronisation des services permet de forcer une synchronisation du service de gestion et du service de distribution de stratégies. Les alertes, les rapports et la distribution des stratégies sont ainsi mis à jour.

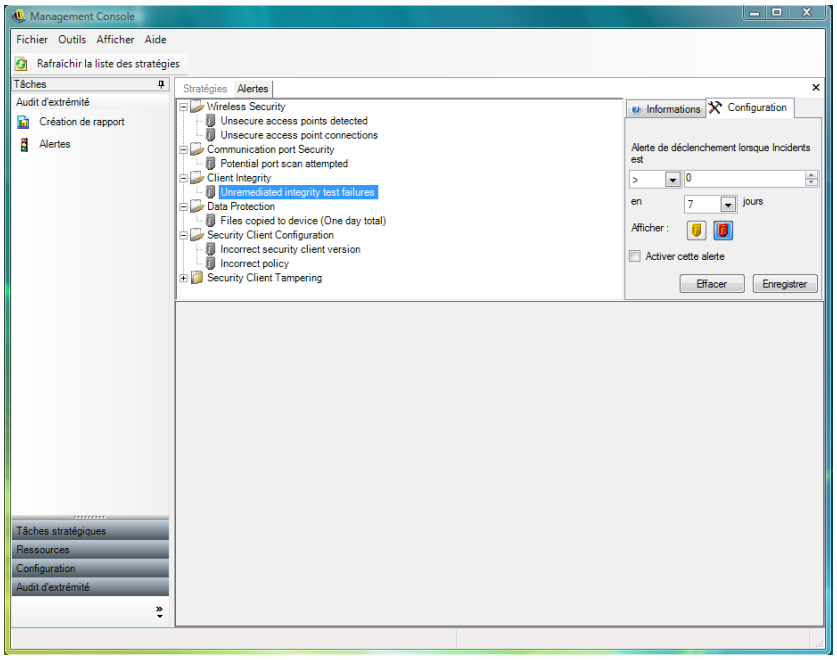


1. Pour mettre à jour l'état actuel du service, cliquez sur *Rafraîchir*.
2. Pour redémarrer les services et traiter les activités actuellement en attente, cliquez sur *Synchroniser*.

1.5 Utilisation de la surveillance des alertes

La surveillance des alertes permet à l'administrateur ZENworks® Endpoint Security Management d'évaluer le niveau de sécurité de tous les noeuds d'extrémité gérés via ZENworks Endpoint Security Management dans l'entreprise. Les alertes sont entièrement configurables et peuvent signaler un simple avertissement ou une urgence à part entière. Cet outil est accessible via *Audit du noeud d'extrémité*dans la barre des tâches ou via le menu *Afficher*.

1 Pour accéder aux alertes, cliquez sur l'icône des alertes (Alertes).



Une surveillance des alertes est disponible pour les domaines suivants :

- **Intégrité du client :** signale des résultats de test d'intégrité non résolus.
- **Sécurité du port de communication :** signale des tentatives potentielles d'analyse de port.
- **Protection des données :** signale des fichiers copiés sur des périphériques de stockage amovibles au cours d'une période d'une journée.
- **Configuration du client de sécurité :** signale des stratégies incorrectes et des versions incorrectes du client de sécurité.
- **Falsification du client de sécurité :** signale les tentatives de piratage, les tentatives de désinstallation et les utilisations du mot de passe prioritaire par utilisateur.
- **Sécurité sans fil :** signale les points d'accès non sécurisés, à la fois détectés et connectés par l'utilisateur final.

1.5.1 Configuration de ZENworks Endpoint Security Management pour les alertes

La surveillance des alertes nécessite la collecte et le téléchargement des données de rapport à intervalle régulier afin de refléter au mieux l'état actuel de l'environnement de sécurité du noeud d'extrémité. Les clients ZENworks® Security Client non gérés ne fournissent pas de données de rapport, et, par conséquent, ne sont pas inclus dans la surveillance des alertes.

Les sections suivantes contiennent davantage d'informations :

- « Activation de la création de rapport » page 27
- « Optimisation de la synchronisation » page 27

Activation de la création de rapport

La création de rapport doit être activée dans chaque stratégie de sécurité. Reportez-vous à la section Section 2.2.4, « Rapport de conformité », page 106 pour plus de détails sur la configuration de la création de rapport pour une stratégie de sécurité. Ajustez les intervalles d'envoi de rapport de manière à obtenir des mises à jour de l'état du noeud d'extrémité en temps opportun. En outre, une alerte ne s'active pas sans rapport. Toute activité pour laquelle vous souhaitez recevoir une alerte doit être associée à un rapport approprié dans la stratégie de sécurité.

Optimisation de la synchronisation

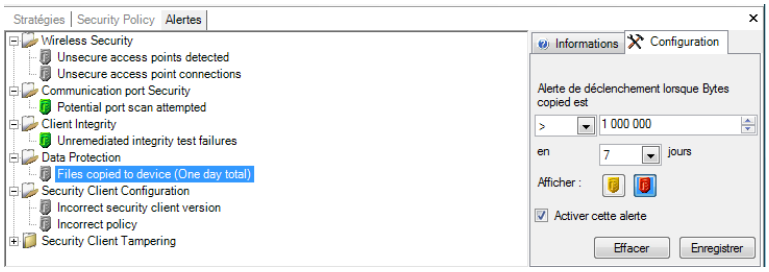
Par défaut, la synchronisation du service de rapport de ZENworks Endpoint Security Management est effectuée toutes les 12 heures. Cela signifie que les données de rapport et d'alerte initiales ne sont disponibles que 12 heures après l'installation de ZENworks Endpoint Security Management. Pour régler cet intervalle, ouvrez l'outil de configuration (voir « Planification » page 15) et réglez l'heure de *création de rapport du client* sur le nombre de minutes appropriées en fonction de vos besoins et de votre environnement.

Si vous avez besoin des données immédiatement, l'option *Synchronisation des services* dans l'outil de configuration peut lancer instantanément le service de distribution de stratégies (qui collecte les données de rapport à partir des noeuds d'extrémité) et le service de rapport (permettant ainsi de mettre à jour toutes les alertes sur la base des données récemment collectées). Reportez-vous à la rubrique Section 1.4.3, « Synchronisation des services », page 24 pour plus d'informations.

1.5.2 Configuration des déclencheurs d'alerte

Les déclencheurs d'alerte peuvent être réglés sur des seuils qui correspondent aux besoins de sécurité de votre entreprise.

1. Sélectionnez une alerte dans la liste et cliquez sur l'onglet *Configuration* à droite dans la console de gestion.



2. Réglez d'abord le seuil de déclenchement en sélectionnant, dans la liste déroulante, la condition qui indique si la valeur de déclenchement est :
   - = (égal à)
   - < (supérieur à)
   - <= (supérieur ou égal à)
   - > (inférieur à)
   - >= (inférieur ou égal à)
3. Réglez la valeur de déclenchement. Elle varie en fonction du type d'alerte.
4. Sélectionnez l'intervalle au cours duquel cette valeur doit être atteinte.

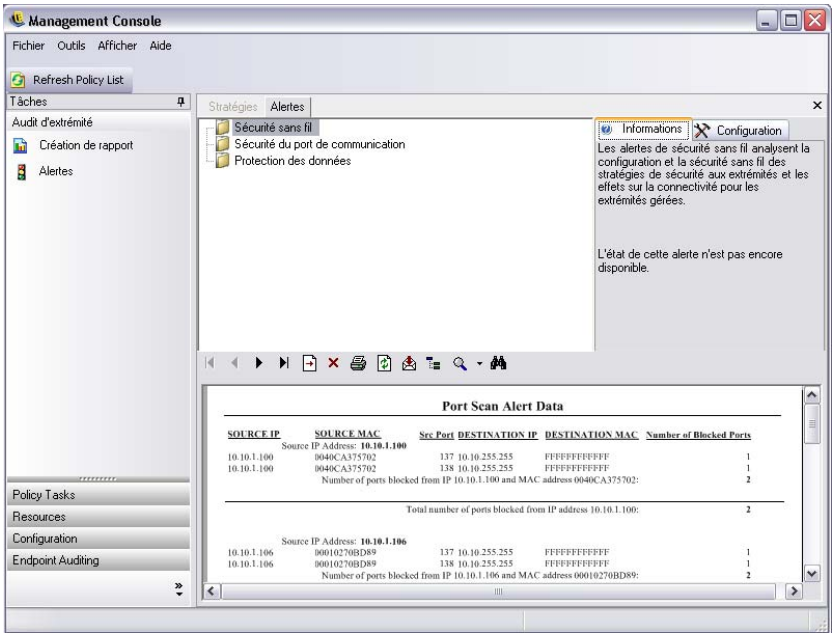
5 Sélectionnez le type de déclenchement. Il peut s'agir d'une icône d'avertissement ( ) ou d'une icône d'urgence ( ).

6 Vérifiez que la case *Activer cette alerte*est cochée.

7 Cliquez sur *Enregistrer* pour enregistrer l'alerte.

1.5.3 Gestion des alertes

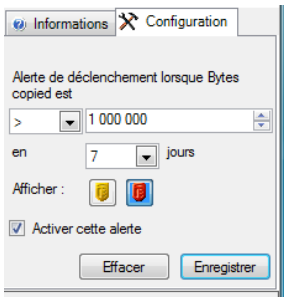
Les alertes vous avertissent des problèmes qui doivent être résolus dans l'environnement de sécurité du noeud d'extrémité. La remédiation est normalement assurée pour un groupe ou pour un utilisateur. Pour aider à identifier le problème, des rapports d'alerte s'affichent lorsque l'alerte est sélectionnée.



Ce rapport affiche les résultats du déclencheur actuel et présente les informations pour le périphérique ou l'utilisateur concerné. Les données de ce rapport fournissent les informations nécessaires pour prendre les mesures correctives permettant de résoudre les éventuels problèmes de sécurité d'entreprise. D'autres informations sont également disponibles en ouvrant Rapport.

Une fois les mesures correctives prises, l'alerte reste active jusqu'à la prochaine mise à jour du rapport. Pour effacer une alerte avant une mise à jour planifiée :

1 Sélectionnez une alerte dans la liste et cliquez sur l'onglet *Configuration* à droite dans la console de gestion.



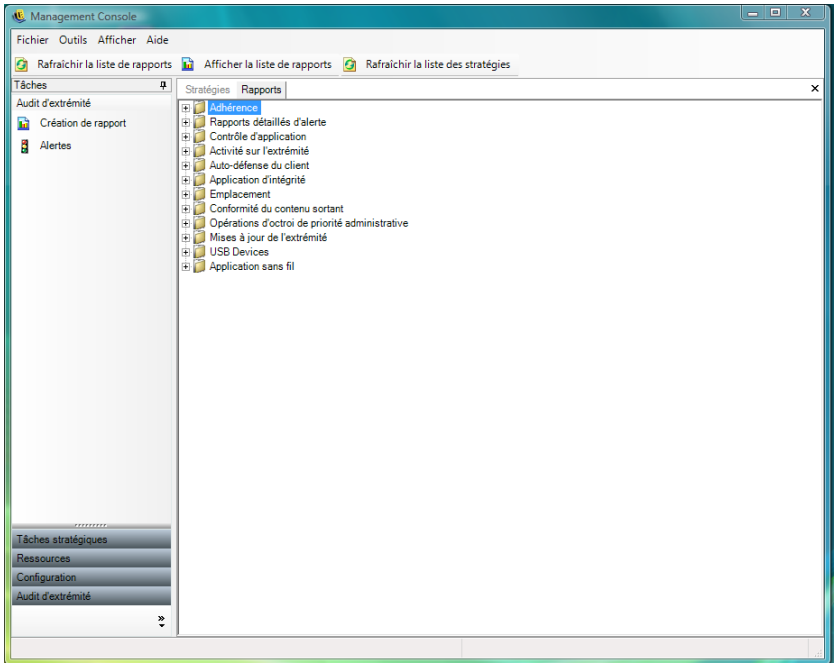
2 Cliquez sur *Effacer*.

Les données de rapport sont alors effacées des alertes (mais restent disponibles dans la base de données des rapports). Aucune réactivation n'a lieu avant la réception de nouvelles données.

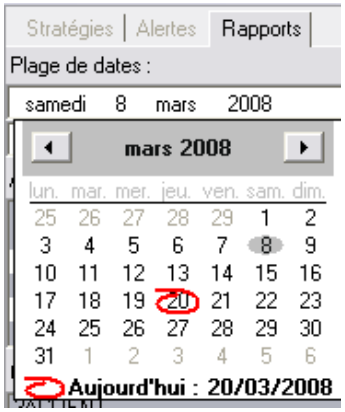
1.6 Utilisation du service de création de rapport

Le service de rapport fournit des rapports d'adhésion et d'état pour l'entreprise. Les données disponibles sont fournies pour les annuaires et les groupes d'utilisateurs au sein d'un même annuaire. Les rapports de Novell® fournissent des informations sur les effets qu'ont les composants de stratégie individuels sur les noeuds d'extrémité de l'entreprise. Les requêtes pour ces rapports sont définies dans la stratégie de sécurité (voir Section 2.2.4, « Rapport de conformité », page 106) et peuvent fournir des données utiles pour la décision de mise à jour des stratégies.

Sélectionnez *Rapports* à partir de la barre des tâches *Audit du noeud d'extrémité* ou du menu *Afficher*. La liste des rapports disponibles s'affiche (cliquez sur le signe plus en regard de chaque type de rapport pour en visualiser la liste complète).



Vous pouvez configurer les rapports en identifiant une plage de dates et d'autres paramètres, par exemple, l'utilisateur ou l'emplacement. Pour définir les dates, cliquez sur la vue du calendrier pour l'agrandir, puis sélectionnez le mois et le jour. Veillez à cliquer sur le jour pour modifier le paramètre de date.



Cliquez sur *Afficher* pour générer le rapport.

Dès que le rapport est généré, la barre d'outils des rapports permet de l'afficher, de l'imprimer, de l'envoyer par messagerie électronique ou de l'exporter au format `PDF`.

Lorsque vous consultez les rapports, les boutons fléchés vous permettent d'en parcourir les pages. En général, la première page des rapports comporte des tableaux et des graphiques, viennent ensuite les données collectées sur les autres pages, classées par date et type.

L'icône *Imprimante* permet d'imprimer la totalité du rapport à l'aide de l'imprimante par défaut de cet ordinateur.

L'icône *Exportation* permet d'enregistrer le rapport sous différents formats : PDF, feuille de calcul Excel*, document Word ou fichier RTF.

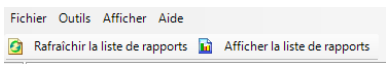
L'icône *Arborescence de groupe* permet d'afficher une liste de paramètres en regard du rapport. Sélectionnez l'un de ces paramètres pour augmenter le niveau de détail du rapport. Cliquez sur l'icône *Arborescence de groupe* pour fermer la barre latérale.

L'icône *Loupe* propose un menu déroulant pour régler la taille de la vue actuelle.

L'icône *Jumelles* permet d'ouvrir une fenêtre de recherche.

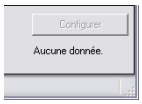
Si vous placez le pointeur de la souris sur un paramètre particulier, comme un nom d'utilisateur ou un nom de périphérique par exemple, il se transforme en loupe. Vous pouvez double-cliquer sur cet élément spécifique et afficher un nouveau rapport pour cet objet uniquement. Cliquez sur le bouton *Fermer* pour fermer l'affichage actuel et revenir au rapport initial.

Pour revenir à la liste des rapports, cliquez sur l'icône *Liste de rapports* située au-dessus de la fenêtre des rapports.



Les rapports ne sont pas disponibles tant que les données n'ont pas été téléchargées à partir des clients ZENworks® Security Client. Par défaut, la synchronisation du service de rapport de ZENworks Endpoint Security Management est effectuée toutes les 12 heures. Cela signifie que les données de rapport et d'alerte initiales ne sont disponibles que 12 heures après l'installation de ZENworks Endpoint Security Management. Pour régler cet intervalle, ouvrez l'outil de configuration (voir « Planification » page 15) et réglez l'heure de *création de rapport du client* sur le nombre de minutes appropriées en fonction de vos besoins et de votre environnement.

Les boutons *Configurer* ou *Aperçu* des rapports pour lesquels aucune donnée n'est disponible sont affichés en grisé avec l'indication « Aucune donnée » en dessous.



Les rapports suivants sont disponibles :

- Section 1.6.1, « Rapports d'adhésion », page 31
- Section 1.6.2, « Rapports détaillés d'alerte », page 32
- Section 1.6.3, « Rapports de contrôle d'application », page 33
- Section 1.6.4, « Rapports de solution de codage », page 34
- Section 1.6.5, « Rapports d'activité du noeud d'extrémité », page 34
- Section 1.6.6, « Rapports des mises à jour du noeud d'extrémité », page 35
- Section 1.6.7, « Rapports d'auto-défense du client », page 35
- Section 1.6.8, « Rapports d'application d'intégrité », page 35
- Section 1.6.9, « Rapports d'emplacement », page 36
- Section 1.6.10, « Rapports de conformité du contenu sortant », page 36
- Section 1.6.11, « Rapport des opérations d'octroi de priorité administrative », page 37
- Section 1.6.12, « Rapports des mises à jour du noeud d'extrémité », page 38
- Section 1.6.13, « Rapports d'application de l'environnement sans fil », page 38

1.6.1 Rapports d'adhésion

Les rapports d'adhésion fournissent des informations de conformité relatives à la distribution des stratégies de sécurité à des utilisateurs gérés. Un résultat d'adhésion de 100 % indique que tous les utilisateurs gérés se sont enregistrés et ont reçu la stratégie actuelle.

Les rapports suivants sont disponibles :

- **Adhérence d'enregistrement des noeuds d'extrémité :** présente un récapitulatif des jours écoulés depuis l'enregistrement par les noeuds d'extrémité de l'entreprise, ainsi que l'âge de leur stratégie actuelle. La moyenne de ces valeurs est calculée pour résumer le rapport. Ce rapport ne nécessite pas la saisie de variables. Il affiche les utilisateurs par nom, les stratégies qui leur ont été assignées, les jours depuis leur dernier enregistrement et l'âge de leur stratégie.
- **Versions du client aux noeuds d'extrémité :** affiche la dernière version signalée du client sur chaque noeud d'extrémité. Définissez les paramètres de date pour générer ce rapport.
- **Noeuds d'extrémité jamais enregistrés:** Liste les comptes utilisateur enregistrés auprès du service de gestion mais qui n'ont jamais recherché une mise à jour des stratégies via le service de distribution. Sélectionnez un ou plusieurs groupes pour générer le rapport.

  Il peut s'agir d'utilisateurs de la console de gestion qui ne disposent d'aucun client de sécurité à leur nom.
- **Non-conformité de la stratégie de groupe :** affiche les groupes dans lesquels certains utilisateurs ne disposent pas de la stratégie appropriée. Vous pouvez sélectionner un ou plusieurs groupes pour générer le rapport.
- **Historique d'état des noeuds d'extrémité par machine:** indique le dernier état (dans une plage de dates donnée) des noeuds d'extrémité protégés par ZENworks Endpoint Security Management, regroupés par nom de machine. Il affiche le nom de l'utilisateur logué, la stratégie actuelle, la version du client ZENworks Endpoint Security Management et l'emplacement réseau. Ce rapport nécessite la saisie d'une plage de dates. L'administrateur peut augmenter le niveau de détail en double-cliquant sur n'importe quelle entrée pour afficher la liste complète des rapports d'état pour une machine en particulier.
- **Assignation de stratégie :** affiche les utilisateurs/groupes (comptes) qui ont reçu la stratégie spécifiée. Sélectionnez la stratégie souhaitée dans la liste, puis cliquez sur *Afficher* pour exécuter le rapport.
- **Historique d'état des noeuds d'extrémité par utilisateur :** indique le dernier état (dans une plage de dates donnée) des noeuds d'extrémité protégés par ZENworks Endpoint Security Management, regroupés par nom d'utilisateur. Il affiche le nom de la machine, la stratégie actuelle, la version du client ZENworks Endpoint Security Management et l'emplacement réseau. Ce rapport nécessite la saisie d'une plage de dates. L'administrateur peut augmenter le niveau de détail en double-cliquant sur n'importe quelle entrée pour afficher la liste complète des rapports d'état pour un utilisateur en particulier.

1.6.2 Rapports détaillés d'alerte

Les rapports détaillés d'alerte contiennent d'autres informations relatives aux alertes. Ces rapports n'affichent des données que si une alerte a été déclenchée. La suppression d'une alerte efface également son rapport ; ses données restent toutefois toujours disponibles dans un rapport standard.

Les rapports suivants sont disponibles :

- **Données d'alerte de falsification du client :** affiche les instances dans lesquelles un utilisateur a effectué une tentative non autorisée de modification ou de désactivation de ZENworks Security Client.

- **Données d'alerte de copie de fichiers :** affiche les comptes qui ont copié des données sur des périphériques de stockage amovibles.
- **Données d'alerte de version incorrecte du client :** affiche l'historique de l'état du processus de mise à jour de ZENworks Security Client.
- **Données d'alerte de stratégie incorrecte du client :** affiche les utilisateurs qui ne disposent pas de la stratégie appropriée.
- **Données d'alerte des échecs d'intégrité :** indique l'historique des échecs et des réussites des vérifications d'intégrité du client.
- **Données d'alerte des opérations d'octroi de priorité :** affiche les instances dans lesquelles la priorité administrative est accordée aux mécanismes d'auto-défense du client, afin d'octroyer un contrôle privilégié sur ZENworks Security Client.
- **Données d'alerte d'analyse de port :** affiche le nombre de paquets bloqués sur un certain nombre de ports différents (un grand nombre de ports pouvant indiquer l'exécution d'une analyse de port).
- **Données d'alerte de tentative de désinstallation :** liste les utilisateurs qui ont tenté de désinstaller ZENworks Security Client.
- **Données d'alerte de points d'accès non sécurisés :** liste les points d'accès non sécurisés détectés par ZENworks Security Client.
- **Données d'alerte de connexion à des points d'accès non sécurisés :** liste les points d'accès non sécurisés connectés par ZENworks Security Client.

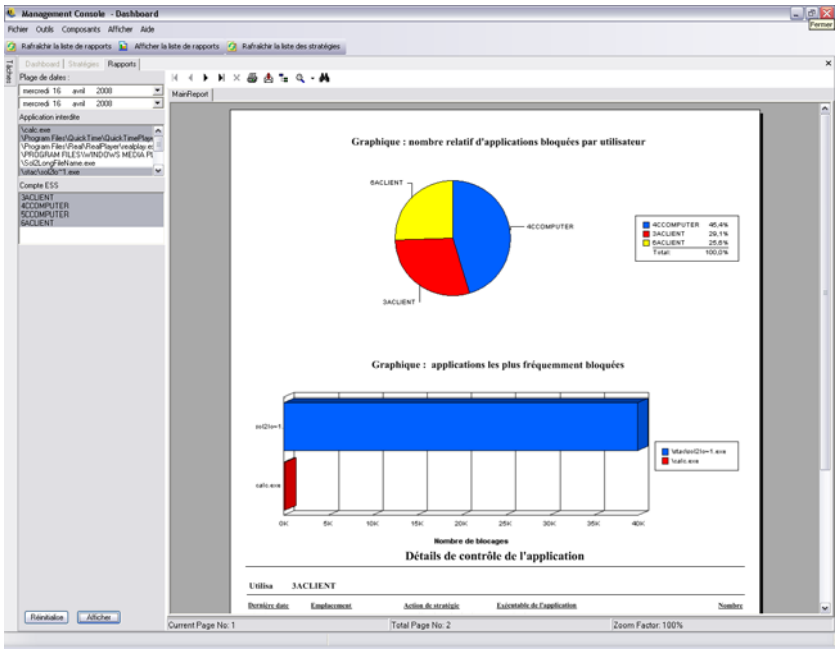
1.6.3 Rapports de contrôle d'application

les rapports de contrôle d'application indiquent toutes les tentatives non autorisées par des applications bloquées pour accéder au réseau ou s'exécuter lorsque la stratégie ne le permet pas.

Le rapport suivant est disponible :

- **Détails du contrôle d'application :** affiche la date, l'emplacement, la mesure prise par ZENworks® Security Client, l'application qui a tenté de s'exécuter et le nombre de démarrages de l'application. Les dates sont affichées au format UTC.

Spécifiez les paramètres de date, sélectionnez le nom des applications dans la liste, sélectionnez les comptes utilisateur et cliquez sur *Afficher* pour exécuter le rapport.



1.6.4 Rapports de solution de codage

Si le codage du noeud d'extrémité est activé, les rapports de solutions de codage affichent le transfert de fichiers vers et à partir des dossiers codés.

Les rapports suivants sont disponibles :

- **Activité de codage de fichier :** affiche les fichiers pour lesquels le codage a été appliqué.
- **Exceptions de codage :** affiche les erreurs du sous-système de codage (par exemple, un fichier protégé qui n'a pas pu être décodé car l'utilisateur ne disposait pas des clés adéquates).
- **Volumes de codage de fichier :** affiche les volumes (par exemple, unités amovibles ou partitions de disque dur) gérés par la solution de codage de Novell.

1.6.5 Rapports d'activité du noeud d'extrémité

Les rapports d'activité du noeud d'extrémité fournissent un feed-back pour les différents composants de stratégie et leur effet sur le fonctionnement du noeud d'extrémité.

Les rapports suivants sont disponibles :

- **Paquets bloqués par adresse IP :** affiche les paquets bloqués filtrés par adresse IP cible. Les dates sont affichées au format UTC.

  Sélectionnez dans la liste l'adresse IP cible et définissez les paramètres de date. Le rapport affiche les dates, les emplacements, les ports affectés et le nom des paquets bloqués.
- **Paquets bloqués par utilisateur:** affiche les paquets bloqués filtrés par utilisateur. Les dates sont affichées au format UTC. Les données sont dans l'ensemble identiques à celles des paquets bloqués par adresse IP cible, si ce n'est qu'elles sont réparties par utilisateur.

- **Statistiques de l'utilisation réseau par utilisateur :** liste les paquets envoyés, reçus ou bloqués et des erreurs réseau, filtrés par utilisateur. Ce rapport nécessite une plage de dates. Les dates sont affichées au format UTC.
- **Statistiques de l'utilisation réseau par type d'adaptateur :** liste les paquets envoyés, reçus ou bloqués et des erreurs réseau, filtrés par type d'adaptateur. Ce rapport nécessite une plage de dates et un emplacement. Les dates sont affichées au format UTC.

1.6.6 Rapports des mises à jour du noeud d'extrémité

Le rapport des mise à jour du noeud d'extrémité affiche l'état du processus de mise à jour de ZENworks Security Client (reportez-vous à la rubrique « Mise à jour de ZSC » page 66). Les dates sont affichées au format UTC.

Les rapports suivants sont disponibles :

- **Graphique de pourcentage des échecs de mise à jour du client de sécurité :** affiche, sous forme de graphique, le pourcentage d'échecs de mises à jour de ZENworks Security Client (qui n'ont pas été résolues) Aucun paramètre n'est requis pour générer ce rapport.
- **Historique de l'état de mise à jour du client de sécurité :** affiche l'historique de l'état du processus de mise à jour de ZENworks Security Client. Sélectionnez la plage de dates et cliquez sur *Afficher* pour exécuter le rapport. Le rapport indique les utilisateurs qui se sont enregistrés et qui ont reçu la mise à jour.
- **Graphique des types d'échec de mise à jour du client de sécurité :** affiche, sous forme de graphique, les échecs de mise à jour de ZENworks Security Client (qui n'ont pas été résolues) Sélectionnez la plage de dates et cliquez sur Afficher pour exécuter le rapport. Le rapport indique les utilisateurs qui se sont enregistrés mais qui ne sont pas parvenus à installer les mises à jour.

1.6.7 Rapports d'auto-défense du client

Les rapports d'auto-défense du client signalent lorsque les utilisateurs tentent de modifier ou de désactiver ZENworks® Security Client.

Le rapport suivant est disponible :

- **Tentatives de piratage de ZENworks Security Client :** Signale les tentatives non autorisées de modification ou de désactivation de ZENworks Security Client. Les dates sont affichées au format UTC.

  Entrez les paramètres de date et cliquez sur *Afficher* pour exécuter le rapport.

1.6.8 Rapports d'application d'intégrité

Les rapports d'application d'intégrité fournissent des rapports concernant les résultats d'intégrité du logiciel antivirus/anti-espion.

Les rapports suivants sont disponibles :

- **Historique d'intégrité client :** signale la réussite ou l'échec des contrôles d'intégrité client. Les dates sont affichées au format UTC.

  Sélectionnez la plage de dates pour le rapport, les règles d'intégrité et les noms d'utilisateur.

- **Échecs d'intégrité non résolus par règle :** signale les tests et règles d'intégrité qui ont échoué et n'ont pas encore été résolus.

  Sélectionnez les règles d'intégrité, puis cliquez sur *Afficher* pour exécuter le rapport.
- **Échecs d'intégrité non résolus par utilisateur :** signale les utilisateurs pour lesquels les tests d'intégrité ont échoué et n'ont pas encore été résolus.

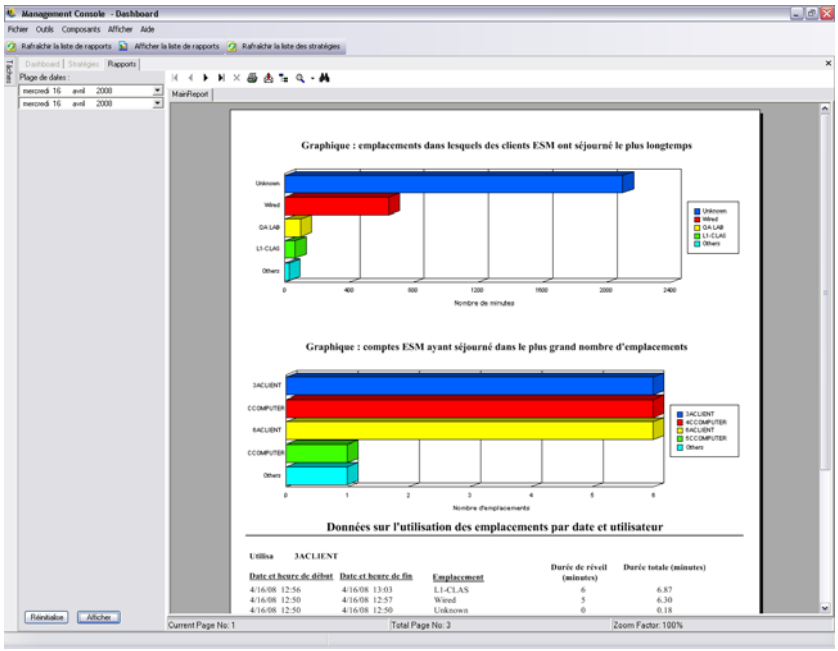
  Sélectionnez les noms d'utilisateur, puis cliquez sur *Afficher* pour exécuter le rapport.

1.6.9 Rapports d'emplacement

Le rapport d'emplacement fournit des données concernant les emplacements les plus couramment utilisés par les utilisateurs finaux.

Le rapport suivant est disponible :

Données sur l'utilisation des emplacements par date et utilisateur : fournit des informations collectées à partir des différents clients concernant le nom des emplacements utilisés et la date/heure de leur utilisation. Les dates sont affichées au format UTC. Les emplacements affichés sont ceux employés par l'utilisateur ; les emplacements inutilisés ne sont pas affichés. Sélectionnez une plage de dates pour générer le rapport.



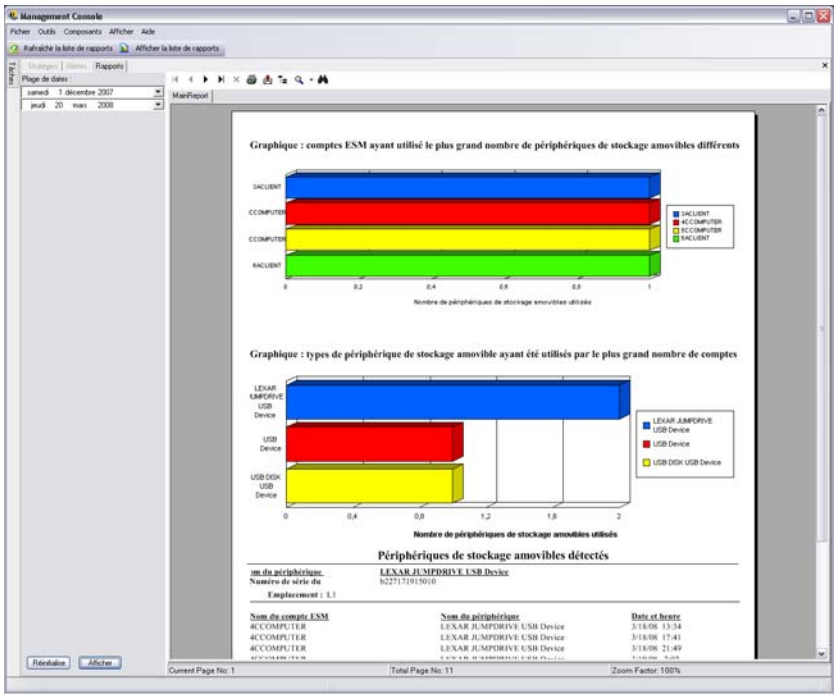
1.6.10 Rapports de conformité du contenu sortant

Les rapports de conformité du contenu sortant fournissent des informations concernant l'utilisation des unités amovibles et identifient quels fichiers ont été téléchargés sur ces unités.

Les rapports suivants sont disponibles :

- **Activité de stockage amovible par compte :** affiche les comptes qui ont copié des données sur un support de stockage amovible. Aucun paramètre n'est requis pour générer ce rapport.

- **Activité de stockage amovible par périphérique:** affiche les périphériques de stockage amovibles sur lesquels des fichiers ont été copiés. Sélectionnez la plage de dates, les noms d'utilisateur et les emplacements pour générer ce rapport.
- **Copies à partir de supports de stockage amovibles par compte :** affiche les périphériques de stockage amovibles dans lesquels des fichiers ont été copiés.
- **Périphériques de stockage amovibles détectés :** affiche les périphériques de stockage amovibles qui ont été détectés sur le noeud d'extrémité. Sélectionnez la plage de dates, les noms d'utilisateur et les emplacements pour générer ce rapport.



- **Graphique hebdomadaire de l'activité de stockage amovible par compte :** affiche un graphique des comptes ayant récemment copié des données sur un support de stockage amovible. Entrez la plage de dates pour générer ce rapport.

1.6.11 Rapport des opérations d'octroi de priorité administrative

Le rapport des opérations d'octroi de priorité administrative signale les instances dans lesquelles la priorité administrative est accordée aux mécanismes d'auto-défense du client, afin d'octroyer un contrôle privilégié sur le client ZENworks® Security Client.

Le rapport suivant est disponible :

- **Opérations d'octroi de priorité dans ZENworks Security Client :** affiche les tentatives réussies d'octroi de priorité par utilisateur et par date. Les dates sont affichées au format UTC.

  Sélectionnez l'utilisateur et la plage de dates, puis cliquez sur *Afficher* pour exécuter le rapport.

1.6.12 Rapports des mises à jour du noeud d'extrémité

Les rapports de mise à jour des noeuds d'extrémité affichent l'état du processus de mise à jour de ZENworks® Security Client (reportez-vous à la rubrique « Mise à jour de ZSC » page 66). Les dates sont affichées au format UTC.

Les rapports suivants sont disponibles :

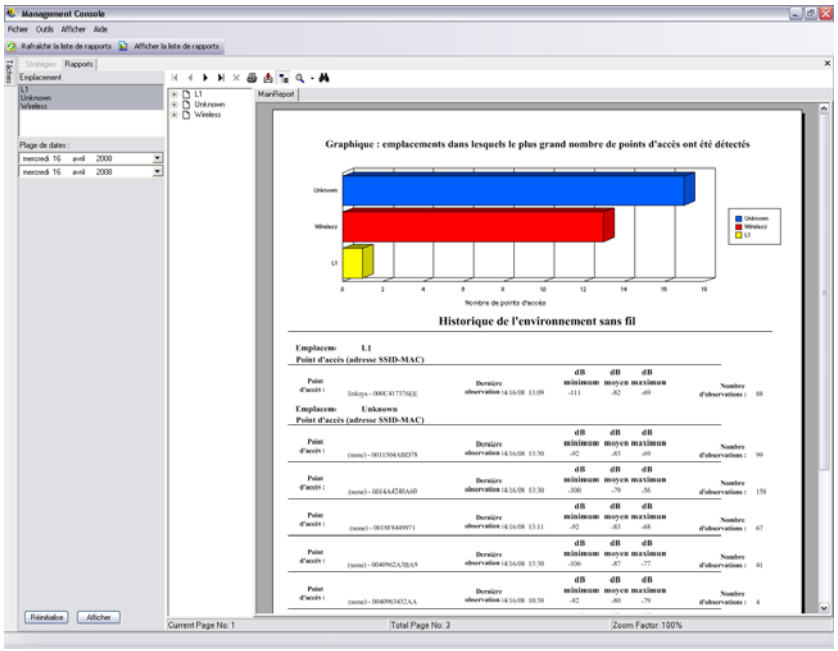
- **Graphique de pourcentage des échecs de mise à jour de sécurité :** affiche, sous forme de graphique, le pourcentage d'échecs de mises à jour de ZENworks Security Client qui n'ont pas été résolues. Aucun paramètre n'est requis pour générer ce rapport.
- **Historique de l'état de mise à jour du client de sécurité :** affiche l'historique de l'état du processus de mise à jour de ZENworks Security Client. Sélectionnez la plage de dates, puis cliquez sur *Afficher* pour exécuter le rapport. Le rapport indique les utilisateurs qui se sont enregistrés et qui ont reçu la mise à jour.
- **Graphique des types d'échec de mise à jour du client de sécurité :** affiche, sous forme de graphique, les échecs de mise à jour de ZENworks Security Client qui n'ont pas été résolues. Sélectionnez la plage de dates, puis cliquez sur *Afficher* pour exécuter le rapport. Le rapport indique les utilisateurs qui se sont enregistrés mais qui ne sont pas parvenus à installer les mises à jour.

1.6.13 Rapports d'application de l'environnement sans fil

Les rapports d'application de l'environnement sans fil fournissent des rapports concernant les environnements Wi-Fi auxquels est exposée le noeud d'extrémité.

Les rapports suivants sont disponibles :

- **Disponibilité de la connexion sans fil :** affiche les points d'accès disponibles pour la connexion par stratégie et emplacement. Indique le canal, l'identificateur SSID, l'adresse MAC et l'éventuel codage du point d'accès.
- **Tentatives de connexion sans fil :** fournit une liste de points d'accès auxquels les périphériques tentent de se connecter, par emplacement et par compte.
- **Historique de l'environnement sans fil :** fournit un historique de tous les points d'accès détectés, quel qu'en soit le propriétaire. Indique la fréquence, l'intensité du signal et l'éventuel codage du point d'accès. Les dates sont affichées au format UTC. Sélectionnez les emplacements souhaités et la plage de dates pour générer ce rapport.



1.7 Utilisation de ZENworks Storage Encryption Solution

ZENworks® Storage Encryption Solution (SES) garantit une gestion de sécurité complète et centralisée de toutes les données mobiles via l'application active d'une stratégie de codage d'entreprise sur le noeud d'extrémité proprement dit.

ZENworks Storage Encryption Solution permet d'effectuer les opérations suivantes :

- Création, distribution, application et audit centralisés des stratégies de codage sur l'ensemble des noeuds d'extrémité et des périphériques de stockage amovibles.
- Codage de tous les fichiers enregistrés ou copiés dans un répertoire spécifique sur toutes les partitions de disque fixes sur le disque dur.
- Codage de tous les fichiers copiés sur des périphériques de stockage amovibles.
- Partage libre des fichiers autorisés au sein d'une organisation et blocage de l'accès aux fichiers non autorisés.
- Partage des fichiers codés protégés par mot de passe avec des personnes externes à l'organisation par le biais d'un utilitaire de décodage disponible.
- Mise à jour, sauvegarde et récupération aisées des clés à l'aide de la stratégie sans perte de données.

1.7.1 Présentation de ZENworks Storage Encryption Solution

Le codage des données est assuré par la création et la distribution de stratégies de sécurité de codage de données. Les données sensibles du noeud d'extrémité sont stockées dans un dossier codé. L'utilisateur peut copier et accéder à ces données en dehors du dossier codé et partager les fichiers. Toutefois, tant qu'elles resteront dans ce dossier, les données restent codées. Les tentatives de lecture

des données par tout utilisateur non autorisé sur cette machine échoueront. Lorsque la stratégie est activée, un dossier avec codage `Safe Harbor` est ajouté au répertoire racine des volumes autres que système sur le noeud d'extrémité.

Les données sensibles placées sur une clé USB ou tout autre périphérique de stockage amovible sont immédiatement codées et ne peuvent être lues que sur les machines du même groupe de stratégie. Un dossier de partage peut éventuellement être activé, ce qui permet aux utilisateurs de partager les fichiers, à l'aide d'un mot de passe, avec des personnes n'appartenant pas au même groupe de stratégie (reportez-vous à la rubrique « Codage de données » page 64).

1.7.2 Partage de fichiers codés

Les utilisateurs au sein du même groupe de stratégie (par ex., ceux ayant reçu la même stratégie de sécurité) détiendront les clés pour accéder aux données stockées sur le noeud d'extrémité, ainsi qu'à celles placées sur des clés USB et d'autres périphériques amovibles.

Les utilisateurs appartenant à un autre groupe de stratégies (avec codage activé) peuvent accéder, à l'aide d'un mot de passe, aux données codées placées dans le dossier`Fichiers partagés`. Ces utilisateurs ne peuvent toutefois pas lire les fichiers codés en dehors du dossier `Fichiers partagés`.

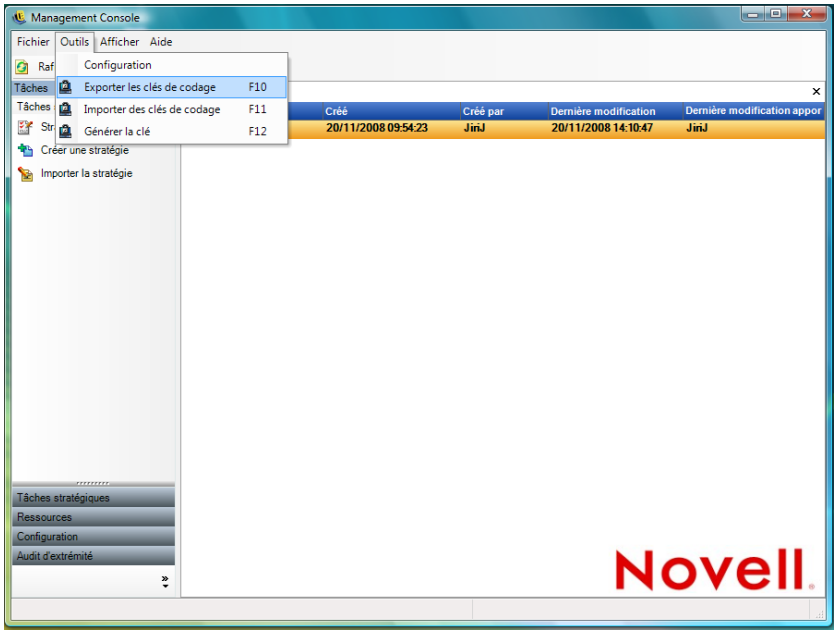
Les utilisateurs qui n'ont pas de codage activé dans leur stratégie ainsi que ceux qui n'ont pas de client ZENworks Security Client installé sur leurs ordinateurs (par ex., les sous-traitants) n'auront pas accès aux fichiers en dehors du dossier `Fichiers partagés`. Ils ont besoin de l'utilitaire de décodage de fichiers ZENworks® pour lire les fichiers et y accéder à l'aide d'un mot de passe Pour plus d'informations, reportez-vous à Section 1.9, « Utilisation de l'utilitaire de décodage de fichiers ZENworks », page 42.

1.8 Utilisation de la gestion de clé

La gestion de clé vous permet de sauvegarder, d'importer et de mettre à jour une clé de codage. Il est recommandé d'exporter et d'enregistrer les clés de codage pour garantir que les données pourront être décodées en cas d'échec système ou d'un changement de stratégie inopiné.

La clé commune est la clé de codage par défaut utilisée pour tous les agents de codage de données. Elle peut être mise à jour si elle est corrompue ou par mesure de sécurité. La génération d'une nouvelle clé commune diminue temporairement les performances pendant le réencodage du contenu géré.

Les commandes de la clé de codage sont accessibles via le menu *Outils* de la console de gestion.



1.8.1 Exportation des clés de codage

À des fins de sauvegarde et pour envoyer la clé à une autre instance du service de gestion, le « jeu de clés » de codage actuel peut être exporté vers un emplacement de fichiers désigné.

1. Cliquez sur *Outils* > *Exporter les clés de codage*.
2. Spécifiez le chemin et un nom de fichier ou cliquez sur le bouton *Parcourir* pour le rechercher et sélectionner un emplacement de fichiers.
3. Spécifiez un mot de passe. La clé ne peut pas être importée sans ce mot de passe.
4. Cliquez sur *OK*.

Tous les fichiers de clé de la base de données sont inclus dans le fichier exporté.

1.8.2 Importation des clés de codage

Vous pouvez importer des clés à partir d'une sauvegarde ou d'une autre instance du service de gestion. Cette opération permet aux noeuds d'extrémité gérés par le service de gestion de lire les fichiers protégés par d'autres installations ZENworks Endpoint Security Management. Lors de l'importation des clés, les doublons sont ignorés. Les clés importées font partie de votre « jeu de clés » et ne remplacent pas la clé commune actuelle. Toutes les clés sont transmises lors de la publication d'une nouvelle stratégie.

1. Cliquez sur *Outils* > *Importer les clés de codage*.
2. Spécifiez le nom de fichier et son emplacement ou cliquez sur le bouton *Parcourir* pour le rechercher et sélectionner le fichier de clé.
3. Spécifiez le mot de passe de la clé de codage.
4. Cliquez sur *OK* pour importer la clé dans la base de données.

1.8.3 Génération d'une clé

1 Cliquez sur *Outils* > *Générer la clé*.

Toutes les anciennes clés sont stockées dans la stratégie.

1.9 Utilisation de l'utilitaire de décodage de fichiers ZENworks

L'utilitaire de décodage de fichiers ZENworks® permet d'extraire les données protégées du dossier `Fichiers partagés` sur des périphériques de stockage amovibles codés. Cet outil simple peut être fourni à des tiers afin de leur permettre d'accéder au dossier `Fichiers partagés` sans pour autant pouvoir être placé sur un périphérique de stockage amovible.

- Section 1.9.1, « Utilisation de l'utilitaire de décodage de fichiers », page 42
- Section 1.9.2, « Configuration de l'utilitaire de décodage de fichiers », page 42

Les sections suivantes contiennent davantage d'informations :

1.9.1 Utilisation de l'utilitaire de décodage de fichiers

Procédure d'utilisation de l'utilitaire de décodage de fichiers :

1 Raccordez le périphérique de stockage au port approprié de votre ordinateur.

2 Ouvrez l'utilitaire de décodage de fichiers.

3 Accédez au répertoire `Fichiers partagés` du périphérique de stockage et sélectionnez le fichier souhaité.

4 Pour extraire les dossiers et non les fichiers, cliquez sur le bouton *Avancé*, puis sélectionnez *Répertoires*, accédez ensuite au répertoire approprié (cliquez sur *Base* pour revenir à la vue par défaut).

5 Sur la machine locale, recherchez et sélectionnez l'emplacement de stockage de ces fichiers.

6 Cliquez sur *Extraire*.

L'opération peut être contrôlée en cliquant sur le bouton *Afficher la progression*.

1.9.2 Configuration de l'utilitaire de décodage de fichiers

L'utilitaire de décodage de fichiers peut être configuré en mode administrateur avec le jeu de clés actuel et extraire toutes les données d'un périphérique de stockage codé. Cette configuration n'est pas recommandée, étant donné qu'elle risque de compromettre toutes les clés actuellement utilisées par ZENworks Storage Encryption Solution ; toutefois, dans les cas où les données sont impossibles à récupérer d'une autre façon, cette configuration peut s'avérer nécessaire.

Procédure de configuration de l'outil :

1 Créez un raccourci vers l'utilitaire de décodage de fichiers dans son répertoire actuel.

2 Cliquez avec le bouton droit de la souris sur le raccourci, puis cliquez sur *Propriétés*.

3 À la fin du nom cible et après les guillemets, entrez -k (exemple : `"C:\Admin Tools\stdecrypt.exe" -k`).

4 Cliquez sur *Appliquer* > *OK*.

5 Ouvrez l'outil à l'aide du raccourci, puis cliquez sur *Avancé*.

6 Cliquez sur le bouton *Charger les clés* pour ouvrir la boîte de dialogue Importer la clé.

7 Recherchez le fichier de clés et entrez le mot de passe des clés.

Tous les fichiers codés à l'aide de ces clés peuvent désormais être extraits.

1.10 Utilisation du générateur de clé de mot de passe prioritaire

La stratégie de sécurité appliquée par le client ZENworks® Security Client est probablement à l'origine des interruptions de productivité auxquelles peuvent être confrontés les utilisateurs en raison de restrictions de la connectivité, de la désactivation d'un logiciel ou d'un accès impossible à des périphériques de stockage amovibles. La modification des emplacements ou des paramètres de pare-feu élimine généralement ces restrictions et restaure la fonctionnalité interrompue. Toutefois, dans certains cas, la restriction s'applique à tous les emplacements et tous les paramètres de pare-feu ou il est impossible pour les utilisateurs de modifier un emplacement ou un paramètre de pare-feu.

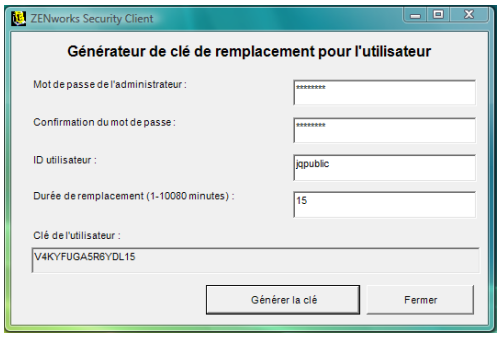
Dans pareils cas, les restrictions de la stratégie actuelle peuvent être éliminées par le biais d'un mot de passe prioritaire pour éviter toute interruption de productivité jusqu'à ce que la stratégie puisse être modifiée. Cette fonction permet à un administrateur de configurer un mot de passe prioritaire protégé pour une fonctionnalité et des utilisateurs spécifiés afin de garantir une poursuite temporaire des activités nécessaires.

Les mots de passe prioritaires désactivent la stratégie de sécurité actuelle et restaurent la stratégie par défaut Tous - Ouvert pour une période prédéfinie. À l'expiration de ce délai, la stratégie actuelle ou mise à jour est restaurée. Le mot de passe d'une stratégie est défini dans les paramètres Règles générales de la stratégie de sécurité.

L'application d'un mot de passe prioritaire :

- débloque l'application ;
- autorise les utilisateurs à modifier les emplacements ;
- autorise les utilisateurs à modifier les paramètres de pare-feu ;
- permet le contrôle du matériel (clés USB, CD-ROM, etc.)

Le mot de passe entré dans la stratégie ne doit jamais être communiqué à un utilisateur. Il est recommandé d'utiliser le générateur de clé de mot de passe prioritaire pour générer une clé à utiliser à court terme.



Pour générer une clé prioritaire :

1. Ouvrez le générateur de clé de mot de passe prioritaire (*Démarrer > Tous les programmes > Novell > Console de gestion ESM > Générateur de clé de mot de passe prioritaire*).
2. Entrez le mot de passe de la stratégie dans le champ *Mot de passe de l'administrateur*, puis confirmez-le dans le champ suivant.
3. Spécifiez le nom d'utilisateur avec lequel l'utilisateur final s'est logué.
4. Définissez la durée de désactivation de la stratégie.
5. Cliquez sur le bouton *Générer la clé* pour générer une clé prioritaire.

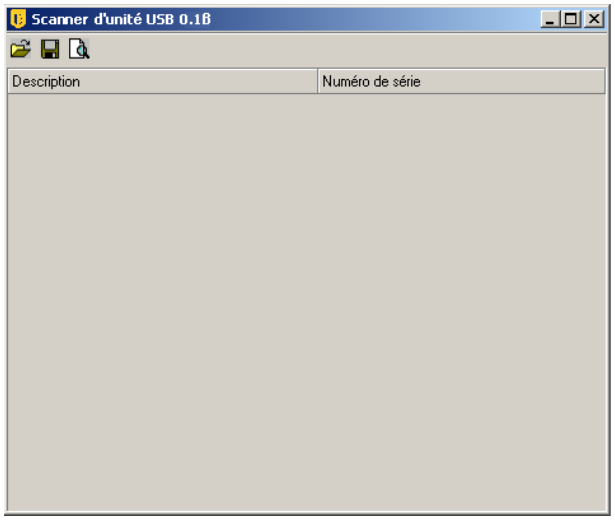
Cette clé peut être communiquée oralement à l'utilisateur lors d'un appel au service d'assistance ou copiée et collée dans un message électronique. L'utilisateur entre ensuite la clé dans la fenêtre d'administration de ZENworks Security Client (reportez-vous au *guide de l'utilisateur du client de sécurité ZENworks Endpoint Security Management*). Cette clé n'est valide que pour la stratégie de cet utilisateur et uniquement pour le délai spécifié. Elle ne peut être utilisée qu'une seule fois.

Remarque : Si l'utilisateur se délogue ou redémarre sa machine alors qu'il utilise un mot de passe prioritaire, ce dernier expire et il doit s'en procurer un nouveau.

Si une nouvelle stratégie a été émise avant l'expiration du délai, l'utilisateur doit être invité à cliquer sur Recherche d'une mise à jour des stratégies plutôt que sur le bouton *Charger la stratégie* de la boîte de dialogue À propos de ZENworks Security Client.

1.11 Scanner d'unité USB

Une liste des périphériques USB autorisés peut être générée et importée dans une stratégie à l'aide de l'outil facultatif Scanner d'unité USB (inclus avec le paquetage d'installation).



Pour générer une liste de périphériques autorisés :

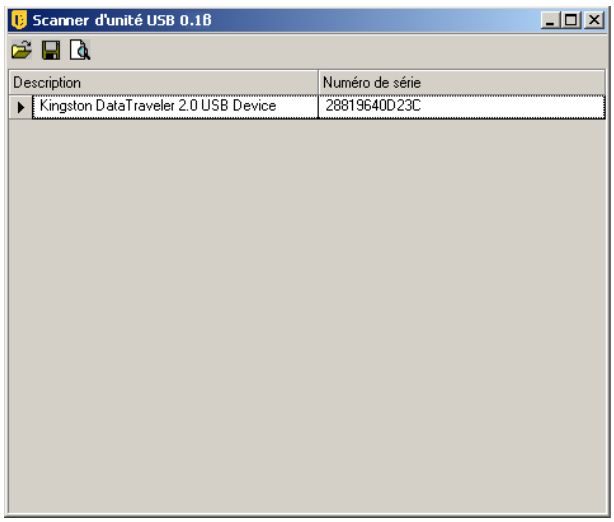
1. Ouvrez l'application Scanner d'unité USB.

   Remarque : Il s'agit d'une installation distincte du service de gestion et de la console de gestion. Un raccourci vers l'outil s'affiche sur le Bureau.

   ---

2 Insérez un périphérique USB dans le port USB de l'ordinateur. Le périphérique doit avoir un numéro de série.

3 Cliquez sur l'icône *Analyser* (). Le nom du périphérique et son numéro de série s'affichent dans les champs appropriés.



4 Répétez l'Étape 2et l'Étape 3 jusqu'à ce que tous les périphériques figurent dans la liste.

5 Cliquez sur l'icône `Enregistrer` ().

Consultez la section Section , « Périphériques préférés », page 56 pour obtenir des instructions concernant l'importation de la liste dans une stratégie.

Pour éditer un fichier enregistré, cliquez sur l'icône *Parcourir*() pour ouvrir le fichier.

Création et distribution des stratégies de sécurité

2

ZENworks® Security Client utilise des stratégies de sécurité pour conférer une sécurité d'emplacement aux utilisateurs mobiles. Les décisions relatives à la disponibilité du port et de l'application réseau, à l'accès aux périphériques de stockage de fichiers et à la connectivité filaire ou Wi-Fi sont prises par l'administrateur pour chaque emplacement.

Les stratégies de sécurité peuvent être personnalisées pour l'entreprise, des groupes d'utilisateurs individuels ou des machines/utilisateurs individuels. Elles garantissent une productivité maximale des employés tout en sécurisant le noeud d'extrémité ou, au contraire, limitent l'exécution de certaines applications et la disponibilité du matériel autorisé à certains employés uniquement.

Les sections suivantes contiennent un complément d'informations :

2.1 Navigation dans la console de gestion

Pour créer une stratégie de sécurité :

1. Dans la console de gestion, cliquez sur *Fichier* > *Créer une nouvelle stratégie*.
2. Nommez la stratégie, puis cliquez sur *Créer* pour que la barre d'outils et les onglets de la stratégie s'affichent dans la console de gestion.

Les sections suivantes décrivent l'interface utilisateur de la console de gestion concernant la création et la distribution des stratégies de sécurité via ZENworks® Endpoint Security Management :

2.1.1 Utilisation des onglets et de l'arborescence de la stratégie

Vous pouvez créer ou éditer une stratégie de sécurité en parcourant les onglets disponibles dans la partie supérieure de la console de gestion et en utilisant les options dans l'arborescence*Paramètres généraux* dans le volet gauche.

Les onglets disponibles sont les suivants :

- **Paramètres de stratégie généraux :** les paramètres de stratégie généraux sont appliqués par défaut à l'ensemble de la stratégie et ne sont pas liés à un emplacement spécifique.

  Ils permettent de configurer les paramètres suivants :

  - Paramètres de la stratégie

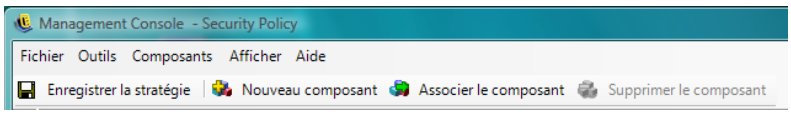
- Contrôle sans fil
- Matériel de communication
- Contrôle des périphériques de stockage
- Connectivité USB
- Codage de données
- ZENworks Security Client
- Application d'un VPN

- **Emplacements :** ces règles de stratégie sont appliquées dans un type d'emplacement spécifique, qu'il soit spécifié comme réseau unique ou comme type de réseau tel qu'une cafétéria ou un aéroport.
- **Règles de remédiation et d'intégrité :** ces règles garantissent l'exécution et la mise à jour de logiciels indispensables (comme un logiciel antivirus et anti-espion) sur le périphérique
- **Rapport de conformité :** indique à la stratégie si des données de rapport (notamment le type de données) sont collectées pour cette stratégie particulière.
- **Publication :** publie la stratégie exécutée aux différents utilisateurs, aux groupes d'utilisateurs du service Annuaire et aux différentes machines.

L'arborescence de la stratégie affiche les composants des sous-ensembles disponibles pour les catégories à onglets. Par exemple, les *paramètres de stratégie généraux* comportent des sous-ensembles de *Paramètres de stratégie*, *Contrôle sans fil*, *Matériel de communication* et *Contrôle des périphériques de stockage*. Seuls les éléments contenus sur la page du sous-ensemble principal sont requis pour définir une catégorie, les autres sous-ensembles étant facultatifs.

2.1.2 Utilisation de la barre d'outils de la stratégie

La barre d'outils de la stratégie comporte six commandes. La commande *Enregistrer la stratégie* est disponible tout au long de la création de la stratégie, alors que les commandes des composants ne sont disponibles que sous les onglets *Emplacements* et *Intégrité et remédiation*.



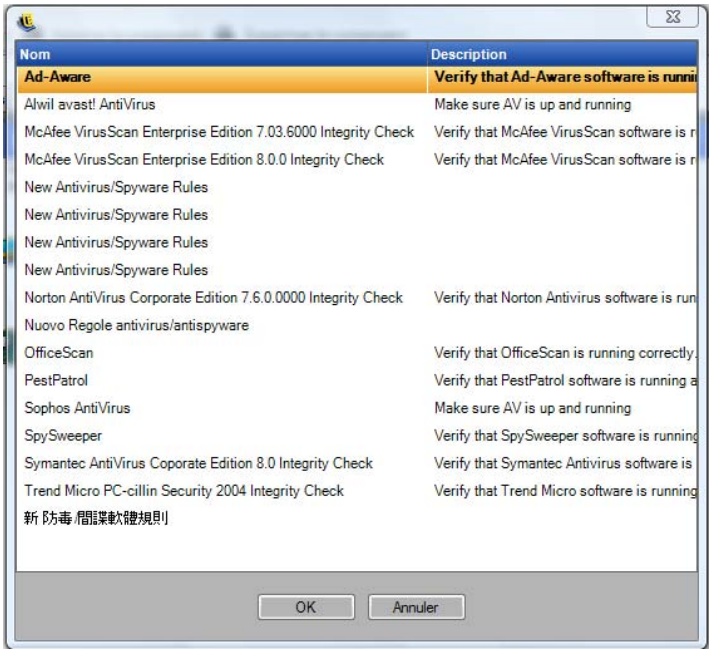
Les outils sont décrits ci-après :

- **Enregistrer Stratégie :** enregistre la stratégie dans son état actuel.

  Important : lors de l'exécution de chaque sous-ensemble de composants, il est vivement recommandé de cliquer sur l'icône *Enregistrer* dans la barre d'outils *Stratégie*. Si vous entrez des données incorrectes ou incomplètes dans un composant, l'écran de notification d'erreur s'affiche (reportez-vous à la rubrique Section 2.2.6, « Notification d'erreur », page 110 pour plus de détails).

- **Nouveau composant :** crée un nouveau composant dans un sous-ensemble d'emplacement ou d'intégrité. Une fois la stratégie enregistrée, un nouveau composant peut être associé dans d'autres stratégies.

- **Associer le composant :** ouvre l'écran de sélection du composant pour le sous-ensemble actuel Les composants disponibles incluent les composants prédéfinis fournis lors de l'installation ainsi que tous les composants créés dans d'autres stratégies.



Important : Les modifications apportées aux composants associés s'appliquent à toutes les autres instances de ce composant.

Par exemple, vous pouvez créer un composant d'emplacement unique appelé Professionnel qui définit les paramètres de sécurité et d'environnement réseau de l'entreprise à appliquer lorsqu'un noeud d'extrémité entre dans cet environnement. Ce composant peut désormais être appliqué à toutes les stratégies de sécurité. Les mises à jour des paramètres de sécurité ou d'environnement peuvent être modifiées dans le composant d'une stratégie. Elles actualiseront le même composant dans toutes les autres stratégies auxquelles il est associé.

Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

- **Supprimer le composant :** supprime un composant de la stratégie. Le composant peut toujours être associé à cette stratégie et à d'autres.
- **Rafraîchir la liste des stratégies :** rafraîchit la liste des stratégies.
- **Liste de rapports :** affiche la liste de rapports.

2.2 Création de stratégies de sécurité

1. Dans la console de gestion, cliquez sur *Fichier* > *Créer une nouvelle stratégie*.
2. Nommez la stratégie, puis cliquez sur *Créer* pour que la barre d'outils et les onglets de la stratégie s'affichent dans la console de gestion.
3. Configurez les paramètres de stratégie en utilisant les informations dans les sections suivantes :

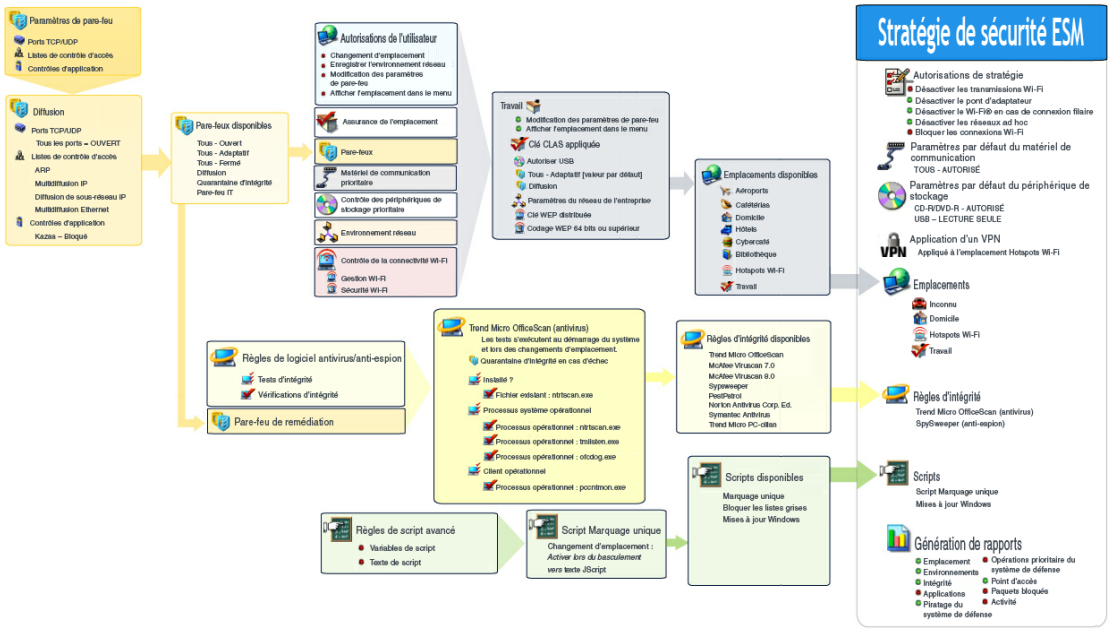
- Section 2.2.1, « Paramètres de stratégie généraux », page 50

- Section 2.2.2, « Emplacements », page 72
- Section 2.2.3, « Règles de remédiation et d'intégrité », page 98
- Section 2.2.4, « Rapport de conformité », page 106
- Section 2.2.5, « Publication », page 108
- Section 2.2.6, « Notification d'erreur », page 110
- Section 2.2.7, « Afficher l'utilisation », page 110

Pour créer des stratégies de sécurité, définissez tous les paramètres généraux (comportements par défaut), puis créez et associez les composants existants pour cette stratégie, comme les emplacements, les pare-feux et les règles d'intégrité, et enfin rédigez un rapport de conformité pour la stratégie.

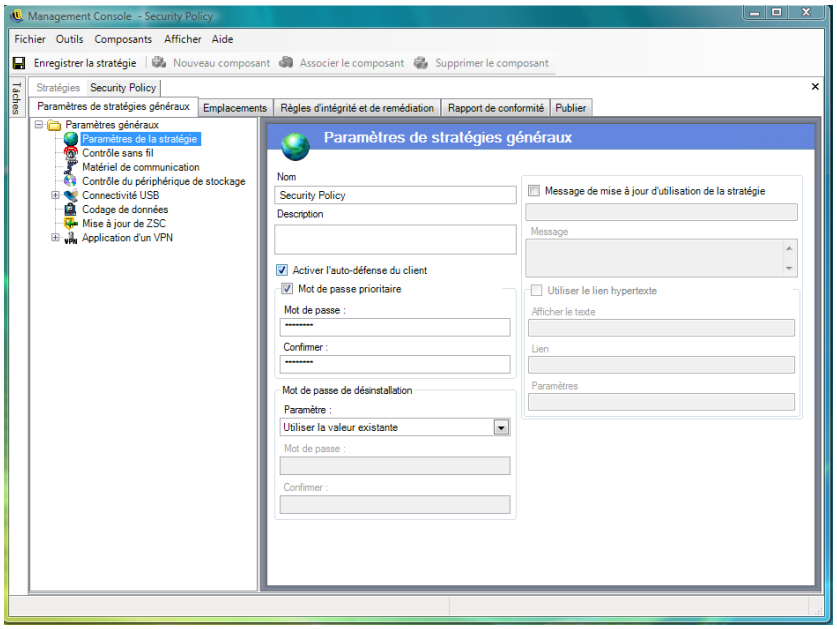
Les composants sont créés dans une stratégie « factice » ou associés à partir d'autres stratégies. Pour vos premières stratégies, vous êtes supposé créer tous les emplacements uniques, les paramètres de pare-feu et les règles d'intégrité pour l'entreprise. Ces composants sont stockés dans la base de données du service de gestion pour une éventuelle utilisation ultérieure dans d'autres stratégies.

Le schéma ci-dessous présente les composants pour chaque niveau ainsi que la stratégie résultante créée à partir des sélections.



2.2.1 Paramètres de stratégie généraux

Les paramètres de stratégie généraux sont appliqués comme valeurs de base par défaut pour la stratégie. Pour accéder à ce contrôle, accédez à la console de gestion, puis cliquez sur l'onglet *Paramètres de stratégie généraux*.



Les sections suivantes contiennent un complément d'informations sur les paramètres que vous pouvez configurer globalement :

- « Paramètres de la stratégie » page 51
- « Contrôle sans fil » page 52
- « Matériel de communication » page 53
- « Contrôle des périphériques de stockage » page 54
- « Connectivité USB » page 57
- « Codage de données » page 64
- « Mise à jour de ZSC » page 66
- « Application d'un VPN » page 67
- « Message utilisateur personnalisé » page 70
- « Liens hypertexte » page 71

Paramètres de la stratégie

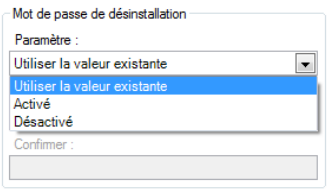
Les principaux paramètres généraux sont les suivants :

- **Nom et description :** le nom de la stratégie est spécifié au début du processus de création de la stratégie. Vous pouvez le modifier ou lui ajouter une description.
- **Activer l'auto-défense du client :** l'auto-défense du client peut être activée ou désactivée par la stratégie. Si vous cochez cette case, l'auto-défense du client est activée. Si vous la désélectionnez, l'auto-défense du client est désactivée pour tous les noeuds d'extrémité utilisant cette stratégie.
- **Mot de passe prioritaire :** cette fonction permet à un administrateur de configurer un mot de passe prioritaire qui peut désactiver temporairement la stratégie pendant une période spécifiée. Cochez la case *Mot de passe prioritaire*et entrez le mot de passe dans le champ approprié. Entrez de nouveau le mot de passe dans le champ de confirmation. Utilisez ce mot de passe

dans le générateur de mot de passe prioritaire pour créer la clé de mot de passe pour cette stratégie. Pour plus d'informations, reportez-vous à Section 1.10, « Utilisation du générateur de clé de mot de passe prioritaire », page 43.

Avertissement : Il est vivement recommandé de ne pas communiquer ce mot de passe à des utilisateurs Le générateur de mot de passe prioritaire doit être utilisé pour créer une clé temporaire pour ces utilisateurs.

- **Mot de passe de désinstallation :** il est recommandé d'installer chaque client ZENworks* Security Client avec un mot de passe de désinstallation pour éviter que les utilisateurs ne désinstallent le logiciel. Ce mot de passe est normalement configuré à l'installation ; toutefois, il peut être mis à jour, activé ou désactivé via la stratégie.



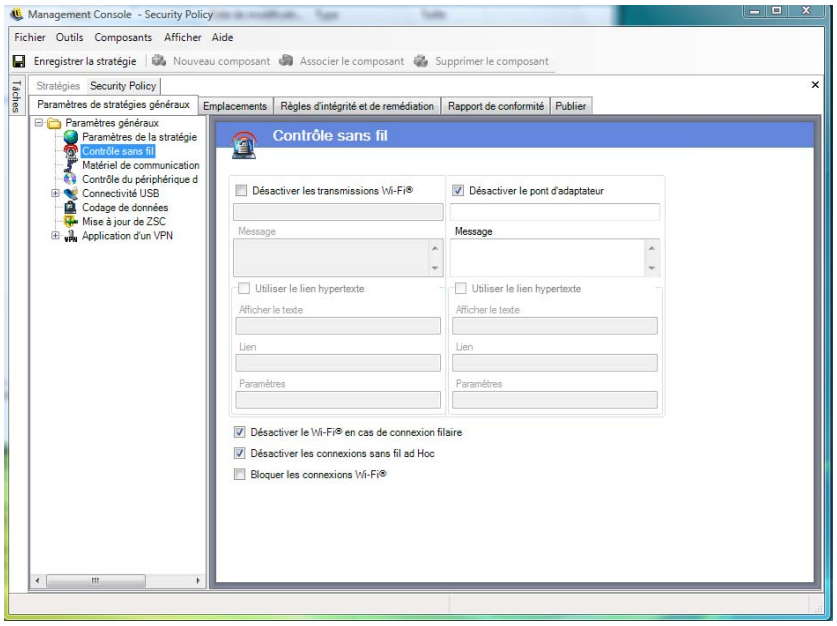
Vous pouvez sélectionner l'un des paramètres suivants dans la liste déroulante.

- **Utiliser celui existant :** ce mode correspond au paramétrage par défaut. Il conserve le mot de passe actuel.
- **Activé :** active un mot de passe de désinstallation ou le modifie. Spécifiez le nouveau mot de passe, puis confirmez-le
- **Mode Désactivé :** désactive l'obligation de spécifier un mot de passe de désinstallation.

- **Utiliser le message de mise à jour de la stratégie :** vous pouvez afficher un message utilisateur personnalisé lors de la mise à jour de la stratégie. Cochez la case, puis entrez les informations du message dans les champs prévus à cet effet.
- **Utiliser le lien hypertexte :** vous pouvez ajouter un lien hypertexte donnant accès à des informations complémentaires, à la stratégie d'entreprise, etc. (reportez-vous à la section « Liens hypertexte » page 71 pour plus d'informations).

Contrôle sans fil

Le contrôle sans fil définit globalement les paramètres de connectivité de l'adaptateur afin de protéger le noeud d'extrémité et le réseau. Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, puis cliquez sur l'icône *Contrôle sans fil* dans l'arborescence de stratégie à gauche.



Les paramètres de contrôle sans fil incluent les éléments suivants :

- **Désactiver les transmissions Wi-Fi :** désactive globalement tous les adaptateurs Wi-Fi, jusqu'à la réduction au silence complet d'une radio Wi-Fi intégrée.

  Vous pouvez choisir d'afficher un message utilisateur personnalisé et un lien hypertexte lorsque l'utilisateur tente d'activer une connexion Wi-Fi. Pour plus d'informations, reportez-vous à « Message utilisateur personnalisé » page 70.

- **Désactiver le pont d'adaptateur :** désactive globalement la fonctionnalité de pont réseau prévue dans Windows* XP, qui permet à l'utilisateur de relier plusieurs adaptateurs via un pont et de faire office de hub sur le réseau.

  Vous pouvez choisir d'afficher un message utilisateur personnalisé et un lien hypertexte lorsque l'utilisateur tente d'activer une connexion Wi-Fi. Pour plus d'informations, reportez-vous à « Message utilisateur personnalisé » page 70.

- **Désactiver le Wi-Fi® en cas de connexion filaire :** désactive globalement tous les adaptateurs Wi-Fi si la connexion de l'utilisateur est de type filaire (LAN via la carte d'interface réseau).

- **Désactiver les connexions sans fil ad hoc :** désactive globalement toute la connectivité ad hoc, la remplace par une connectivité Wi-Fi via un réseau (par exemple, via un point d'accès) et restreint toute la réseautique poste à poste de ce type.

- **Bloquer les connexions Wi-Fi :** bloque globalement les connexions Wi-Fi sans réduire la radio Wi-Fi au silence. Utilisez ce paramètre si vous souhaitez désactiver les connexions Wi-Fi, mais continuer à utiliser des points d'accès pour la détection d'emplacements. Pour plus d'informations, reportez-vous à Section 2.2.2, « Emplacements », page 72.

Matériel de communication

Les paramètres du matériel de communication contrôlent, par emplacement, les types de matériel qui sont autorisés à se connecter dans cet environnement réseau.

Remarque : Vous pouvez définir des contrôles du matériel de communication globalement sous l'onglet *Paramètres de stratégie généraux* ou pour des emplacements individuels sous l'onglet *Emplacements*.

Pour définir des contrôles du matériel de communication de manière globale, cliquez sur l'onglet *Paramètres de stratégie généraux*, développez les *Paramètres généraux* dans l'arborescence, puis cliquez sur *Matériel de communication*.

Pour définir des contrôles du matériel de communication pour un emplacement, cliquez sur l'onglet *Emplacements*, développez l'emplacement souhaité dans l'arborescence, puis cliquez sur *Matériel de communication*. Pour plus d'informations sur la configuration des paramètres du matériel de communication pour un emplacement, reportez-vous à la rubrique « Matériel de communication » page 75.

Choisissez d'activer ou de désactiver le paramètre général pour chaque périphérique de communication listé :

- **1394 (FireWire) :** contrôle le port d'accès FireWire* sur le noeud d'extrémité.
- **IrDA :** contrôle le port d'accès infrarouge sur le noeud d'extrémité.
- **Bluetooth :** contrôle le port d'accès Bluetooth* sur le noeud d'extrémité.
- **Série / Parallèle :** contrôle l'accès au ports série et parallèle sur le noeud d'extrémité.

Contrôle des périphériques de stockage

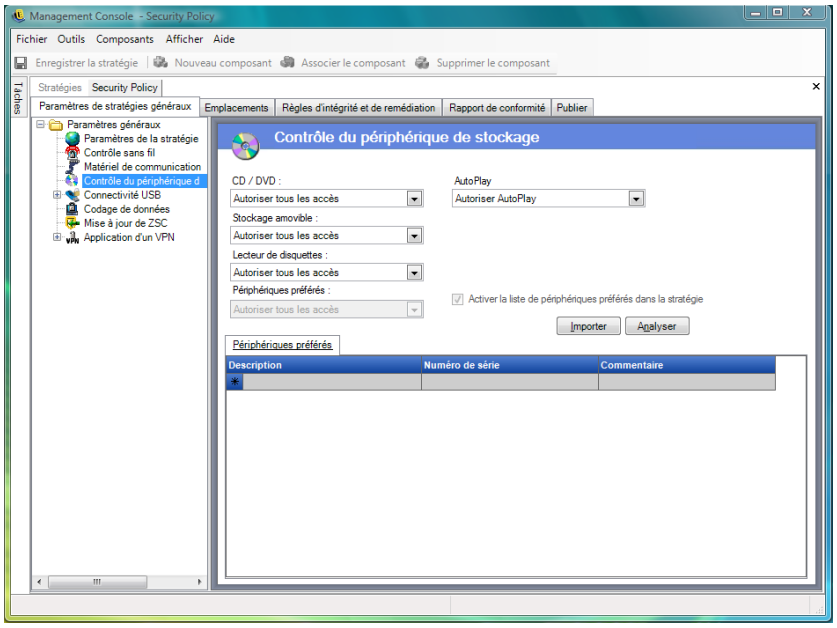
Les contrôles des périphériques de stockage définissent les paramètres par défaut des périphériques de stockage de la stratégie. Ceux-ci spécifient si les périphériques de stockage de fichiers externes sont autorisés à lire ou écrire des fichiers, fonctionnent en mode lecture seule ou sont entièrement désactivés. Lorsqu'ils sont désactivés, ces périphériques sont incapables de récupérer des données provenant du noeud d'extrémité alors que le disque dur et toutes les unités réseau restent accessibles et opérationnelles.

Le contrôle des périphériques de stockage de ZENworks Endpoint Security Management n'est pas autorisé si Storage Encryption Solution est activé.

Remarque : Vous pouvez définir les contrôles des périphériques de stockage de manière globale sous l'onglet *Paramètres de stratégie généraux* ou pour des emplacements individuels sous l'onglet *Emplacements*.

Pour définir les contrôles des périphériques de stockage de manière globale, cliquez sur l'onglet *Paramètres de stratégie généraux*, développez les *Paramètres généraux* dans l'arborescence, puis cliquez sur *Contrôle des périphériques de stockage*.

Pour définir les contrôles des périphériques de stockage pour un emplacement, cliquez sur l'onglet *Emplacements*, développez l'emplacement souhaité dans l'arborescence, puis cliquez sur *Contrôle des périphériques de stockage*. Pour plus d'informations, reportez-vous à « Matériel de communication » page 75.



Le contrôle des périphériques de stockage est réparti dans les catégories suivantes :

- **CD/DVD :** contrôle tous les périphériques figurant dans la liste des *unités DVD/CD-ROM* dans le gestionnaire des périphériques de Windows.
- **Stockage amovible :** contrôle tous les périphériques de stockage amovibles listés sous *Unités de disque* dans le gestionnaire des périphériques de Windows.
- **Unité de disquette :** contrôle tous les périphériques listés sous *Unités de disquette* dans le gestionnaire des périphériques de Windows.
- **Périphériques préférés :** autorise uniquement les périphériques de stockage amovibles listés dans la fenêtre Contrôle des périphériques de stockage. Tous les autres périphériques de stockage amovibles ne figurant pas dans cette liste ne sont pas autorisés.

Les unités de stockage fixes (disques dur) et les unités réseau (lorsqu'elles sont disponibles) sont toujours autorisées.

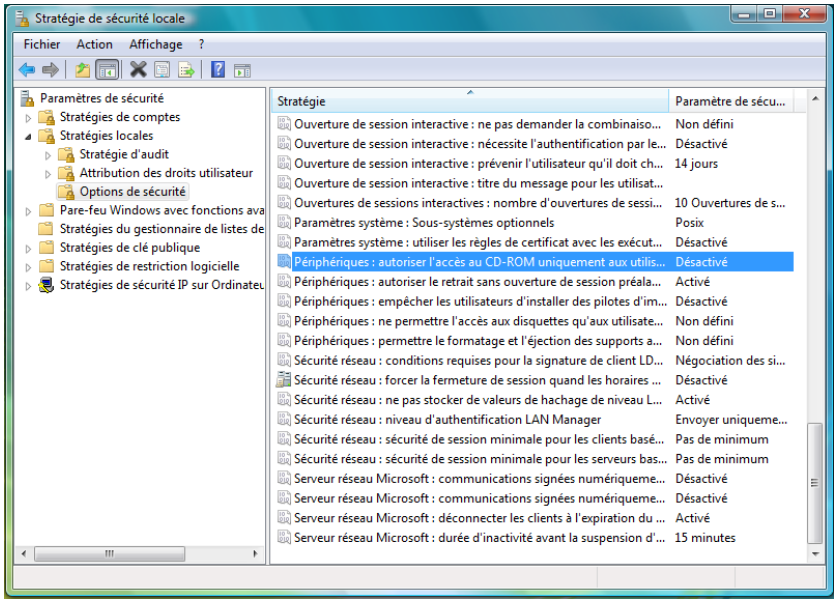
Pour définir les valeurs par défaut des périphériques de stockage de la stratégie, sélectionnez le paramètre général des deux types dans les listes déroulantes :

- **Activer:** ce type de périphérique est autorisé par défaut.
- **Désactiver :** ce type de périphérique n'est pas autorisé. Si des utilisateurs tentent d'accéder à des fichiers se trouvant sur un périphérique de stockage défini, ils reçoivent un message d'erreur du système d'exploitation ou de l'application qui tente d'accéder au périphérique de stockage local, les informant de l'échec de l'opération
- **Lecture seule :** ce type de périphérique est configuré pour un accès en lecture seule. Si des utilisateurs tentent d'écrire sur le périphérique, ils reçoivent un message d'erreur du système d'exploitation ou de l'application qui tente d'accéder au périphérique de stockage local, les informant de l'échec de l'opération

---

Remarque : Si vous souhaitez désactiver ou configurer en lecture seule des unités de CD-ROM ou de disquette sur un groupe de noeuds d'extrémité, les stratégies *Périphériques : limiter l'accès des CD-ROM à l'utilisateur logué localement uniquement* et *Périphériques : limiter l'accès des*

disquettes à l'utilisateur logué localement uniquement dans les paramètres de sécurité locaux (transmis via un objet Stratégie de groupe du service Annuaire) doivent être définies sur Désactivé. Pour vérifier, ouvrez l'objet Stratégie de groupe ou les outils d'administration sur une machine. Vérifiez dans Paramètres de sécurité locaux - Options de sécurité que les deux périphériques sont désactivés. Désactivé est la valeur par défaut.



Les sections suivantes contiennent davantage d'informations :

- « Périphériques préférés » page 56
- « Importation de listes de périphériques » page 57

Périphériques préférés

Les périphériques de stockage amovibles préférés peuvent éventuellement être ajoutés à une liste, pour permettre uniquement l'accès aux périphériques autorisés lorsque le paramètre général est utilisé au niveau d'un emplacement. Les périphériques figurant dans cette liste doivent avoir un numéro de série.

Pour lister un périphérique préféré :

1. Insérez le périphérique dans le port USB de la machine sur laquelle la console de gestion est installée.
2. Une fois le périphérique prêt, cliquez sur le bouton *Analyser*. Si le périphérique a un numéro de série, sa description et son numéro de série s'affichent dans la liste.
3. Sélectionnez un paramètre dans la liste déroulante (le paramètre de *périphérique amovible général* ne s'applique pas pour cette stratégie) :
   - **Activé :** les périphériques figurant dans la liste des périphériques préférés disposent de toutes les fonctionnalités de lecture/écriture ; tous les autres périphériques USB et de stockage externes sont désactivés.
   - **Lecture seule :** les périphériques figurant dans la liste des périphériques préférés disposent de la fonctionnalité de lecture seule ; tous les autres périphériques USB et de stockage externes sont désactivés.

Répétez cette procédure pour tous les périphériques autorisés dans cette stratégie. Le même paramètre est appliqué à tous les périphériques.

Remarque : Les paramètres du contrôle des périphériques de stockage basé sur l'emplacement ont la priorité sur les paramètres généraux. Par exemple, vous pouvez décider d'autoriser tous les périphériques de stockage externes pour l'emplacement « Travail », mais uniquement le paramètre général par défaut pour tous les autres emplacements, afin de limiter l'accès des utilisateurs aux périphériques figurant sur la liste des périphériques préférés.

Importation de listes de périphériques

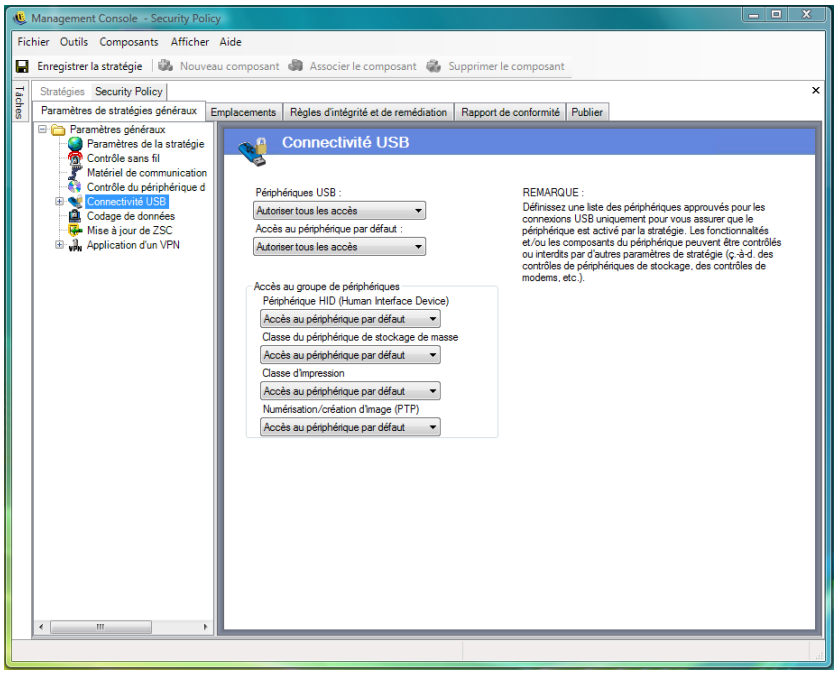
L'application Scanner USB de Novell génère une liste des périphériques et de leur numéro de série (Section 1.11, « Scanner d'unité USB », page 44). Pour importer cette liste, cliquez sur *Importer* et recherchez la liste. Les champs *Description* et *Numéro de série* sont complétés sur la base de cette liste.

Connectivité USB

Tous les périphériques se connectant via le BUS USB peuvent être autorisés ou refusés par la stratégie. Vous pouvez analyser ces périphériques dans la stratégie à partir du rapport d'inventaire des périphériques USB ou en analysant tous les périphériques actuellement connectés à une machine. Vous pouvez filtrer ces périphériques en fonction du fabricant, du nom, du numéro de série, du type de produit, etc. Pour des raisons de prise en charge, l'administrateur peut configurer la stratégie de façon à ce qu'elle accepte un ensemble de périphériques, sur la base du type de fabricant (par exemple, tous les périphériques HP sont autorisés) ou du type de produit (tous les périphériques HID USB, comme la souris et le clavier, sont autorisés). En outre, vous pouvez autoriser des périphériques individuels afin d'éviter l'introduction de périphériques non pris en charge dans le réseau (par exemple, aucune imprimante n'est autorisée à l'exception de celle-ci).

Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, puis cliquez sur*Connectivité USB* dans l'arborescence de stratégie à gauche.

Figure 2-1 *Page Connectivité USB.*



L'accès est d'abord évalué en fonction de l'activation ou de la désactivation du bus, ce qui est déterminé par le paramètre *Périphériques USB*. Si ce paramètre est défini sur *Désactiver tous les accès*, le périphérique est désactivé et l'évaluation s'arrête. S'il est défini sur *Autoriser tous les accès*, le client poursuit l'évaluation et commence à chercher des correspondances de filtre. Comme bon nombre d'autres champs de la console de gestion ZENworks, lorsqu'elle est définie sur un emplacement, la valeur *Périphériques USB* peut également être définie sur *Appliquer les paramètre généraux* pour utiliser en priorité la valeur générale de ce champ.

Le client rassemble les filtres appliqués à partir de la stratégie, en fonction de l'emplacement et des paramètres généraux. Le client groupe ensuite les filtres en fonction de l'accès dans les groupes suivants :

- **Toujours bloquer :** bloque toujours le périphérique. Ce paramètre ne peut pas être remplacé.
- **Toujours autoriser :** autorise toujours l'accès à moins que le périphérique ne corresponde à un filtre *Toujours bloquer*.
- **Bloquer :** bloque l'accès à moins que le périphérique ne corresponde à un filtre *Toujours autoriser*.
- **Autoriser :** autorise l'accès à moins que le périphérique ne corresponde à un filtre *Toujours bloquer*ou *Bloquer*.
- **Accès par défaut au périphérique :** fournit au périphérique le niveau d'accès *Accès par défaut au périphérique* en l'absence de toute autre correspondance.

Un périphérique est évalué par rapport à chaque groupe dans l'ordre ci-dessus (*Toujours bloquer*, puis *Toujours autoriser*, etc.). Lorsqu'un périphérique correspond à au moins un filtre d'un groupe, l'accès au périphérique est défini sur ce niveau et l'évaluation s'arrête. Si le périphérique est évalué par rapport à tous les filtres et qu'aucune correspondance n'est trouvée, le niveau *Accès par défaut au périphérique* est appliqué.

L'accès au périphérique défini dans la zone *Accès au groupe de périphériques* est pris en considération au même titre que tous les autres filtres utilisés à cet emplacement. Cette opération est effectuée en générant des filtres de correspondance pour chaque groupe lorsque la stratégie est publiée pour le client. Ces filtres sont les suivants :

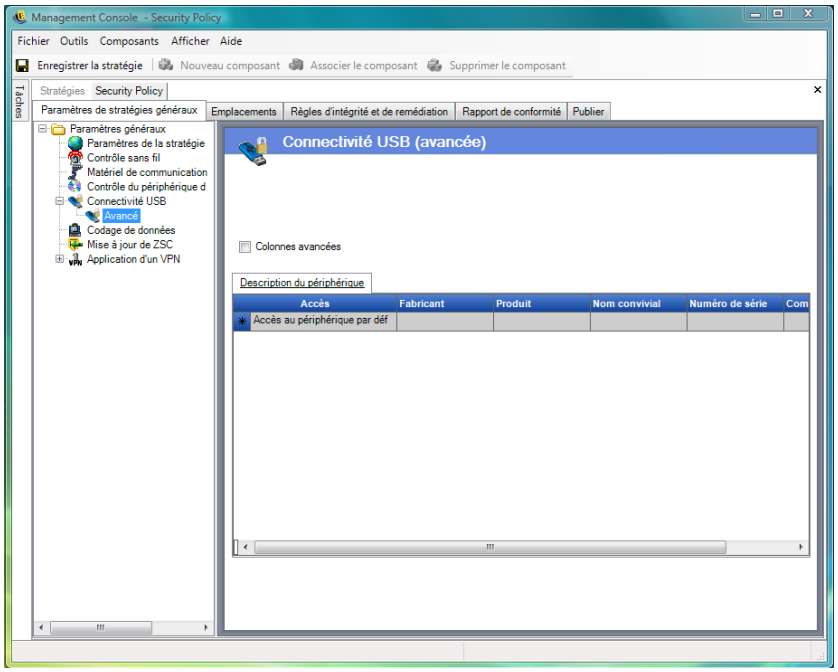
Accès au groupe de périphériques :	Filtre :
Périphérique HID (Human Interface Device)	La "classe de périphérique" est égale à 3.
Classe du périphérique de stockage de masse	La "classe de périphérique" est égale à 8.
Classe d'impression	La "classe de périphérique" est égale à 7.
Numérisation/création d'image (PTP)	La "classe de périphérique" est égale à 6.

Avancé

Dans la plupart des situations, les quatre groupes de périphérique listés sur la page Connectivité USB (Périphérique HID, Classe du périphérique de stockage de masse, Classe d'impression et Numérisation/création d'image) suffisent pour autoriser ou refuser l'accès à la plupart des périphériques USB. Si vous avez des périphériques qui n'appartiennent à aucun de ces groupes, vous pouvez configurer des paramètres sur la page Connectivité USB avancée. Vous pouvez également utiliser les paramètres sur la page Avancé pour autoriser l'accès (liste blanche) à certains périphériques même si l'accès pourrait être refusé en vertu du paramétrage défini sur la page Connectivité USB.

Pour accéder aux options Connectivité USB avancée, cliquez sur le signe plus en regard de *Connectivité USB* dans l'arborescence *Paramètres généraux*, puis cliquez sur *Avancé*. Vous pouvez utiliser le rapport Audit de périphériques USB pour obtenir toutes les informations qui pourraient vous être utiles sur la page Contrôle de connectivité USB avancée.

Figure 2-2 *Page Connectivité USB avancée.*



Les colonnes par défaut sont les suivantes :

- **Accès :** Placez le pointeur de la souris sur *Accès par défaut au périphérique*, puis spécifiez un niveau d'accès :
  - **Toujours bloquer :** bloque toujours le périphérique. Ce paramètre ne peut pas être remplacé.
  - **Toujours autoriser :** autorise toujours l'accès à moins que le périphérique ne corresponde à un filtre *Toujours bloquer*.
  - **Bloquer :** bloque l'accès à moins que le périphérique ne corresponde à un filtre *Toujours autoriser*.
  - **Autoriser :** autorise l'accès à moins que le périphérique ne corresponde à un filtre *Toujours bloquer*ou *Bloquer*.
  - **Accès par défaut au périphérique :** fournit au périphérique le niveau d'accès *Accès par défaut au périphérique* en l'absence de toute autre correspondance.
- **Fabricant :** Cliquez sur la colonne *Fabricant*, puis tapez le nom du fabricant que vous souhaitez inclure dans le filtre (Canon, par exemple).
- **Produit :** Cliquez sur la colonne *Produit*, puis tapez le nom du produit que vous souhaitez inclure dans le filtre.
- **Nom convivial :** Cliquez sur la colonne *Nom convivial*, puis tapez le nom convivial du périphérique que vous souhaitez inclure dans le filtre.
- **Numéro de série :** Cliquez sur la colonne *Numéro de série*, puis tapez le numéro de série du périphérique que vous souhaitez inclure dans le filtre.
- **Commentaire :** Cliquez sur la colonne *Commentaire*, puis tapez le commentaire que vous souhaitez inclure dans le filtre (Canon, par exemple).

Vous pouvez cliquer dans la zone *Colonnes avancées* pour ajouter les colonnes suivantes : *Version USB*, *Classe de périphérique, Sous-classe de périphérique, Protocole de périphérique, ID fournisseur, ID produit, Périphérique BCD, ID périphérique O/S* et *Classe périphérique O/S*.

Un périphérique met un ensemble d'attributs à la disposition du système d'exploitation. Le client met en relation ces attributs avec les champs requis par un filtre. Tous les champs du filtre doivent correspondre à un attribut fourni par le périphérique pour obtenir une correspondance. Si le périphérique ne fournit pas d'attribut ou de champ requis par le filtre, ce filtre n'a pas de correspondance.

Supposons, par exemple, qu'un périphérique fournisse les attributs suivants : Fabricant : Acme, Classe : 8, Numéro de série : "1234".

Le filtre Classe == 8 reprendra ce périphérique. Le filtre Produit == "Acme" ne le reprendra pas car le périphérique n'a pas fourni d'attribut de produit au système d'exploitation.

Les champs suivants sont des correspondances de sous-chaînes : Fabricant, Produit et Nom convivial. Tous les autres champs sont des correspondances exactes.

Il est intéressant de noter que le champ Numéro de série USB (SN) par spéc. n'est unique que lorsqu'il est pris en considération lors de la spécification des champs suivants avec le numéro de série : Version USB, ID fournisseur, ID production et Périphérique BCD.

Les valeurs actuellement valides pour la version USB en décimale sont : 512 - USB 2.0, 272 - USB 1.1, 256 - USB 1.0.

Les sections suivantes contiennent un complément d'informations :

- « Ajout manuel de périphériques » page 61
- « Mise en liste blanche/noire d'un périphérique par type de produit » page 62

Ajout manuel de périphériques

La méthode suivante vous permet de compléter la liste de façon à pouvoir autoriser ou refuser la connectivité USB à certains périphériques :

Pour ajouter manuellement un périphérique :

1. Insérez le périphérique dans le port USB de la machine sur laquelle la console de gestion est installée.
2. Une fois le périphérique prêt, cliquez sur le bouton *Analyser*. Si le périphérique a un numéro de série, sa description et son numéro de série s'affichent dans la liste.
3. Sélectionnez un paramètre dans la liste déroulante (le paramètre de *Périphérique amovible général* n'est pas appliqué pour cette stratégie) :
   - **Activer :** les périphériques figurant dans la liste des périphériques préférés disposent de toutes les fonctionnalités de lecture/écriture ; tous les autres périphériques USB et de stockage externes sont désactivés.
   - **Lecture seule :** les périphériques figurant dans la liste des périphériques préférés disposent de la fonctionnalité de lecture seule ; tous les autres périphériques USB et de stockage externes sont désactivés.

Répétez ces étapes pour chaque périphérique à autoriser dans cette stratégie. Le même paramètre est appliqué à tous les périphériques.

Mise en liste blanche/noire d'un périphérique par type de produit

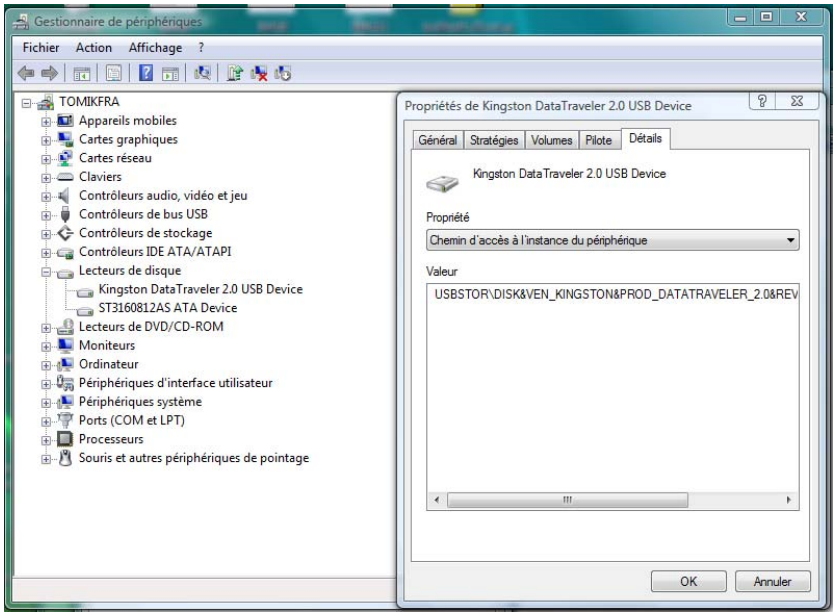
La section suivante décrit comment mettre en liste blanche/noire un périphérique USB par type de produit.

Remarque : La procédure suivante indique, à titre d'exemple, comment pouvoir identifier le type de produit pour votre périphérique de stockage amovible USB. Selon les informations fournies par le fabricant de votre périphérique, il se peut que la procédure ne fonctionne pas. Vous pouvez utiliser le rapport Audit de périphériques USB pour obtenir toutes les informations qui pourraient vous être utiles sur la page Contrôle de connectivité USB avancée.

Pour déterminer le type de produit d'un périphérique de stockage amovible USB :

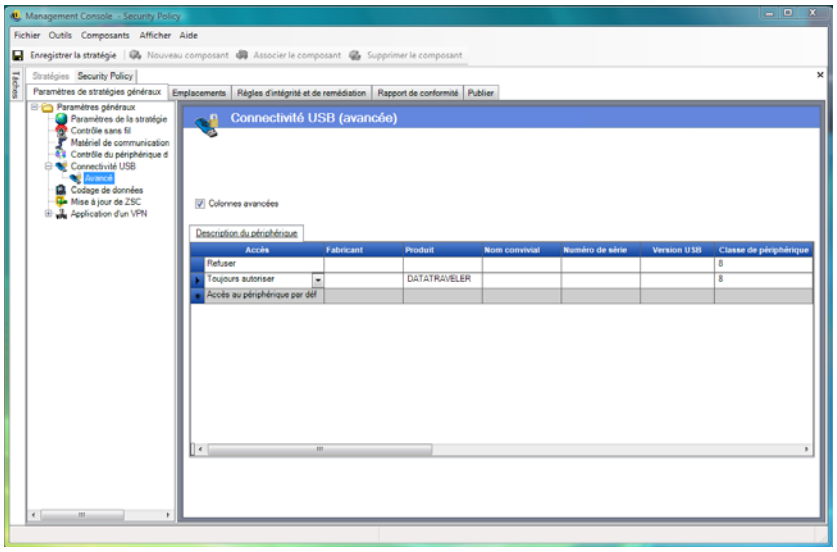
1. Dans la console de gestion de l'ordinateur Microsoft Windows, cliquez sur *Gestionnaire de périphériques*.
2. Cliquez sur le signe plus en regard de *Unités de disque* pour développer l'arborescence.
3. Cliquez avec le bouton droit sur le périphérique USB, puis cliquez sur *Propriétés* pour afficher la boîte de dialogue Propriétés du périphérique.
4. Cliquez sur l'onglet *Détails*, puis sélectionnez *Numéro d'identification de l'instance du périphérique* dans la liste déroulante.

   Le type de produit est indiqué après &PROD dans le numéro d'identification de l'instance du périphérique. Dans l'exemple suivant, le type de produit est DATATRAVELER.



Mise en liste blanche d'un périphérique USB : Sur la page Connectivité USB, ne modifiez pas les paramètres par défaut. Sur la page Avancé, créez deux lignes. Sur la première ligne, indiquez *Refuser* dans la colonne *Accès* et 8 dans la colonne *Classe de périphérique* (si la colonne *Classe de périphérique* n'est pas disponible, cochez la case *Colonnes avancées*). Sur la seconde ligne, spécifiez *Toujours autoriser* dans la colonne *Accès*, le type de produit (DATATRAVELER, pour cet exemple) dans la colonne *Produit* et 8 dans la colonne *Classe de périphérique*.

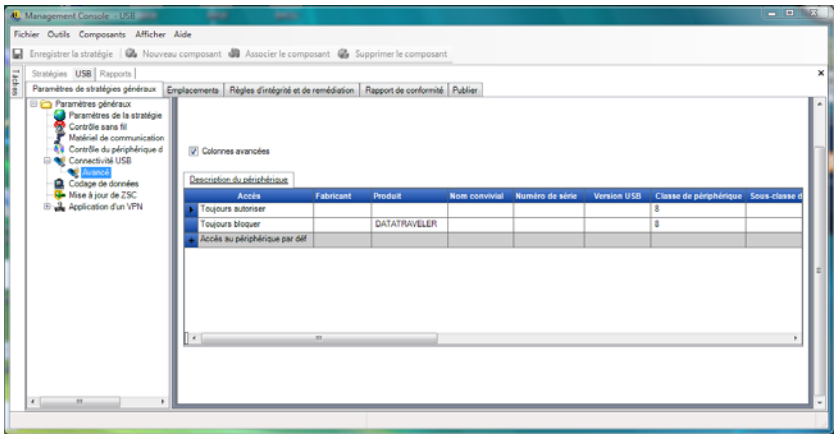
La page Connectivité USB (avancée) doit se présenter comme dans l'exemple suivant :



Le périphérique USB DATATRAVELER est maintenant en liste blanche, ce qui signifie qu'il dispose d'un accès octroyé par ZENworks Endpoint Security Management et que tous les autres périphériques de stockage amovibles USB ont un accès refusé.

Mise en liste noire d'un périphérique USB : Sur la page Connectivité USB, ne modifiez pas les paramètres par défaut. Sur la page Avancé, créez deux lignes. Sur la première ligne, indiquez *Toujours autoriser* dans la colonne *Accès* et 8 dans la colonne *Classe de périphérique* (si la colonne *Classe de périphérique* n'est pas disponible, cochez la case *Colonnes avancées*). Sur la seconde ligne, spécifiez *Toujours bloquer* dans la colonne *Accès*, le type de produit (DATATRAVELER, pour cet exemple) dans la colonne *Produit* et 8 dans la colonne *Classe de périphérique*.

La page Connectivité USB (avancée) doit se présenter comme dans l'exemple suivant :



Le périphérique USB DATATRAVELER est maintenant en liste noire, ce qui signifie que l'accès lui est refusé par ZENworks Endpoint Security Management et que tous les autres périphériques de stockage amovibles USB disposent d'un accès autorisé.

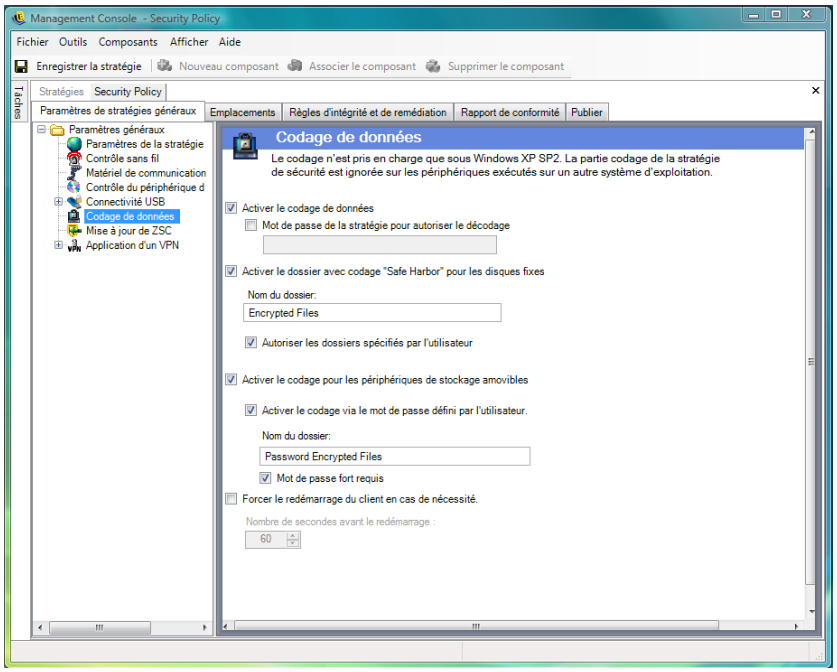
Codage de données

Le codage de données détermine si le codage de fichier est appliqué sur le noeud d'extrémité et quel type de codage est disponible. Vous pouvez coder des données pour permettre le partage de fichiers (avec protection par mot de passe) ou définir des données codées ne pouvant être lues que sur des ordinateurs exécutant ZENworks Storage Encryption Solution.

Remarque : Le codage n'est pris en charge que sous Windows XP SP2. La fonctionnalité de codage de la stratégie de sécurité est ignorée sur les périphériques qui ne prennent pas en charge ce système d'exploitation.

Le contrôle des périphériques de stockage de ZENworks Endpoint Security Management n'est pas autorisé si ZENworks Storage Encryption Solution est activé.

Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, puis cliquez sur*Codage de données* dans l'arborescence de stratégie à gauche.



Pour activer les contrôles individuels, cochez la case *Activer le codage de données*.

Remarque : Les clés de codage sont distribuées à toutes les machines qui reçoivent des stratégies du service de distribution de stratégies, que le codage de données soit activé ou non. Toutefois, ce contrôle indique à ZENworks Security Client d'activer ses pilotes de codage, qui permettent aux utilisateurs de lire les fichiers qu'ils ont reçus sans avoir besoin de l'utilitaire de décodage de fichiers. Reportez-vous à la rubrique Section 1.9, « Utilisation de l'utilitaire de décodage de fichiers ZENworks », page 42 pour plus d'informations.

Déterminez les niveaux de codage autorisés par cette stratégie :

- **Mot de passe de la stratégie autorisant le décodage :** spécifiez un mot de passe que tous les utilisateurs employant cette stratégie devront entrer avant de pouvoir décoder les fichiers codés stockés dans leurs dossiers `Safe Harbor`.

  Ce paramètre est facultatif. Laissez ce champ vide si vous ne souhaitez pas définir de mot de passe.

- **Activer le dossier avec codage « Safe Harbor » pour les disques fixes (volume autre que système) :** ce paramètre crée un dossier `Fichiers protégés par codage` à la racine de tous les volumes autres que système sur le noeud d'extrémité. Tous les fichiers contenus dans ce dossier sont codés et gérés par ZENworks Security Client. Les données de ce dossier sont automatiquement codées et uniquement accessibles par les utilisateurs autorisés sur cette machine.

  Vous pouvez modifier le nom du dossier en cliquant sur le champ *Nom du dossier*, en sélectionnant le texte actuel et en spécifiant le nom souhaité.

  - **Coder le dossier « Mes documents » de l'utilisateur :** cochez cette case pour définir le dossier `Mes documents` des utilisateurs comme un dossier codé (en plus du dossier `Safe Harbor`). Le codage ne s'applique qu'au dossier `Mes documents` local.
  - **Autoriser les dossiers spécifiés par l'utilisateur (volume autre que système) :** cochez cette case pour permettre aux utilisateurs de déterminer les dossiers de leur ordinateur qui doivent être codés. Ce paramètre s'applique uniquement aux dossiers locaux ; les périphériques de stockage amovibles et les unités réseau ne peuvent pas être codés.

Avertissement : Avant de désactiver le codage des données, assurez-vous que toutes les données contenues dans ces dossiers ont été extraites par l'utilisateur et stockées dans un autre emplacement.

- **Activer le codage pour les périphériques de stockage amovibles :** toutes les données inscrites sur des périphériques de stockage amovibles à partir d'un noeud d'extrémité protégé par cette stratégie sont codées. Les utilisateurs disposant de cette stratégie sur leur machine peuvent lire les données. Il est donc possible de partager des fichiers via le périphérique de stockage amovible au sein d'un groupe de stratégies. Les utilisateurs n'appartenant pas à ce groupe de stratégies ne peuvent pas lire les fichiers codés sur l'unité et ne peuvent accéder aux fichiers contenus dans le dossier `Fichiers partagés` (s'il est activé) qu'avec un mot de passe fourni.

  - **Activer le codage via le mot de passe défini par l'utilisateur :** ce paramètre permet à l'utilisateur de stocker des fichiers dans un dossier `Fichiers partagés` sur le périphérique de stockage amovible (ce dossier est créé automatiquement lorsque ce paramètre est appliqué). L'utilisateur peut spécifier un mot de passe lorsque des fichiers sont ajoutés à ce dossier, lequel est employé par les utilisateurs qui n'appartiennent pas au groupe de stratégies actuel pour extraire les fichiers.

Vous pouvez modifier le nom du dossier en cliquant sur le champ *Nom du dossier*, en sélectionnant le texte actuel et en spécifiant le nom souhaité.

- **Exiger un mot de passe fort :** ce paramètre oblige l'utilisateur à définir un mot de passe fort pour le dossier Fichiers partagés. Un mot de passe fort doit avoir les caractéristiques suivantes :
  - sept caractères ou plus
  - au moins un de chacun des quatre types de caractères :
    - majuscules de A à Z
    - minuscules de a à z
    - chiffres de 0 à 9
    - au moins un caractère spécial ~!@#$%^&*()+{}[]:;<>?,./

  Par exemple : y9G@wb?

Avertissement : Avant de désactiver le codage des données, assurez-vous que toutes les données contenues sur des périphériques de stockage amovibles ont été extraites par l'utilisateur et stockées dans un autre emplacement.

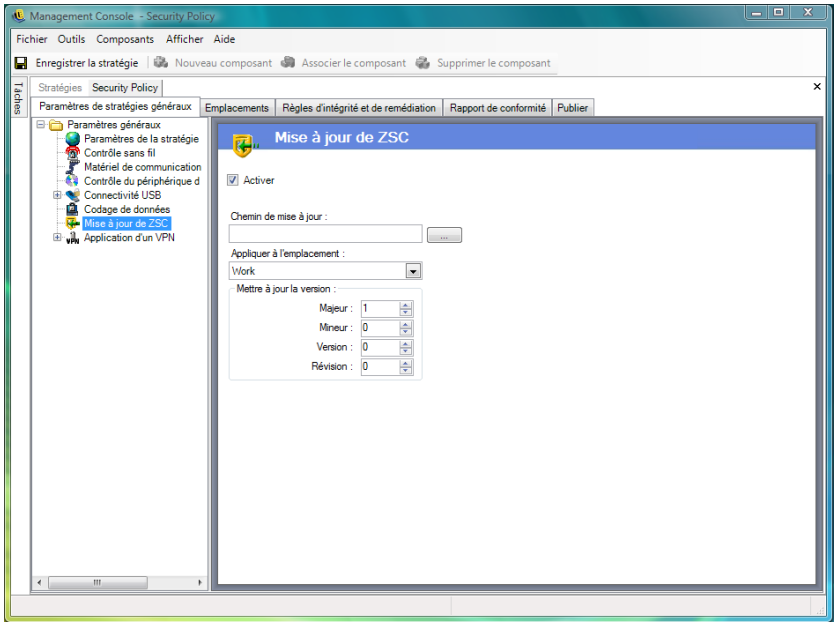
- **Forcer le redémarrage du client en cas de nécessité:** lorsque le codage est ajouté à une stratégie, il ne devient actif qu'après le redémarrage du noeud d'extrémité. Ce paramètre force le redémarrage requis en affichant un compte à rebours qui avertit l'utilisateur que la machine redémarrera dans le nombre de secondes spécifié. L'utilisateur dispose de ce laps de temps pour enregistrer son travail avant le redémarrage de sa machine.

  Vous devez redémarrer lors de la première activation du codage dans une stratégie et aussi lors de l'activation du codage « Safe Harbor » ou des périphériques de stockage amovibles (si leur activation est indépendante de celle du codage). Par exemple, lorsqu'une stratégie de codage est appliquée pour la première fois, deux redémarrages sont nécessaires : le premier pour initialiser les pilotes et le second pour placer les dossiers Safe Harbor dans un espace codé. Si d'autres dossiers Safe Harbor sont sélectionnés après l'application de la stratégie, un seul redémarrage suffit pour placer le dossier Safe Harbor dans la stratégie.

Mise à jour de ZSC

Des correctifs visant à corriger des anomalies mineures dans ZENworks Security Client sont disponibles avec les mises à jour régulières de ZENworks Endpoint Security Management. Plutôt que de fournir un nouveau programme d'installation, qui doit être distribué à tous les noeuds d'extrémité via MSI, la fonction de mise à jour de ZENworks Security Client permet à l'administrateur de consacrer une zone sur le réseau pour distribuer des correctifs de mise à jour aux utilisateurs finaux lorsque ces derniers rejoignent cet environnement réseau.

Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, puis cliquez sur*Mise à jour de ZSC* dans l'arborescence de stratégie à gauche.



Pour permettre une distribution simple et sécurisée de ces correctifs à tous les utilisateurs de ZENworks Security Client :

1. Cochez la case *Activer* pour activer l'écran et la règle.
2. Spécifiez l'emplacement où ZENworks Security Client doit rechercher les mises à jour.

   En raison des recommandations de l'étape suivante, l'emplacement associé à l'environnement de l'entreprise (par exemple, l'emplacement Travail) est conseillé.
3. Spécifiez l'indicateur URI où le correctif a été stocké.

   Il doit pointer vers le fichier du correctif, qui peut être le fichier setup.exe pour ZENworks Security Client ou un fichier MSI créé à partir du fichier .exe. Pour des raisons de sécurité, il est recommandé de stocker ces fichiers sur un serveur sécurisé derrière le pare-feu de l'entreprise.
4. Spécifiez les informations de version de ce fichier dans les champs prévus.

   Pour accéder à ces informations, installez ZENworks Security Client et ouvrez l'écran À propos de (consultez le*guide d'installation de ZENworks Security Client* pour plus d'informations). Le numéro de version du fichier `STEngine.exe` est celui que vous entrez dans les champs.

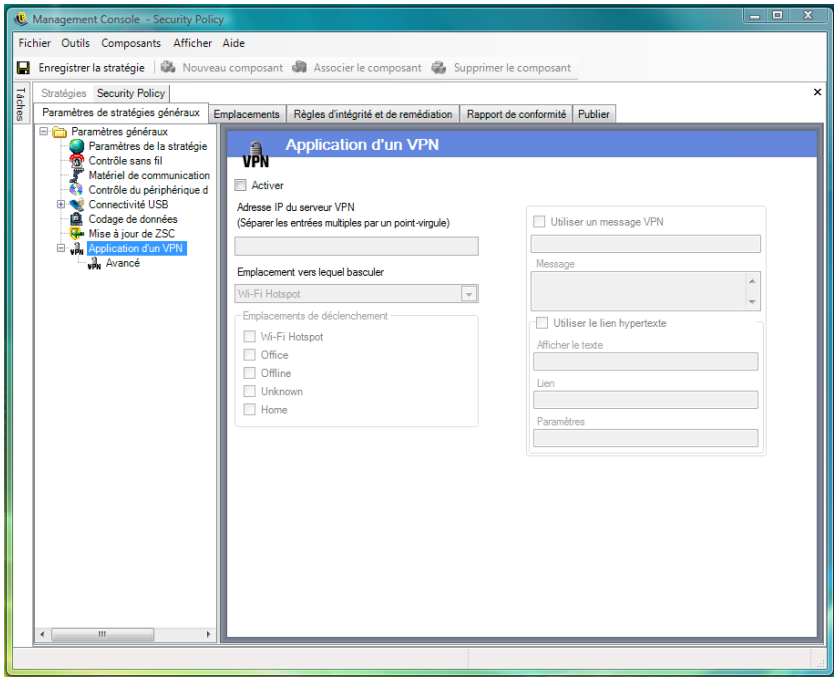
Chaque fois que l'utilisateur accède à l'emplacement attribué, ZENworks Security Client consulte l'identificateur URI pour rechercher une mise à jour correspondant à ce numéro de version. Si une mise à jour est disponible, ZENworks Security Client la télécharge et l'installe.

Application d'un VPN

Cette règle impose l'utilisation d'un réseau privé virtuel (VPN) SSL ou client. Elle est généralement appliquée dans des zones réactives sans fil et permet à l'utilisateur de se connecter au réseau public, auquel cas elle tente d'établir la connexion VPN, puis fait basculer l'utilisateur vers une configuration de pare-feu et d'emplacement définie. Tous les paramètres sont laissés à la discrétion de l'administrateur. Ils ont tous la priorité sur les paramètres de stratégie existants. Avant son lancement, le composant Application d'un VPN nécessite la connexion de l'utilisateur à un réseau.

Remarque : Cette fonction est uniquement disponible dans l'installation de ZENworks Endpoint Security Management et ne peut pas être utilisée pour les stratégies de sécurité UWS.

Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, puis cliquez sur*Application d'un VPN* dans l'arborescence de stratégie à gauche.



Pour pouvoir utiliser la règle d'application d'un VPN, il doit exister au moins deux emplacements.

Pour ajouter l'application d'un VPN à une stratégie de sécurité nouvelle ou existante :

1. Cochez la case *Activer* pour activer l'écran et la règle.
2. Spécifiez les adresses IP du serveur VPN dans le champ prévu. Si vous entrez plusieurs adresses, séparez-les par un point virgule (par exemple, 10.64.123.5;66.744.82.36).
3. Sélectionnez l'*emplacement vers lequel basculer* dans la liste déroulante.

   Il s'agit de l'emplacement vers lequel ZENworks Security Client bascule lorsque le VPN est activé. Il est recommandé que cet emplacement contienne des restrictions ainsi qu'une seule configuration de pare-feu restrictive comme valeur par défaut.

   Le paramètre de pare-feu *Tous - Fermé*, qui ferme tous les ports TCP/UDP, est conseillé pour l'application stricte d'un VPN. Ce paramètre empêche toute réseautique non autorisée, tandis que l'adresse IP du VPN fait office de liste de contrôle d'accès au serveur VPN et autorise la connectivité réseau.
4. Sélectionnez les emplacements de déclenchement dans lesquels la règle d'application d'un VPN est appliquée. Pour l'application stricte d'un VPN, il est recommandé d'utiliser l'emplacement Inconnu par défaut pour cette stratégie. Après l'authentification par le réseau, la règle VPN est activée et bascule vers l'emplacement attribué.

Remarque : Le changement d'emplacement se produit avant la connexion du VPN, dès que le réseau a procédé à l'authentification.

5 Entrez un message utilisateur personnalisé qui s'affichera une fois le VPN authentifié auprès du réseau. Pour un VPN non-client, cette opération devrait être suffisante.

Pour un VPN avec un client, prévoyez un lien hypertexte qui pointe vers le client VPN.

Exemple : `C:\Program Files\Cisco Systems\VPN Client\ipsecdialer.exe`

Ce lien lance l'application, mais l'utilisateur doit toujours se loguer. Vous pouvez entrer un paramètre dans le champ *Paramètres* ou créer un fichier de traitement par lots et pointer vers ce dernier, plutôt que vers l'exécutable du client.

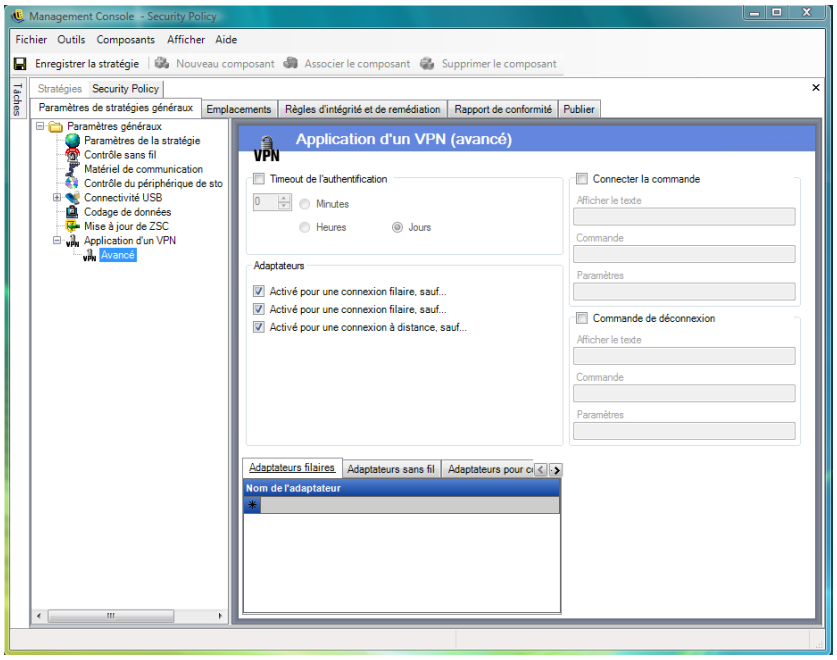
Remarque : Les clients VPN qui génèrent des adaptateurs virtuels (par ex., Cisco Systems* VPN Client 4.0) affichent le message suivant : `La stratégie a été mise à jour.` La stratégie n'a pas été mise à jour pour autant, ZENworks Security Client compare simplement l'adaptateur virtuel aux éventuelles restrictions figurant dans la stratégie actuelle.

Les paramètres d'application standard d'un VPN décrits ci-dessus rendent la connectivité VPN facultative. Les utilisateurs se voient accorder une connectivité au réseau actuel, qu'il lance ou non son VPN. Pour une application plus stricte, reportez-vous à la rubrique Paramètres VPN avancés.

Paramètres VPN avancés

Les contrôles VPN avancés permettent de définir des timeouts d'authentification pour protéger le VPN contre un échec, des commandes de connexion pour des VPN avec client et des contrôles d'adaptateur pour contrôler les adaptateurs autorisés à accéder au VPN.

Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, cliquez sur le signe « + » en regard de l'option *Application d'un VPN*, puis cliquez sur *Avancé* dans l'arborescence de stratégie sur la gauche.



Les paramètres d'application d'un VPN avancés suivants peuvent être configurés :

Timeout d'authentification : les administrateurs peuvent placer le noeud d'extrémité dans une configuration de pare-feu sécurisée (paramètre de pare-feu de l'*emplacement vers lequel basculer*) pour le protéger contre tout échec de la connectivité VPN. Le *timeout d'authentification* correspond au délai d'attente de ZENworks Security Client avant d'obtenir une authentification auprès du serveur VPN. Il est recommandé que la valeur de ce paramètre soit supérieure à 1 minute pour permettre l'authentification sur des connexions plus lentes.

Commandes de connexion/déconnexion : si vous utilisez le timeout d'authentification, les commandes de *connexion* et de *déconnexion* permettent de contrôler l'activation d'un VPN avec client. Spécifiez l'emplacement du client VPN ainsi que les paramètres requis dans les champs *Paramètres*. La commande de déconnexion est facultative et destinée aux clients VPN qui exigent la déconnexion de l'utilisateur avant de se déloguer du réseau.

Remarque : Les clients VPN qui génèrent des adaptateurs virtuels (par ex, Cisco Systems VPN Client 4.0) afficheront le message suivant : `La stratégie a été mise à jour` et peuvent s'écarter temporairement de l'emplacement actuel. La stratégie n'a pas été mise à jour pour autant, ZENworks Security Client compare simplement l'adaptateur virtuel aux éventuelles restrictions figurant dans la stratégie actuelle. Lors de l'exécution de clients VPN de ce type, il est recommandé de ne pas utiliser le lient hypertexte la Commande de déconnexion.

Adaptateurs : il s'agit principalement d'une mini stratégie d'adaptateur spécifique à l'application d'un VPN.

Si un adaptateur est sélectionné (son état devient Activés, sauf), tous les adaptateurs de ce type (le type « sans fil » étant spécifique à un type de carte) sont autorisés à se connecter au VPN,

sauf ceux figurant dans la liste d'exceptions dans la partie inférieure de la fenêtre.

Si un adaptateur n'est pas sélectionné (Désactivés, sauf), seuls les adaptateurs figurant dans la liste d'exceptions sont autorisés à se connecter au VPN. La connectivité de tous les autres est refusée.

Ce contrôle peut être utilisé pour des adaptateurs non compatibles avec le VPN, par exemple, ou non pris en charge par votre service informatique.

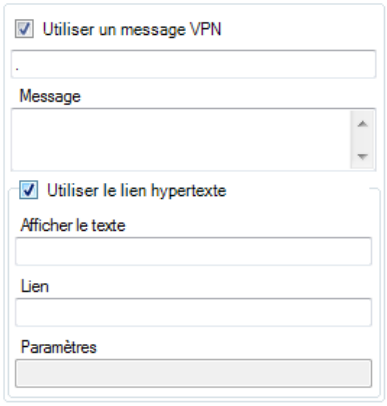
Cette règle a la priorité sur la stratégie d'adaptateur définie pour l'emplacement vers lequel basculer.

Message utilisateur personnalisé

Les messages utilisateur personnalisés permettent à l'administrateur de ZENworks Endpoint Security Management de créer des messages qui répondent directement aux questions de stratégie de sécurité lorsque l'utilisateur est confronté à des restrictions de sécurité appliquées par la stratégie. Ces messages peuvent également fournir des instructions spécifiques à l'utilisateur. Les contrôles des messages utilisateur sont disponibles dans divers composants de la stratégie.

Pour créer un message utilisateur personnalisé :

1. Spécifiez un titre pour le message. Celui-ci s'affiche dans la barre de titre de la zone de message.
2. Spécifiez le message. Le message est limité à 1 000 caractères.
3. Si un lien hypertexte est requis, cochez la case*Afficher les liens hypertexte* et spécifiez les informations nécessaires.



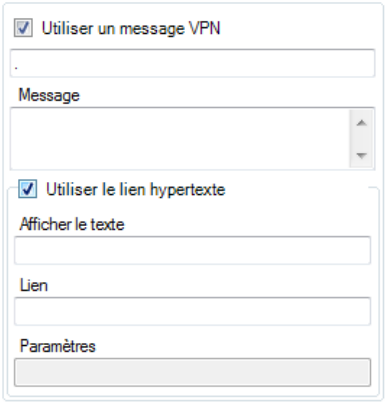
Remarque : Si vous changez le message ou le lien hypertexte d'un composant partagé, il sera également modifié dans toutes les autres instances de ce composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

Liens hypertexte

Un administrateur peut insérer des liens hypertexte dans des messages personnalisés pour expliquer des stratégies de sécurité ou fournir des liens vers des mises à jour logicielles afin de maintenir la conformité en termes d'intégrité. Des liens hypertexte sont disponibles dans plusieurs composants de stratégie. Vous pouvez créer un lien hypertexte VPN qui peut pointer vers l'exécutable du client VPN ou vers un fichier de traitement par lots qui s'exécute et logue complètement l'utilisateur au VPN (reportez-vous à la rubrique « Application d'un VPN » page 67 pour plus de détails).

Pour créer un lien hypertexte :

1. Spécifiez le nom du lien. Il s'agit du nom qui s'affiche au-dessous du message. Ce nom est également requis pour les liens hypertexte VPN avancés.
2. Spécifiez le lien hypertexte.
3. Spécifiez d'éventuels paramètres pour le lien.

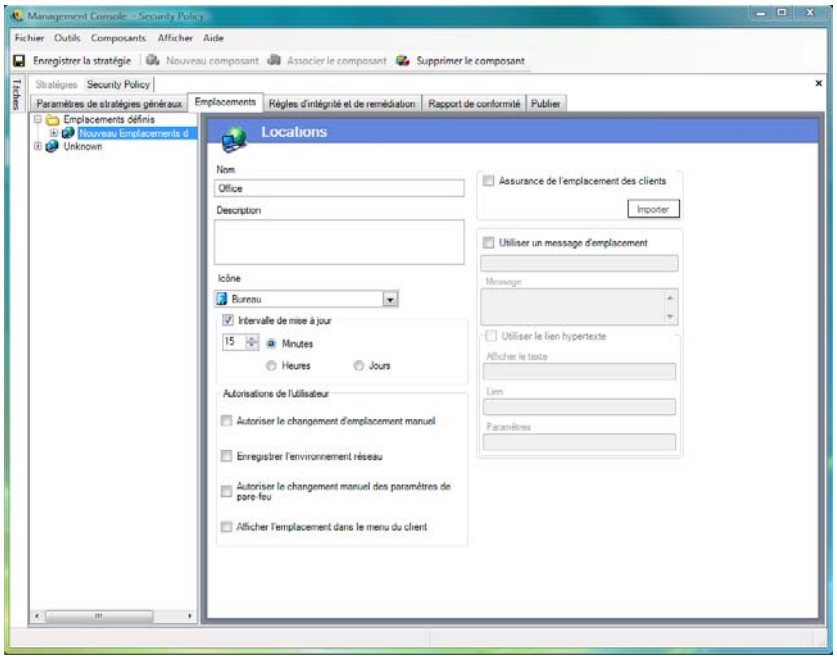


Remarque : Si vous changez le message ou le lien hypertexte d'un composant partagé, il sera également modifié dans toutes les autres instances de ce composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

2.2.2 Emplacements

Les emplacements sont des groupes de règles attribués à des environnements réseau. Ces environnements peuvent être définis dans la stratégie (reportez-vous à la rubrique « Environnements réseau » page 90) ou par l'utilisateur lorsque celui-ci y est autorisé. Chaque emplacement peut se voir accorder des paramètres de sécurité uniques qui lui interdisent l'accès à certains types de réseautique ou de matériel dans des environnements réseau plus hostiles et lui octroient un accès plus large au sein d'environnements approuvés.

Pour accéder aux contrôles d'emplacement, cliquez sur l'onglet *Emplacements*.



Les sections suivantes contiennent davantage d'informations :

- « À propos des emplacements » page 73
- « Matériel de communication » page 75
- « Contrôle des périphériques de stockage » page 77
- « Paramètres de pare-feu » page 79
- « Environnements réseau » page 90
- « Connectivité USB » page 92
- « Gestion Wi-Fi » page 93
- « Sécurité Wi-Fi » page 97

À propos des emplacements

Les types d'emplacement suivants peuvent être configurés :

Emplacement Inconnu : Toutes les stratégies ont un emplacement Inconnu par défaut. Il s'agit de l'emplacement vers lequel ZENworks Security Client fait basculer les utilisateurs lorsque ceux-ci quittent un environnement réseau connu. Cet emplacement Inconnu est spécifique à chaque stratégie et n'est pas disponible comme composant partagé. Aucun environnement réseau ne peut être défini ou enregistré pour cet emplacement.

Pour accéder aux contrôles de l'emplacement Inconnu, cliquez sur l'onglet *Emplacements*, puis cliquez sur l'emplacement *Inconnu* dans l'arborescence de stratégie à gauche.

Emplacements définis : Il est possible de créer des emplacements définis pour la stratégie ou d'associer des emplacements existants (créés pour d'autres stratégies).

Pour créer un emplacement :

1. Cliquez sur *Emplacements définis*, puis cliquez sur le bouton *Nouveau composant* dans la barre d'outils.
2. Entrez un nom et une description pour l'emplacement.
3. Définissez les paramètres d'emplacement :

   Icône : sélectionnez une icône d'emplacement pour fournir à l'utilisateur une indication visuelle lui permettant d'identifier l'emplacement actuel. L'icône d'emplacement s'affiche sur la barre des tâches dans la zone de notification. Utilisez la liste déroulante pour afficher et opérer une sélection parmi les icônes d'emplacement disponibles.

   Intervalle de mise à jour : ce paramètre détermine la fréquence à laquelle ZENworks Security Client recherche une mise à jour des stratégies lorsqu'il accède à cet emplacement. L'intervalle est défini en minutes, en heures ou en jours. Si ce paramètre n'est pas activé, ZENworks Security Client ne recherche pas de mise à jour à cet emplacement.

   Autorisations utilisateur : spécifiez les autorisations utilisateur :

   - **Autoriser le changement d'emplacement manuel :** permet à l'utilisateur de basculer de/vers cet emplacement. Pour des emplacements non gérés (zones réactives, aéroports, hôtels, etc.), cette autorisation doit être accordée. Dans les environnements contrôlés, où les paramètres réseau sont connus, elle peut être désactivée. Si cette autorisation est désactivée, l'utilisateur ne peut pas basculer de/vers un emplacement ; ZENworks Security Client se base plutôt sur les paramètres de l'environnement réseau spécifié pour cet emplacement.
   - **Enregistrer l'environnement réseau :** permet à l'utilisateur d'enregistrer l'environnement réseau dans cet emplacement pour lui permettre de basculer automatiquement vers ce dernier à son retour. Ce paramètre est recommandé pour tous les emplacements vers lesquels l'utilisateur doit basculer. Il est possible d'enregistrer plusieurs environnements réseau pour un emplacement unique. Par exemple, si un emplacement défini comme "Aéroport" fait partie de la stratégie actuelle, chaque aéroport où l'utilisateur s'est rendu peut être enregistré comme environnement réseau pour cet emplacement. Ainsi, un utilisateur mobile peut retourner dans un environnement « Aéroport » enregistré et ZENworks Security Client bascule automatiquement vers cet emplacement et applique les paramètres de sécurité définis. Un utilisateur peut, évidemment, basculer vers un autre emplacement et ne pas enregistrer l'environnement.
   - **Autoriser la modification manuelle des paramètres de pare-feu :** permet à l'utilisateur de modifier les paramètres de pare-feu.
   - **Afficher l'emplacement dans le menu du client :** permet d'afficher l'emplacement dans le menu du client. Si ce paramètre n'est pas activé, l'emplacement ne s'affiche jamais.

   Assurance de l'emplacement des clients : étant donné qu'il est facile de falsifier les informations relatives à l'environnement réseau utilisées pour déterminer un emplacement, ce qui expose le noeud d'extrémité à une éventuelle intrusion, le service CLAS (Client Location Assurance Service) propose l'option de vérification cryptographique d'un emplacement. Ce service est uniquement fiable dans les environnements réseau qui sont totalement et exclusivement contrôlés par l'entreprise. Ce service est uniquement fiable dans les environnements réseau qui sont totalement et exclusivement contrôlés par l'entreprise.

ZENworks Security Client utilise un port fixe, configurable en entreprise pour envoyer une vérification d'identité au service CLAS. Ce dernier décode le paquet et répond à la vérification d'identité, en apportant la preuve qu'il possède la clé privée correspondant à la clé publique. L'icône de la barre des tâches comporte une coche qui indique que l'utilisateur se trouve dans l'emplacement approprié.

ZENworks Security Client ne peut pas basculer vers l'emplacement à moins qu'il ne détecte le serveur CLAS. Si le serveur CLAS n'est pas détecté, même si tous les autres paramètres réseau correspondent, ZENworks Security Client reste dans l'emplacement Inconnu pour sécuriser le noeud d'extrémité.

Pour activer la fonctionnalité CLAS pour un emplacement, cochez la case *Assurance de l'emplacement des clients*, cliquez sur *Importer*, puis recherchez et sélectionnez le fichier. Le mot Configuré s'affiche une fois la clé importée.

Cette option n'est pas disponible pour l'emplacement Inconnu.

Utiliser un message d'emplacement: permet d'afficher un message utilisateur personnalisé facultatif lorsque ZENworks Security Client bascule vers cet emplacement. Ce message peut fournir des instructions pour l'utilisateur final, des détails sur les restrictions de stratégies dans cet emplacement ou un lien hypertexte pour plus d'informations.

4 Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Pour associer un emplacement existant :

1 Cliquez sur *Emplacements définis*, puis cliquez sur le bouton *Associer le composant* dans la barre d'outils.

2 Sélectionnez les emplacements souhaités dans la liste.

3 Au besoin, éditez les paramètres.

Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

---

4 Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Il est recommandé de définir dans la stratégie plusieurs emplacements définis (en plus des emplacements simples Travail et Inconnu) pour fournir aux utilisateurs différentes autorisations de sécurité lorsqu'ils se connectent à l'extérieur du pare-feu d'entreprise. Attribuez des noms simples aux emplacements (par exemple, Cafétérias, Aéroports, Domicile) et prévoyez une indication visuelle via l'icône de la barre des tâches de l'emplacement pour que les utilisateurs puissent facilement basculer vers les paramètres de sécurité appropriés pour chaque environnement réseau.

Matériel de communication

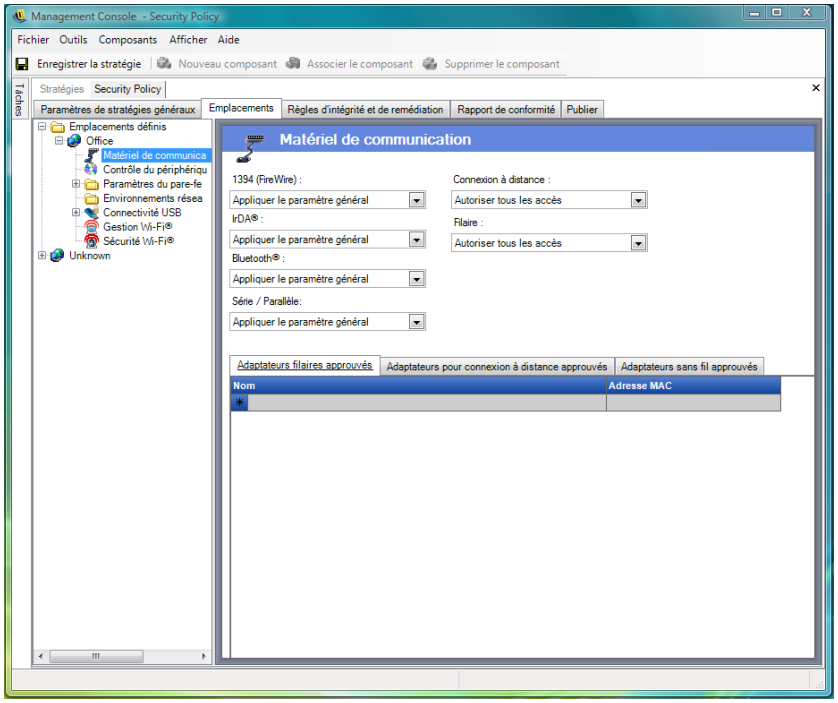
Les paramètres du matériel de communication contrôlent, par emplacement, les types de matériel qui sont autorisés à se connecter dans cet environnement réseau.

Remarque : Vous pouvez définir des contrôles du matériel de communication globalement sous l'onglet *Paramètres de stratégie généraux* ou pour des emplacements individuels sous l'onglet *Emplacements*.

Pour définir des contrôles du matériel de communication pour un emplacement, cliquez sur l'onglet *Emplacements*, développez l'emplacement souhaité dans l'arborescence, puis cliquez sur *Matériel de communication*.

ou

Pour définir des contrôles du matériel de communication de manière globale, cliquez sur l'onglet *Paramètres de stratégie généraux*, développez les *Paramètres généraux* dans l'arborescence, puis cliquez sur *Matériel de communication*. Pour plus d'informations, reportez-vous à « Matériel de communication » page 53.



Choisissez d'activer, de désactiver ou d'appliquer le paramètre général pour chaque périphérique de communication listé :

- **1394 (FireWire) :** contrôle le port d'accès FireWire* sur le noeud d'extrémité.
- **IrDA :** contrôle le port d'accès infrarouge sur le noeud d'extrémité.
- **Bluetooth :** contrôle le port d'accès Bluetooth* sur le noeud d'extrémité.
- **Série / Parallèle :** contrôle l'accès au ports série et parallèle sur le noeud d'extrémité.
- **Connexion à distance :** contrôle la connectivité modem par emplacement. Cette option n'est pas disponible lorsque vous configurez les paramètres du matériel de communication de manière globale, via l'onglet *Paramètres de stratégie généraux*.
- **Filaire :** contrôle la connectivité de la carte LAN par emplacement. Cette option n'est pas disponible lorsque vous configurez les paramètres du matériel de communication de manière globale, via l'onglet *Paramètres de stratégie généraux*.

L'activation permet l'accès complet au port de communication.

La désactivation refuse l'accès au port de communication.

Remarque : Les adaptateurs Wi-Fi sont soit contrôlés globalement soit désactivés localement à l'aide des contrôles de sécurité Wi-Fi. Les adaptateurs peuvent être spécifiés par marque à l'aide de la liste des adaptateurs sans fil approuvés.

Liste des adaptateurs pour connexion à distance approuvés : ZENworks Security Client peut bloquer la connexion de tous les adaptateurs pour connexion à distance (modems) approuvés, sauf de ceux spécifiés. Par exemple, un administrateur peut implémenter une stratégie qui autorise uniquement une marque ou un type spécifique de carte modem. Cela réduit les coûts associés à l'utilisation par le personnel du matériel non pris en charge.

Liste des adaptateurs sans fil approuvés : ZENworks Security Client peut bloquer la connexion de tous les adaptateurs sans fil approuvés, sauf de ceux spécifiés. Par exemple, un administrateur peut implémenter une stratégie qui autorise uniquement une marque ou un type spécifique de carte sans fil. Cela réduit les coûts d'assistance associés à l'utilisation par le personnel du matériel non pris en charge, et améliore la prise en charge et l'application d'initiatives de sécurité basées sur les standards de l'IEEE, ainsi que des normes LEAP, PEAP, WPA, TKIP, etc.

Utilisation de la fonction AdapterAware :

ZENworks Security Client est informé lors de l'installation d'un périphérique réseau dans le système et détermine si ce périphérique est autorisé. ZENworks Security Client est informé lors de l'installation d'un périphérique réseau dans le système et détermine si ce périphérique est autorisé.

Remarque : Lorsqu'un nouvel adaptateur non autorisé (pour connexion à distance et sans fil) installe pour la première fois ses pilotes sur le noeud d'extrémité (via PCMCIA ou USB), il s'affiche comme activé dans le gestionnaire de périphériques de Windows jusqu'au redémarrage du système, même si la connectivité réseau est totalement bloquée.

Spécifiez le nom de chaque adaptateur autorisé. Les noms partiels d'adaptateur sont autorisés. Les noms d'adaptateur sont limités à 50 caractères et respectent la casse. Le système d'exploitation Windows 2000 a besoin du nom de périphérique pour offrir cette fonctionnalité. Si vous n'entrez aucun adaptateur, tous les adaptateurs de ce type sont autorisés. Si un seul adaptateur est entré, seul cet adaptateur sera autorisé à cet emplacement.

Remarque : Si le noeud d'extrémité se trouve dans un emplacement qui utilise uniquement l'identificateur SSID d'un point d'accès comme identification réseau, ZENworks Security Client bascule vers cet emplacement avant de désactiver l'adaptateur non autorisé. Un mot de passe prioritaire doit être utilisé pour permettre dans ce cas de basculer manuellement vers un emplacement.

Contrôle des périphériques de stockage

Les contrôles des périphériques de stockage définissent les paramètres par défaut des périphériques de stockage de la stratégie, où tous les périphériques de stockage de fichiers externes sont autorisés à lire/écrire des fichiers, fonctionnent en mode lecture seule ou sont entièrement désactivés. Lorsqu'ils sont désactivés, ces périphériques sont incapables de récupérer des données provenant du noeud d'extrémité alors que le disque dur et toutes les unités réseau restent accessibles et opérationnelles.

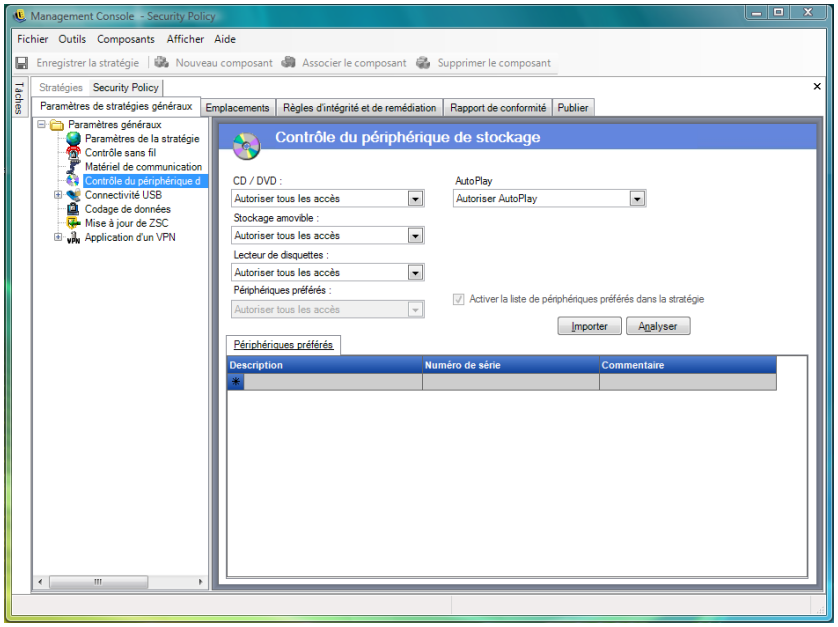
Le contrôle des périphériques de stockage de ZENworks Endpoint Security Management n'est pas autorisé si ZENworks Storage Encryption Solution est activé.

Remarque : Vous pouvez définir les contrôles des périphériques de stockage de manière globale sous l'onglet *Paramètres de stratégie généraux* ou pour des emplacements individuels sous l'onglet *Emplacements*.

Pour définir les contrôles des périphériques de stockage pour un emplacement, cliquez sur l'onglet *Emplacements*, développez l'emplacement souhaité dans l'arborescence, puis cliquez sur *Contrôle des périphériques de stockage*.

ou

Pour définir les contrôles des périphériques de stockage de manière globale, cliquez sur l'onglet *Paramètres de stratégie généraux*, développez les *Paramètres généraux* dans l'arborescence, puis cliquez sur *Contrôle des périphériques de stockage*. Pour plus d'informations, reportez-vous à « Contrôle des périphériques de stockage » page 54.



Le contrôle des périphériques de stockage est réparti dans les catégories suivantes :

- **CD/DVD :** contrôle tous les périphériques figurant dans la liste des *unités DVD/CD-ROM* dans le gestionnaire des périphériques de Windows.
- **Stockage amovible :** contrôle tous les périphériques de stockage amovibles listés sous *Unités de disque* dans le gestionnaire des périphériques de Windows.
- **Unité de disquette :** contrôle tous les périphériques listés sous *Unités de disquette* dans le gestionnaire des périphériques de Windows.

Les unités de stockage fixes (disques dur) et les unités réseau (lorsqu'elles sont disponibles) sont toujours autorisées.

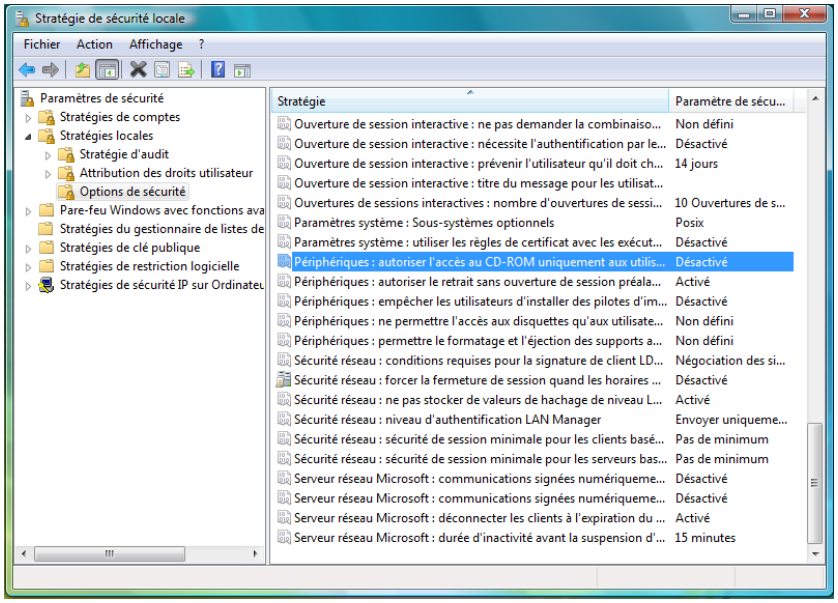
Pour définir les valeurs par défaut des périphériques de stockage de la stratégie, sélectionnez le paramètre général des deux types dans les listes déroulantes :

- **Activer:** ce type de périphérique est autorisé par défaut.

- **Désactiver :** ce type de périphérique n'est pas autorisé. Si des utilisateurs tentent d'accéder à des fichiers se trouvant sur un périphérique de stockage défini, ils reçoivent un message d'erreur du système d'exploitation ou de l'application qui tente d'accéder au périphérique de stockage local, les informant de l'échec de l'opération
- **Lecture seule :** ce type de périphérique est configuré pour un accès en lecture seule. Si des utilisateurs tentent d'écrire sur le périphérique, ils reçoivent un message d'erreur du système d'exploitation ou de l'application qui tente d'accéder au périphérique de stockage local, les informant de l'échec de l'opération

---

Remarque : Si vous souhaitez désactiver ou configurer en lecture seule des unités de CD-ROM ou de disquette sur un groupe de noeuds d'extrémité, les stratégies *Périphériques : limiter l'accès des CD-ROM à l'utilisateur logué localement uniquement* et *Périphériques : limiter l'accès des disquettes à l'utilisateur logué localement uniquement* dans les paramètres de sécurité locaux (transmis via un objet Stratégie de groupe du service Annuaire) doivent être définies sur Désactivé. Pour vérifier, ouvrez l'objet Stratégie de groupe ou les outils d'administration sur une machine. Vérifiez dans Paramètres de sécurité locaux - Options de sécurité que les deux périphériques sont désactivés. Désactivé est la valeur par défaut.



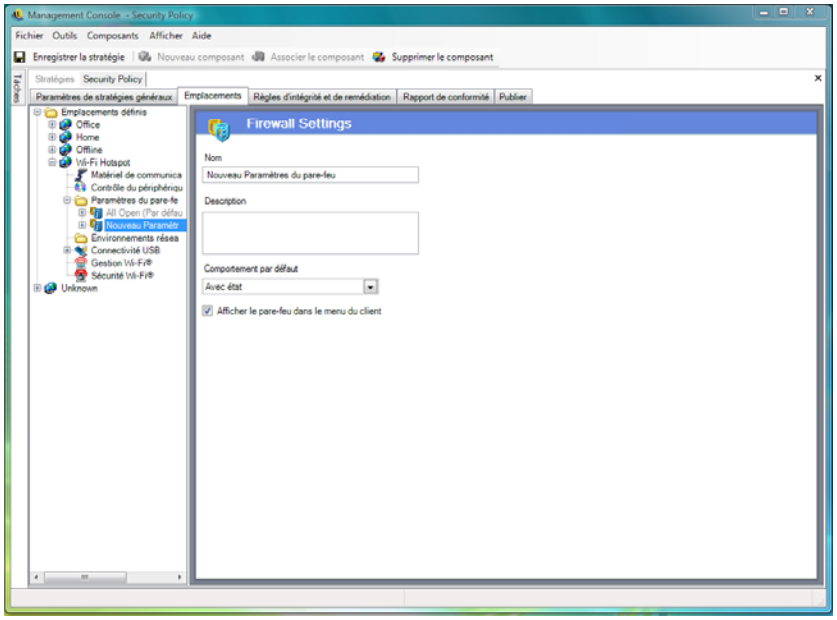
Paramètres de pare-feu

Les paramètres de pare-feu contrôlent la connectivité de tous les ports réseau, les listes de contrôle d'accès, les paquets réseau (ICMP, ARP, etc.) ainsi que les applications qui sont autorisées à obtenir une connexion sortante ou à fonctionner lorsque le paramètre de pare-feu est appliqué.

Remarque : Cette fonction est uniquement disponible dans l'installation de ZENworks Endpoint Security Management et ne peut pas être utilisée pour les stratégies de sécurité UWS.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, puis cliquez sur l'icône *Paramètres du pare-feu* dans l'arborescence de la stratégie à gauche.

Chaque composant d'un paramètre de pare-feu est configuré séparément et seul le comportement par défaut des ports TCP/UDP doit être défini. Lorsqu'il est activé, ce paramètre affecte tous les ports TCP/UDP. Les ports groupés ou individuels peuvent être créés avec un paramètre différent.



Pour créer un paramètre de pare-feu :

1. Sélectionnez *Paramètres du pare-feu* dans l'arborescence des composants, puis cliquez sur le bouton *Nouveau composant*.
2. Entrez un nom et une description pour le paramètre de pare-feu.
3. Cliquez avec le bouton droit *Ports TCP/UDP* dans l'arborescence des composants, puis cliquez sur *Ajouter de nouveaux ports TCP/UDP* pour sélectionner le comportement par défaut pour tous les ports TCP/UDP.

   Il est possible d'ajouter des ports et des listes supplémentaires aux paramètres de pare-feu et de leur attribuer des comportements uniques qui auront la priorité sur les paramètres par défaut.

   Par exemple, le comportement par défaut pour tous les ports est défini sur Tous - Avec état. Cela signifie que les listes des ports pour la diffusion multimédia en continu et la navigation Web sont ajoutées au paramètre de pare-feu. Le comportement du port de diffusion multimédia en continu est défini sur Fermé et celui du port de navigation Web sur Ouvert. Le trafic réseau via les ports TCP 7070, 554, 1755 et 8000 est bloqué. Le trafic réseau via les ports 80 et 443 est ouvert et visible sur le réseau. Tous les autres ports opèrent en mode Avec état, impliquant que le trafic par leur intermédiaire soit sollicité en premier.

   Pour plus d'informations, reportez-vous à « Ports TCP/UDP » page 81.
4. Cliquez avec le bouton droit sur *Listes de contrôle d'accès*, puis cliquez sur *Ajouter de nouvelles listes de contrôle d'accès* pour ajouter des adresses qui pourraient nécessiter que le trafic non sollicité soit autorisé, quel que soit le comportement de port actuel.

   Pour plus d'informations, reportez-vous à « Listes de contrôle d'accès » page 85.
5. Cliquez avec le bouton droit sur *Contrôle d'application*, puis cliquez sur *Ajouter de nouveaux contrôles d'application* pour empêcher l'accès des applications au réseau, voire leur exécution.

   Pour plus d'informations, reportez-vous à « Contrôles d'application » page 88.

6 Choisissez d'afficher éventuellement ce pare-feu dans le menu ZENworks Security Client (si cette option n'est pas sélectionnée, l'utilisateur ne voit pas ce paramètre de pare-feu).

7 Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Pour associer un paramètre de pare-feu existant :

1 Sélectionnez *Paramètres du pare-feu* dans l'arborescence des composants, puis cliquez sur le bouton *Associer le composant*.

2 Sélectionnez les paramètres de pare-feu souhaités dans la liste,

3 le cas échéant, modifiez le paramètre de comportement par défaut.

Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

---

4 Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Plusieurs paramètres de pare-feu peuvent être inclus dans un seul emplacement. L'un est défini comme paramètre par défaut et les autres sont disponibles en tant qu'options pour l'utilisateur. Il peut s'avérer utile de disposer de plusieurs paramètres lorsqu'un utilisateur a normalement besoin de certaines restrictions de sécurité au sein d'un environnement réseau et qu'occasionnellement, elles doivent être levées ou renforcées pour une courte période, p. ex. pour des diffusions ICMP.

Les paramètres de pare-feu suivants sont inclus à l'installation :

- **Tous - Adaptatif :** définit tous les ports réseau comme Avec état (tout le trafic réseau entrant non sollicité est bloqué. Tout le trafic réseau sortant est autorisé), les paquets ARP et 802.1x sont autorisés et toutes les applications réseau sont autorisées à se connecter au réseau.
- **Tous - Ouvert :** définit tous les ports réseau comme ouverts (tout le trafic réseau est autorisé) et tous les types de paquets sont autorisés. définit tous les ports réseau comme ouverts (tout le trafic réseau est autorisé) et tous les types de paquets sont autorisés.
- **Tous - Fermé :** ferme tous les ports réseau et limite tous les types de paquets.

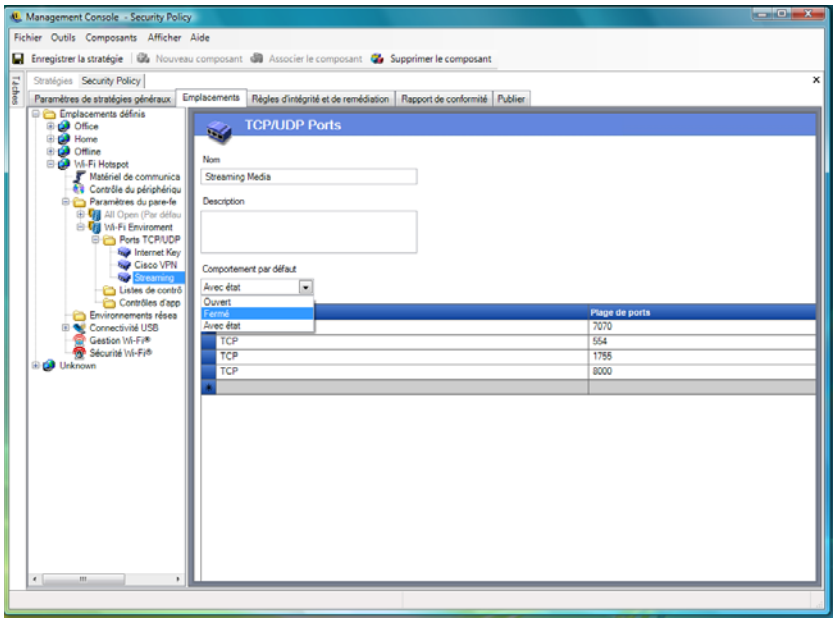
Pour un nouvel emplacement, le paramètre de pare-feu unique par défaut est Tous - Ouvert. Pour définir un autre paramètre de pare-feu, cliquez avec le bouton droit de la souris sur le paramètre de pare-feu souhaité, puis sélectionnez *Définir comme valeur par défaut*.

Ports TCP/UDP

Les données du noeud d'extrémité sont essentiellement sécurisées par le contrôle de l'activité des ports TCP/UDP. Cette fonctionnalité permet de créer une liste de ports TCP/UDP qui sont gérés de manière unique dans ce paramètre de pare-feu. Cette liste contient un ensemble de ports et de plages de ports, ainsi que leur type de transport qui définit la fonction de la plage.

Remarque : Cette fonction est uniquement disponible dans l'installation de ZENworks Endpoint Security Management et ne peut pas être utilisée pour les stratégies de sécurité UWS.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, cliquez sur le signe + en regard de *Paramètres du pare-feu*, cliquez sur le signe « + » en regard du pare-feu souhaité, puis cliquez sur l'icône *Ports TCP/UDP* dans l'arborescence de stratégie à gauche.



Il est possible de définir de nouvelles listes de ports TCP/UDP avec des ports individuels ou en tant que plage (1-100) pour chaque ligne de la liste.

Pour créer un paramètre de port TCP/UDP :

1. Cliquez avec le bouton droit sur *Ports TCP/UDP* dans l'arborescence des composants, puis cliquez sur *Ajouter de nouveaux ports TCP/UDP*.
2. Entrez un nom et une description pour la liste des ports.
3. Sélectionnez le comportement du port dans la liste déroulante :
   - **Ouvert :** tout le trafic réseau entrant et sortant est autorisé. Étant donné que tout le trafic réseau est autorisé, l'identité de votre ordinateur est visible pour ce port ou cette plage de ports.
   - **Fermé :** tout le trafic réseau entrant et sortant est bloqué. Étant donné que toutes les requêtes d'identification réseau sont bloquées, l'identité de votre ordinateur est dissimulée pour ce port ou cette plage de ports.
   - **Avec état :** tout le trafic réseau entrant non sollicité est bloqué. Tout le trafic réseau sortant est autorisé sur ce port ou cette plage de ports.
4. Spécifiez le type de transport en cliquant sur la flèche vers le bas dans la colonne *Type de port*.
   - TCP/UDP
   - Ether
   - IP
   - TCP
   - UDP
5. Entrez les ports et plages de ports, de l'une des manières suivantes :
   - Ports uniques
   - Plage de ports, avec le premier numéro de port suivi d'un tiret, puis le dernier numéro de port

Par exemple, 1-100 ajoute tous les ports entre 1 et 100

Visitez les pages IANA (Internet Assigned Numbers Authority (http://www.iana.org)) pour une liste complète des ports et types de transport.

6 Cliquez sur *Enregistrer la stratégie*.

Pour associer un port TCP/UDP existant à ce paramètre de pare-feu :

1 Sélectionnez *Ports TCP/UDP* dans l'arborescence des composants, puis cliquez sur le bouton *Associer le composant*.

2 Sélectionnez les ports souhaitées dans la liste.

3 Configurer les paramètres de comportement par défaut.

La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

4 Cliquez sur *Enregistrer la stratégie*.

Plusieurs groupes de ports TCP/UDP ont été associés et sont disponibles à l'installation :

Nom	Description	Transport	Valeur
Tous les ports	Tous les ports	Tous	1-65535
Blue Ridge VPN	Ports utilisés par le client Blue Ridge VPN	UDP	820
Cisco VPN	Ports utilisés par le client Cisco* VPN	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524
Réseautique courante	Ports réseau généralement requis pour la conception de pare-feux	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847

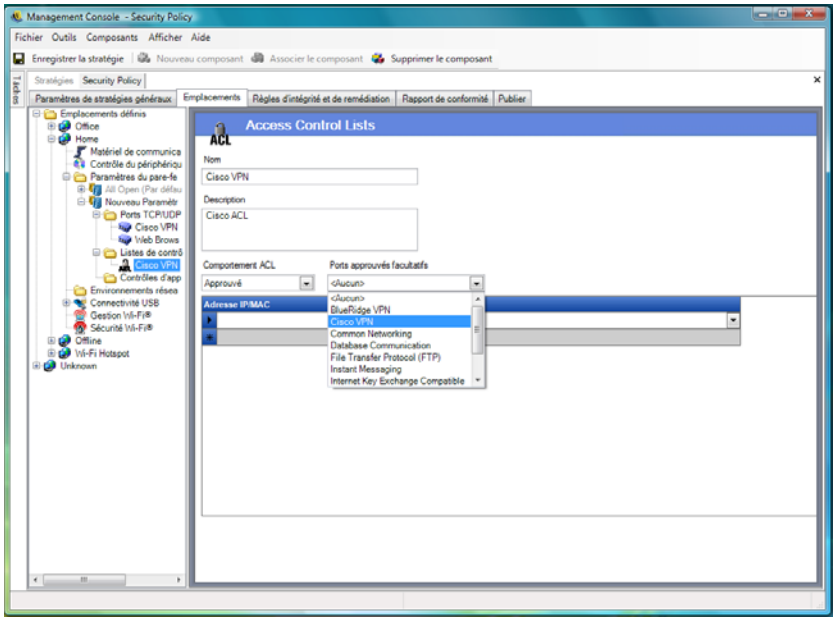
Nom	Description	Transport	Valeur
Communication de base de données	Ports de base de données Microsoft*, Oracle*, Siebel*, Sybase*, SAP*	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
Protocole FTP (File Transfer Protocol)	Port FTP	TCP/UDP	21
Messagerie instantanée	Ports de messagerie instantanée Microsoft, AOL* et Yahoo*	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
VPN compatible IKE (Internet Key Exchange)	Ports utilisés par les clients du VPN compatible IKE	UDP	500
Réseautique Microsoft	Ports Partage de fichiers communs / Active Directory*	TCP/UDP	135-139, 445
Ports ouverts	Ports ouverts pour ce pare-feu	TCP/UDP	80
Diffusion multimédia en continu	Ports Microsoft et de diffusion multimédia en continu communs	TCP	7070, 554, 1755, 8000
Navigation Web	Ports de navigation Web communs, y compris SSL	Tous	80, 443

Listes de contrôle d'accès

Certaines adresses nécessitent que le trafic non sollicité soit autorisé, quel que soit le comportement de port actuel (par exemple, le serveur de sauvegarde d'entreprise, serveur Exchange, etc.). Lorsque le trafic non sollicité doit être autorisé vers et à partir des serveurs approuvés, une liste de contrôle d'accès résout ce problème.

Remarque : Cette fonction est uniquement disponible dans l'installation de ZENworks Endpoint Security Management et ne peut pas être utilisée pour les stratégies de sécurité UWS.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, cliquez sur le signe + en regard de *Paramètres de pare-feu*, cliquez sur le signe « + » en regard du pare-feu souhaité, cliquez avec le bouton droit sur *Listes de contrôle d'accès* dans l'arborescence de stratégie à gauche, puis cliquez sur *Ajouter de nouvelles listes de contrôle d'accès*.



Pour créer un paramètre de liste de contrôle d'accès :

1. Cliquez avec le bouton droit sur *Listes de contrôle d'accès* dans l'arborescence des composants, puis cliquez sur *Ajouter de nouvelles listes de contrôle d'accès*.
2. Entrez un nom et une description pour la liste de contrôle d'accès.
3. Spécifiez la macro ou l'adresse de la liste de contrôle d'accès.
4. Spécifiez le type de liste de contrôle d'accès :
   - **IP :** l'adresse est limitée à 15 caractères et ne doit contenir que les chiffres de 0 à 9 et des points, par exemple 123.45.6.189. Les adresses IP peuvent également être entrées sous la forme d'une plage, par exemple 123.0.0.0 - 123.0.0.255.
   - **MAC :** l'adresse est limitée à 12 caractères et ne doit contenir que les chiffres de 0 à 9 et les lettres de A à F (majuscules et minuscules), séparés par des deux-points (exemple : 00:01:02:34:05:B6).

5. Sélectionnez la liste déroulante Comportement des listes de contrôle d'accès et déterminez si les listes de contrôle d'accès répertoriées doivent avoir le comportement *Approuvé* (toujours l'autoriser même si tous les ports TCP/UDP sont fermés) ou *Non approuvé* (bloquer l'accès).
6. Si le comportement est *Approuvé*, sélectionnez les *Ports approuvés facultatifs (TCP/UDP) que cette liste de contrôle utilisera*. Ces ports autorisent l'ensemble du trafic des listes de contrôle d'accès, tandis que les autres ports TCP/UDP conservent leurs paramètres actuels. Cliquez sur *Aucun* pour que cette liste de contrôle d'accès puisse utiliser n'importe quel port.
7. Cliquez sur *Enregistrer la stratégie*.

Pour associer une macro ou une liste de contrôle d'accès existante à ce paramètre de pare-feu :

1. Sélectionnez *Liste de contrôle d'accès* dans l'arborescence des composants, puis cliquez sur le bouton *Associer le composant*.
2. Sélectionnez les macros ou les listes de contrôle d'accès dans la liste.
3. Configurez, au besoin, les paramètres de comportement des listes de contrôle d'accès.

   Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.
4. Cliquez sur *Enregistrer la stratégie*.

Liste des macros d'adresse réseau

Voici une liste de macros de contrôle d'accès spéciales. Elles peuvent être individuellement associées dans le cadre d'une liste de contrôle d'accès dans un paramètre de pare-feu.

Tableau 2-1 *Macros d'adresse réseau*

Macro	Description
[Arp]	Autorise les paquets ARP (Address Resolution Protocol). La *résolution d'adresse* fait référence au processus de recherche d'une adresse d'un ordinateur dans un réseau. L'adresse est résolue à l'aide d'un protocole dans lequel une information est envoyée par un processus client s'exécutant sur l'ordinateur local à un processus serveur s'exécutant sur un ordinateur distant. L'information reçue par le serveur lui permet d'identifier de manière unique le système réseau pour lequel l'adresse était requise pour fournir l'adresse nécessaire. La procédure de résolution d'adresse est terminée lorsque le client reçoit une réponse du serveur contenant l'adresse nécessaire.
[Icmp]	Autorise les paquets ICMP (Internet Control Message Protocol). Les paquets ICMP sont utilisés par les routeurs, les périphériques intermédiaires ou les hôtes pour communiquer les mises à jour ou les informations sur les erreurs aux autres routeurs, périphériques intermédiaires ou hôtes. Les messages ICMP sont envoyés à diverses occasions, par exemple lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque la passerelle ne dispose pas de la capacité de mise en mémoire tampon pour transférer un datagramme et lorsque la passerelle peut indiquer à l'hôte d'envoyer le trafic sur une route plus courte.

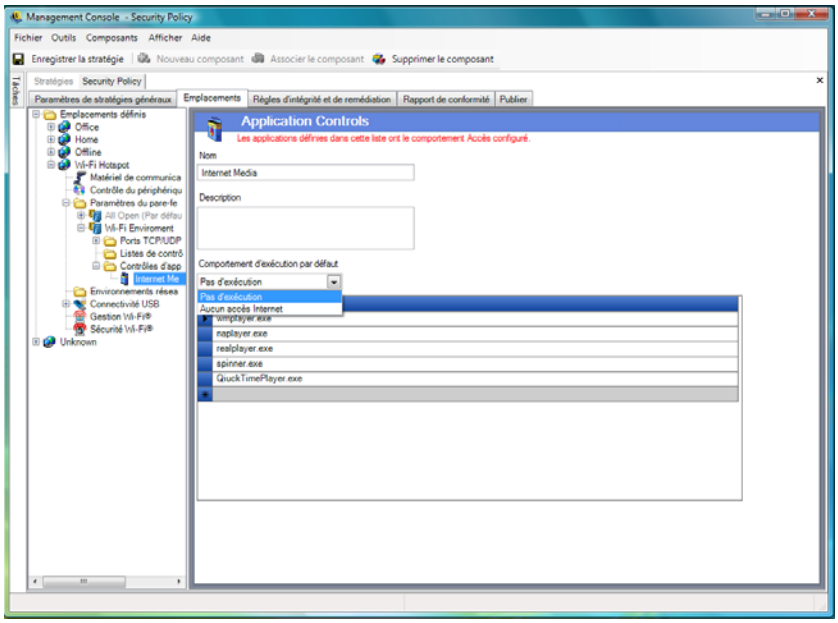
Macro	Description
[IpMulticast]	Autorise les paquets de multidiffusion IP. La multidiffusion est une technologie de conservation de bande passante qui réduit le trafic en fournissant simultanément un flux unique d'informations à des milliers d'utilisateurs privés et destinataires professionnels. Parmi les applications qui tirent profit de la multidiffusion, citons la vidéoconférence, les communications d'entreprise, l'enseignement à distance et la diffusion de logiciels, de cotations boursières et d'actualités. Les paquets de multidiffusion peuvent être distribués à l'aide des adresses IP ou Ethernet.
[EthernetMulticast]	Autorise les paquets de multidiffusion Ethernet.
[IpSubnetBrdcast]	Autorise les paquets de diffusion de sous-réseau. Les diffusions de sous-réseau sont utilisées pour envoyer des paquets à tous les hôtes d'un sous-réseau, d'un super-réseau ou d'un réseau sans classe. Tous les hôtes d'un réseau sans classe écoutent et traitent les paquets adressés à l'adresse de diffusion de sous-réseau.
[Snap]	Autorise les paquets codés au format SNAP.
[LLC]	Autorise les paquets codés au format LLC.
[Allow8021X]	Autorise les paquets 802.1x. Pour parer aux défaillances de clés WEP (Wired Equivalent Privacy), Microsoft et d'autres sociétés utilisent 802.1x comme méthode d'authentification alternative. 802.1x est un contrôle d'accès réseau basé sur un port, qui utilise le protocole EAP (Extensible Authentication Protocol) ou des certificats. À l'heure actuelle, les principaux fournisseurs de cartes sans fil et de nombreux fournisseurs de points d'accès prennent en charge la norme 802.1x. Ce paramètre permet également d'autoriser les paquets d'authentification LEAP (Light Extensible Authentication Protocol) et WPA (WiFi Protected Access).
[Gateway]	Représente l'adresse de la passerelle par défaut de la configuration IP actuelle. Une fois que cette valeur est entrée, ZENworks Security Client autorise tout le trafic réseau au départ de la passerelle par défaut de la configuration IP actuelle comme une liste ACL approuvée.
[GatewayAll]	Fonctionne comme [Gateway], mais pour toutes les passerelles définies.
[Wins]	Représente l'adresse du serveur WINS par défaut de la configuration IP client actuelle. Une fois que cette valeur est entrée, ZENworks Security Client autorise tout le trafic réseau au départ du serveur WINS par défaut de la configuration IP actuelle comme une liste ACL approuvée.
[WinsAll]	Fonctionne comme [Wins], mais pour tous les serveurs WINS définis.
[Dns]	Représente l'adresse du serveur DNS par défaut de la configuration IP client actuelle. Une fois que cette valeur est entrée, ZENworks Security Client autorise tout le trafic réseau au départ du serveur DNS par défaut de la configuration IP actuelle comme une liste ACL approuvée.
[DnsAll]	Fonctionne comme [Dns], mais pour tous les serveurs DNS définis.
[Dhcp]	Représente l'adresse du serveur DHCP par défaut de la configuration IP client actuelle. Une fois que cette valeur est entrée, ZENworks Security Client autorise tout le trafic réseau au départ du serveur DHCP par défaut de la configuration IP actuelle comme une liste ACL approuvée.
[DhcpAll]	Fonctionne comme [Dhcp], mais pour tous les serveurs DHCP définis.

Contrôles d'application

Cette fonction permet à l'administrateur d'empêcher l'accès des applications au réseau, voire leur exécution.

Remarque : Cette fonction est uniquement disponible dans l'installation de ZENworks Endpoint Security Management et ne peut pas être utilisée pour les stratégies de sécurité UWS.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, cliquez sur le signe + en regard de *Paramètres du pare-feu*, cliquez sur le signe « + » en regard du pare-feu souhaité, puis cliquez sur l'icône *Contrôles d'application* dans l'arborescence de stratégie à gauche.



Pour créer un nouveau paramètre de contrôle d'application :

1. Cliquez avec le bouton droit sur *Contrôles d'application* dans l'arborescence des composants, puis cliquez sur *Ajouter de nouveaux contrôles d'application*.
2. Nommez la liste de contrôles d'application et décrivez-la.
3. Sélectionnez un comportement d'exécution. Ce comportement est appliqué à toutes les applications de la liste. Si plusieurs comportements sont requis (par exemple, certaines applications réseau ne sont pas autorisées à accéder au réseau, alors que toutes les applications de partage de fichiers ne sont pas autorisées à s'exécuter), plusieurs contrôles d'application doivent être définis. Sélectionnez l'un des paramètres suivants :
   - **Tous - Autorisé :** toutes les applications listées sont autorisées à s'exécuter et à accéder au réseau.
   - **Pas d'exécution :** toutes les applications listées ne sont pas autorisées à s'exécuter.
   - **Aucun accès réseau :** toutes les applications listées ne sont pas autorisées à accéder au réseau. L'accès au réseau est également refusé aux applications (telles que les navigateurs Web) lancées à partir d'une application.

Remarque : Le blocage de l'accès réseau d'une application n'affecte pas l'enregistrement de fichiers sur des unités réseau mappés. Les utilisateurs sont autorisés à effectuer des enregistrements sur toutes les unités réseau à leur disposition.

4 Spécifiez chaque application à bloquer. N'entrez qu'une application par ligne.

Important : Le blocage de l'exécution d'applications stratégiques pourrait nuire au fonctionnement du système. Les applications Microsoft Office bloquées tentent d'exécuter leur programme d'installation.

5 Cliquez sur *Enregistrer la stratégie*.

Pour associer une liste de contrôles d'application existante à ce paramètre de pare-feu :

1 Sélectionnez Contrôles d'application dans l'arborescence des composants, puis cliquez sur le bouton *Associer le composant*.

2 Sélectionnez un ensemble d'applications dans la liste.

3 Configurez, au besoin, les applications et le niveau de restriction.

Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

4 Cliquez sur *Enregistrer la stratégie*.

Les contrôles d'application disponibles sont identifiés ci-dessous ; le comportement d'exécution par défaut est Aucun accès réseau.

Tableau 2-2 *Contrôles d'application*

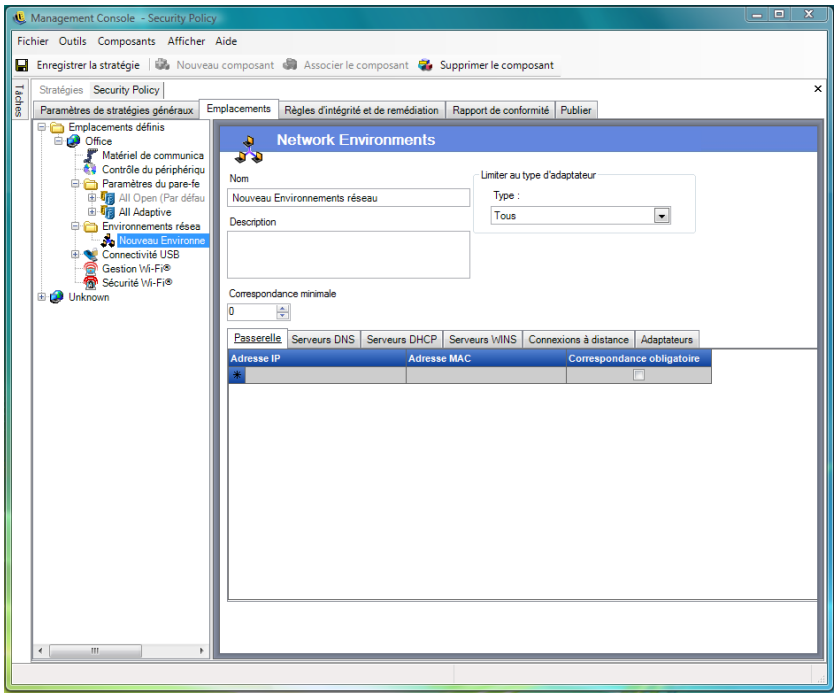
Nom	Applications
Navigateurs Web	explore.exe ; netscape.exe ; netscp.exe
Messagerie instantanée	aim.exe ; icq.exe ; msmsgs.exe ; msnmsgr.exe ; trillian.exe ; ypager.exe
Partage de fichiers	blubster.exe ; grokster.exe ; imesh.exe ; kazaa.exe ; morpheus.exe ; napster.exe ; winmx.exe
Média Internet	mplayer2.exe ; wmplayer.exe ; naplayer.exe ; realplay.exe ; spinner.exe ; QuickTimePlayer.exe

Si la même application est ajoutée à deux contrôles d'application différents dans le même paramètre de pare-feu (par exemple, l'exécution de `kazaa.exe` est bloquée dans un contrôle d'application et son accès au réseau est bloqué dans un autre contrôle d'application défini dans le même paramètre de pare-feu), le contrôle le plus strict pour l'exécutable donné est appliqué (l'exécution de kazaa sera bloquée).

Environnements réseau

Si vous connaissez les paramètres réseau (serveurs de passerelle, serveurs DNS, serveurs DHCP, serveurs WINS, points d'accès disponibles et connexions d'adaptateur spécifiques) d'un emplacement, vous pouvez entrer les détails de service (IP et MAC), qui identifient le réseau, dans la stratégie pour basculer immédiatement vers l'emplacement sans devoir (faire) enregistrer l'environnement en tant qu'emplacement.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, puis cliquez sur le dossier *Environnements réseau*dans l'arborescence de stratégie à gauche.



Les listes permettent à l'administrateur de définir les services réseau présents dans l'environnement. Chaque service réseau peut contenir plusieurs adresses. L'administrateur détermine combien d'adresses correspondantes sont requises dans l'environnement pour basculer vers l'emplacement.

Vous devez utiliser au moins deux paramètres d'emplacement dans chaque définition d'environnement réseau.

Pour définir un environnement réseau :

1. Sélectionnez *Environnements réseau* dans l'arborescence des composants, puis cliquez sur le bouton *Nouveau composant*.
2. Entrez un nom et une description pour l'environnement réseau.
3. Dans la liste déroulante *Restriction de type d'adaptateur*, sélectionnez le type d'adaptateur autorisé à accéder à cet environnement réseau :
   - sans fil
   - Tous
   - Modem

- Filaire
- sans fil

4 Spécifiez le nombre minimal de services réseau requis pour identifier cet environnement réseau.

Chaque environnement réseau comporte un minimum d'adresses que ZENworks Security Client utilise pour l'identifier. Le nombre spécifié dans *Correspondance minimale* ne doit pas être supérieur au nombre total d'adresses réseau identifié comme nécessaire dans les listes à onglets. Spécifiez le nombre minimal de services réseau requis pour identifier cet environnement réseau.

5 Spécifiez les informations suivantes pour chaque service :

- **Adresse IP :** ce type d'adresse est limité à 15 caractères et contient uniquement les chiffres de 0 à 9 et des points. par exemple 123.45.6.789
- **Adresse MAC :** (facultatif) ce type d'adresse est limité à 12 caractères et contient uniquement les chiffres de 0 à 9 et les lettres de A à F (majuscules et minuscules), séparés par des deux-points. Par exemple, 00:01:02:34:05:B6
- Cochez la case *Doit correspondre* si l'identification de ce service est nécessaire pour définir l'environnement réseau.

6 Pour les onglets *Connexions à distance* et*Adaptateurs*, spécifiez les exigences suivantes :

- Pour les *Connexions à distance*, spécifiez le nom de l'entrée RAS de l'annuaire téléphonique ou le numéro composé.

  Remarque : Les entrées de l'annuaire téléphonique doivent contenir des caractères alphanumériques et ne peuvent pas inclure uniquement des caractères spéciaux (@, #, $,%, -, etc.) ou numériques (1-9). Les entrées contenant uniquement des caractères spéciaux et numériques sont supposées être des numéros composés.

- Pour les adaptateurs, spécifiez l'identificateur SSID pour chaque adaptateur autorisé. Vous pouvez spécifier des adaptateurs pour limiter exactement ceux qui sont autorisés à accéder à cet environnement réseau. Si vous n'entrez aucun identificateur SSID, l'accès est octroyé à tous les adaptateurs du type autorisé.

Pour associer un environnement réseau existant avec cet emplacement :

Remarque : L'association d'un environnement réseau unique avec plusieurs emplacements dans la même stratégie de sécurité entraîne des résultats imprévisibles et n'est pas recommandée.

1 Sélectionnez *Environnements réseau* dans l'arborescence des composants, puis cliquez sur le bouton *Associer le composant*.

2 Sélectionnez les environnements réseau dans la liste.

3 Configurez, au besoin, les paramètres d'environnement.

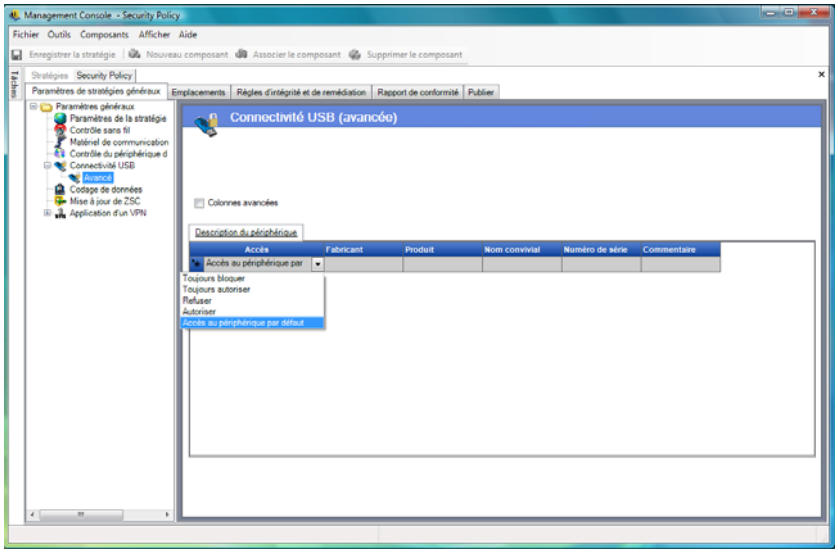
Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

4 Cliquez sur *Enregistrer la stratégie*.

Connectivité USB

Tous les périphériques se connectant via le BUS USB peuvent être autorisés ou refusés par la stratégie. Vous pouvez analyser ces périphériques dans la stratégie à partir du rapport d'inventaire des périphériques USB ou en analysant tous les périphériques actuellement connectés à une machine. Vous pouvez filtrer ces périphériques en fonction du fabricant, du nom, du numéro de série, du type de produit, etc. À des fins de prise en charge, l'administrateur peut configurer la stratégie de façon à ce qu'elle accepte un ensemble de périphériques, en les triant soit par type de fabricant (par exemple, tous les périphériques HP sont autorisés), soit par type de produit (tous les périphériques HID USB, comme la souris et le clavier, sont autorisés). En outre, vous pouvez autoriser des périphériques individuels de façon à éviter que des périphériques non pris en charge ne soient introduits dans le réseau (par exemple, aucune imprimante n'est autorisée à l'exception de celles figurant dans la stratégie).

Pour accéder à ce contrôle, cliquez sur l'onglet *Paramètres de stratégie généraux*, puis cliquez sur*Connectivité USB* dans l'arborescence de stratégie à gauche.



Spécifiez si vous autorisez ou refusez l'accès aux périphériques ne figurant pas sur la liste.

Les méthodes suivantes vous permettent de compléter la liste de façon à pouvoir autoriser ou refuser la connectivité USB à certains périphériques :

- « Ajout manuel de périphériques » page 92
- « Importation de listes de périphériques » page 93

Ajout manuel de périphériques

1 Insérez le périphérique dans le port USB de la machine sur laquelle la console de gestion est installée.

2 Une fois le périphérique prêt, cliquez sur le bouton *Analyser*. Si le périphérique a un numéro de série, sa description et son numéro de série s'affichent dans la liste.

3 Sélectionnez un paramètre dans la liste déroulante (le paramètre de *Périphérique amovible général* n'est pas appliqué pour cette stratégie) :

- **Activer :** les périphériques figurant dans la liste des périphériques préférés disposent de toutes les fonctionnalités de lecture/écriture ; tous les autres périphériques USB et de stockage externes sont désactivés.
- **Lecture seule :** les périphériques figurant dans la liste des périphériques préférés disposent de la fonctionnalité de lecture seule ; tous les autres périphériques USB et de stockage externes sont désactivés.

Répétez cette procédure pour tous les périphériques autorisés dans cette stratégie. Le même paramètre est appliqué à tous les périphériques.

Importation de listes de périphériques

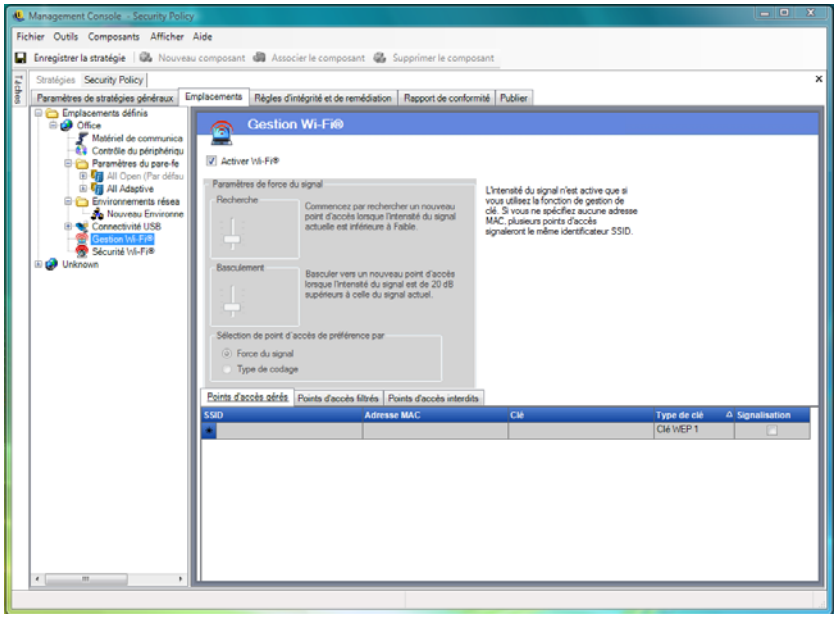
L'application Scanner USB de Novell génère une liste des périphériques et de leur numéro de série (Section 1.11, « Scanner d'unité USB », page 44). Pour importer cette liste, cliquez sur *Importer* et recherchez la liste. Les champs *Description* et *Numéro de série* sont complétés sur la base de cette liste.

Gestion Wi-Fi

La gestion Wi-Fi permet à l'administrateur de créer des listes de points d'accès. Les points d'accès sans fil entrés dans ces listes déterminent à quels points d'accès le noeud d'extrémité est autorisé à se connecter au sein de l'emplacement et quels points d'accès il est autorisé à voir dans le gestionnaire Configuration zéro de Microsoft (Zero Config). Les gestionnaires de configuration sans fil tiers ne sont pas pris en charge avec cette fonctionnalité. Si aucun point d'accès n'est entré, ils sont tous disponibles pour le noeud d'extrémité.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, puis cliquez sur l'icône *Gestion Wi-Fi* dans l'arborescence de la stratégie à gauche.

Remarque : Pour les contrôles de connectivité Sécurité Wi-Fi et Gestion Wi-Fi, la désélection de la case *Activer* désactive toute la connectivité Wi-Fi de cet emplacement.



L'intégration de points d'accès dans la liste *Points d'accès gérés* désactive Zero Config et force le noeud d'extrémité à se connecter uniquement aux points d'accès listés lorsqu'ils sont disponibles. Si les points d'accès gérés ne sont pas disponibles, ZENworks Security Client reprend la liste des points d'accès filtrés. Les points d'accès entrés dans la liste des points d'accès interdits ne s'affichent jamais dans Zero Config.

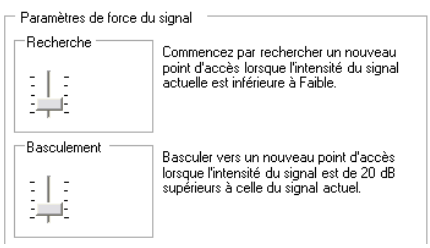
Remarque : La liste des points d'accès est uniquement prise en charge sous Windows* XP. Avant de déployer une liste de points d'accès, il est recommandé que tous les noeuds d'extrémité effacent la liste des réseaux préférés de Zero Config.

Les sections suivantes contiennent un complément d'informations :

- « Paramètres d'intensité du signal Wi-Fi » page 94
- « Points d'accès gérés » page 95
- « Points d'accès filtrés » page 96
- « Points d'accès interdits » page 97

Paramètres d'intensité du signal Wi-Fi

Si plusieurs points d'accès gérés WEP sont définis dans la liste, vous pouvez régler l'intensité du signal de basculement pour l'adaptateur Wi-Fi. Les seuils d'intensité du signal peuvent être réglés par emplacement afin de déterminer quand ZENworks Security Client recherchera, rejettera et basculera vers un autre point d'accès défini dans la liste.



Il est possible de paramétrer les informations suivantes :

- **Rechercher :** lorsque ce niveau d'intensité du signal est atteint, ZENworks Security Client commence à rechercher un nouveau point d'accès auquel se connecter. Le paramètre par défaut est Faible [- 70 dB].
- **Paramètre :** pour que ZENworks Security Client se connecte à un nouveau point d'accès, le niveau d'intensité du signal de ce dernier doit dépasser celui de la connexion actuelle en fonction de la valeur spécifiée. Le paramètre par défaut est +20 dB.

Les seuils d'intensité du signal sont déterminés selon la puissance (en dB) indiquée par le pilote miniport de l'ordinateur. Étant donné que chaque carte et radio Wi-Fi peut traiter différemment les signaux en dB pour leur indication d'intensité du signal reçu (RSSI), les valeurs varient d'un adaptateur à l'autre.

Vous pouvez définir votre préférence pour la sélection des points d'accès sur la base des éléments suivants :

- Intensité du signal
- Type de codage

Les valeurs par défaut associées aux seuils définis dans la console de gestion sont génériques pour la plupart des adaptateurs Wi-Fi. Il est recommandé de rechercher les valeurs RSSI de votre adaptateur Wi-Fi pour entrer un niveau exact. Les valeurs de Novell sont les suivantes :

Nom	Valeur par défaut
Excellent	-40 dB
Très bon	-50 dB
Bon	-60 dB
Faible	-70 dB
Très faible	-80 dB

Remarque : Bien que les noms d'intensité de signal ci-dessus correspondent à ceux utilisés par le service de configuration zéro de Microsoft, il se peut que les seuils ne correspondent pas. Zero Config détermine ses valeurs en fonction du rapport signal/bruit et pas uniquement sur la valeur en dB indiquée par RSSI. Par exemple, si un adaptateur Wi-Fi reçoit un signal à -54 dB et affiche un niveau sonore de -22 dB, le rapport signal/bruit est de 32 dB (-54 - -22 = 32), ce qui, sur l'échelle de Zero Configuration, se traduirait par une excellente intensité de signal, alors que, sur l'échelle de Novell, le signal -54 dB (s'il est signalé de cette manière par le pilote miniport) indiquerait une très bonne intensité de signal.

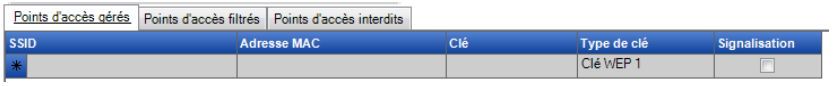
Il importe de noter que l'utilisateur final ne voit jamais les seuils d'intensité du signal de Novell ; cette information étant communiquée pour montrer la différence entre ce que l'utilisateur peut voir via Zero Config et ce qui se passe dans la réalité.

Points d'accès gérés

ZENworks Endpoint Security Management propose un processus simple permettant d'appliquer et de distribuer automatiquement des clés WEP (Wired Equivalent Privacy) sans l'intervention de l'utilisateur (contournement et fermeture du gestionnaire Configuration Zéro de Microsoft). Ce

processus protège l'intégrité des clés en ne les transmettant pas en texte clair dans un message électronique ou des notes écrites. En fait, l'utilisateur final ne doit jamais connaître la clé pour se connecter automatiquement au point d'accès. Il est ainsi possible d'éviter une éventuelle redistribution des clés à des utilisateurs non autorisés.

En raison des vulnérabilités de sécurité inhérentes à l'authentification des clés WEP partagées, Novell prend uniquement en charge l'authentification ouverte des clés WEP. En mode authentification partagée, le processus de validation de la clé AP/du client envoie une version en texte clair et une version codée d'une phrase d'identification facilement piratable en mode sans fil. Le pirate peut alors disposer des versions codée et en texte clair de la phrase. Une fois qu'il détient ces informations, déchiffrer la clé devient un jeu d'enfant.



Indiquez les informations suivantes pour chaque point d'accès :

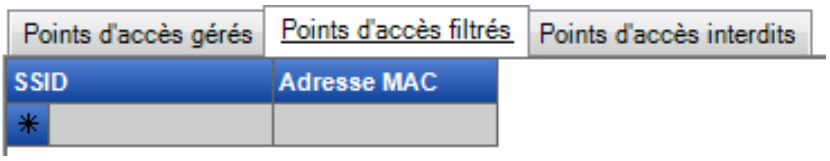
- **SSID :** identifiez le numéro SSID. Le numéro SSID respecte la casse.
- **Adresse MAC :** identifiez l'adresse MAC (recommandé, en raison des similitudes entre les SSID). Si vous ne spécifiez pas l'adresse MAC, plusieurs points d'accès sont supposés signaler le même numéro SSID.
- **Clé :** spécifiez la clé WEP pour le point d'accès (10 ou 26 caractères hexadécimaux).
- **Type de clé :** identifiez l'indice de la clé de codage en sélectionnant le niveau adéquat dans la liste déroulante.
- **Signalisation :** cochez cette case si le point d'accès défini diffuse actuellement son SSID. Ne la cochez pas s'il s'agit d'un point d'accès sans signal.

Remarque : ZENworks Security Client tente d'abord de se connecter à chaque point d'accès de signalisation listé dans la stratégie. Si aucun point d'accès de signalisation ne peut être localisé, ZENworks Security Client tente alors de se connecter à tous les points d'accès sans signal (identifiés par l'identificateur SSID) listés dans la stratégie.

Lorsqu'un ou plusieurs points d'accès sont définis dans la liste *Points d'accès gérés*, il est possible de définir l'intensité du signal de basculement pour l'adaptateur Wi-Fi.

Points d'accès filtrés

Les points d'accès entrés dans la liste des *Points d'accès filtrés* sont les seuls points d'accès qui s'affichent dans Zero Config. Cela permet d'éviter qu'un noeud d'extrémité se connecte à des points d'accès non autorisés.

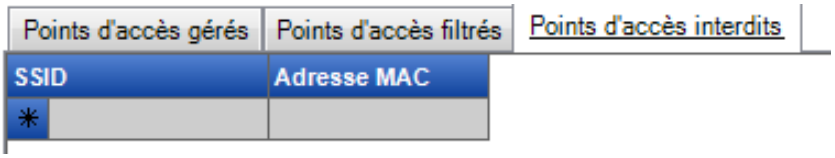


Entrez les informations suivantes pour chaque point d'accès :

- **SSID :** identifiez le numéro SSID. Le numéro SSID respecte la casse.
- **Adresse MAC :** identifiez l'adresse MAC (recommandé, en raison des similitudes entre les SSID). Si vous ne spécifiez pas l'adresse MAC, plusieurs points d'accès sont supposés signaler le même numéro SSID.

Points d'accès interdits

Les points d'accès entrés dans la liste des *Points d'accès interdits* ne s'affichent pas dans Zero Config et le noeud d'extrémité n'est pas autorisé à s'y connecter.



Entrez les informations suivantes pour chaque point d'accès :

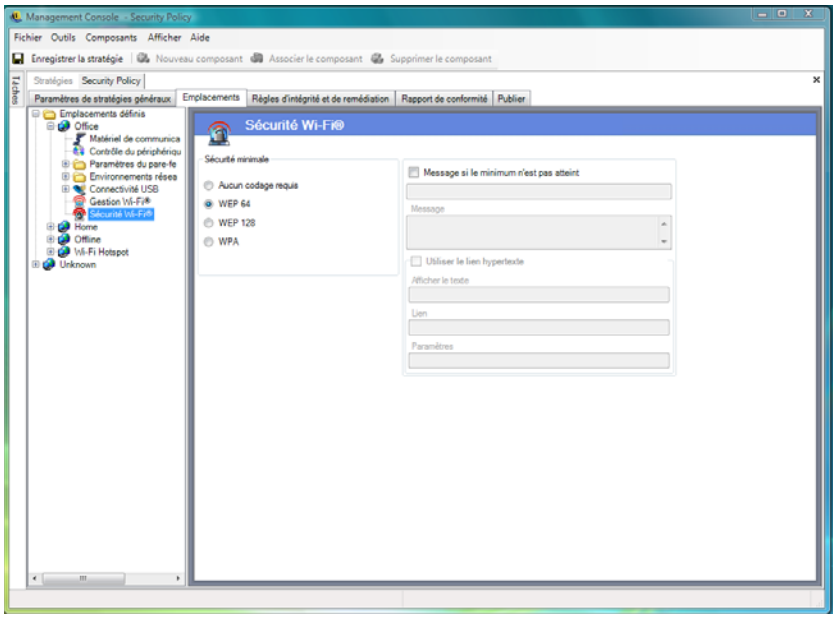
- **SSID :** identifiez le numéro SSID. Le numéro SSID respecte la casse.
- **Adresse MAC :** identifiez l'adresse MAC (recommandé, en raison des similitudes entre les SSID). Si vous ne spécifiez pas l'adresse MAC, plusieurs points d'accès sont supposés signaler le même numéro SSID.

Sécurité Wi-Fi

Si du matériel de communication Wi-Fi (cartes PCMCIA adaptateur Wi-Fi ou autres et radios Wi-Fi intégrées) est globalement autorisé (reportez-vous à la rubrique « Contrôle sans fil » page 52), des paramètres supplémentaires peuvent être appliqués à l'adaptateur à cet emplacement.

Pour accéder à ce contrôle, cliquez sur l'onglet *Emplacements*, puis cliquez sur *Sécurité Wi-Fi* dans l'arborescence de la stratégie à gauche.

Remarque : Pour les contrôles de connectivité Sécurité Wi-Fi et Gestion Wi-Fi, la désélection de la case *Activer* désactive toute la connectivité Wi-Fi de cet emplacement.



L'adaptateur Wi-Fi peut être configuré pour communiquer uniquement avec les points d'accès présentant un niveau de codage spécifique dans un emplacement donné.

Par exemple, si une configuration WPA de points d'accès est déployée dans une succursale, l'adaptateur peut être limité pour ne communiquer qu'avec les points d'accès présentant un niveau de codage WEP 128 ou supérieur, afin d'empêcher toute association accidentelle avec des points d'accès non sécurisés.

Il est recommandé de rédiger un message utilisateur personnalisé lorsque le paramètre est différent de *Aucun codage requis*.

Une préférence peut être définie pour établir une connexion à des points d'accès par ordre de niveau de codage ou par intensité de signal lorsque plusieurs points d'accès sont entrés dans les listes *Points d'accès gérés* et *Points d'accès filtrés*. Le niveau sélectionné applique la connectivité avec les points d'accès qui répondent aux exigences de codage minimales.

Prenons l'exemple de l'exigence de codage WEP 64 : si la préférence est définie sur le codage, les points d'accès présentant la puissance de codage la plus élevée ont la préférence sur tous les autres. Si la préférence est définie sur l'intensité du signal, le signal le plus puissant aura la préférence lors de la connexion.

2.2.3 Règles de remédiation et d'intégrité

ZENworks Endpoint Security Management permet de vérifier que le logiciel requis est en cours d'exécution sur le noeud d'extrémité et fournit des procédures de remédiation instantanée en cas d'échec de la vérification.

Les sections suivantes contiennent davantage d'informations :

- « Règles de logiciel antivirus/anti-espion » page 99
- « Tests d'intégrité » page 100

- « Vérifications d'intégrité » page 102
- « Règles de script avancé » page 103

Règles de logiciel antivirus/anti-espion

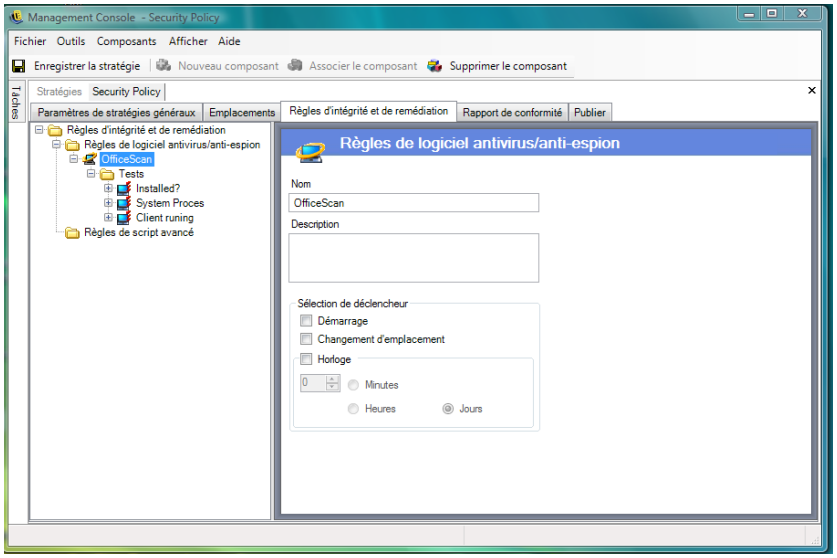
Les règles de logiciel antivirus/anti-espion vérifient que le logiciel antivirus ou anti-espion désigné sur le noeud d'extrémité est en cours d'exécution et actualisé. Les tests sont exécutés pour déterminer si le logiciel est en cours d'exécution et actualisé. La réussite des deux vérifications permet également de basculer vers n'importe quel emplacement défini. L'échec d'un des tests peut entraîner l'exécution des opérations suivantes (définies par l'administrateur) :

- Un rapport est envoyé au service de rapport.
- Un message utilisateur personnalisé s'affiche. Il contient un lien facultatif expliquant comment résoudre la violation de la règle.
- L'utilisateur bascule en état de quarantaine, ce qui limite son accès au réseau et bloque l'accès de certains programmes au réseau, empêchant l'utilisateur de l'infecter davantage.

Dès qu'un un test de suivi juge les noeuds d'extrémité conformes, les paramètres de sécurité reprennent automatiquement leur état initial.

Remarque : Cette fonction est uniquement disponible dans l'installation de ZENworks Endpoint Security Management et ne peut pas être utilisée pour les stratégies de sécurité UWS.

Pour accéder à ce contrôle, cliquez sur l'onglet *Règles d'intégrité et de remédiation*, puis sur *Règles de logiciel antivirus/anti-espion* dans l'arborescence de stratégie à gauche.



Il est possible de créer des tests personnalisés pour les logiciels ne figurant pas sur la liste par défaut. Un test individuel peut être créé pour exécuter des vérifications pour un ou plusieurs logiciels au sein de la même règle. Chaque ensemble de vérifications visant à contrôler si le processus est opérationnel et si le fichier existe a ses propres résultats de réussite et d'échec.

Pour créer une nouvelle règle de logiciel antivirus/anti-espion :

1. Sélectionnez *Règles de logiciel antivirus/anti-espion* dans l'arborescence des composants, puis cliquez sur *Nouvelle règle antivirus/anti-espion*.
2. Cliquez sur *Nouveau composant*.
3. Nommez la règle et décrivez-la.
4. Sélectionnez le déclencheur pour la règle :
   - **Startup :** exécute les tests au démarrage du système.
   - **Changement d'emplacement :** exécute les tests lorsque ZENworks Security Client bascule vers un nouvel emplacement.
   - **Horloge :** exécute des tests d'intégrité selon un planning défini par minute, heure ou jour.
5. Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.
6. Définissez les tests d'intégrité.

Pour associer des règles de logiciel antivirus/anti-espion existantes :

1. Sélectionnez *Règles de logiciel antivirus/anti-espion*, puis cliquez sur *Associer le composant*.
2. Sélectionnez les règles souhaitées dans la liste.
3. Redéfinissez les tests, vérifications et résultats (facultatif).

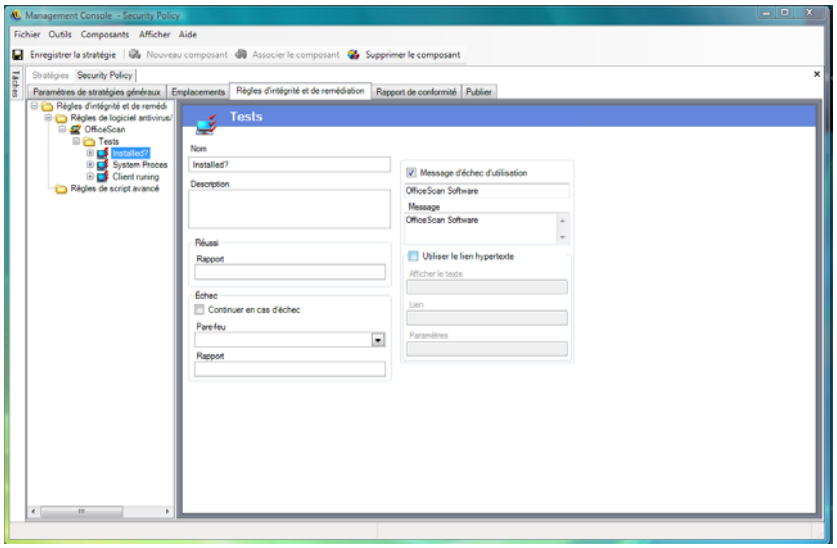
   Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

   ---
4. Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Les vérifications et tests d'intégrité sont automatiquement inclus et peuvent être édités au besoin.

Tests d'intégrité

Chaque test d'intégrité peut effectuer deux vérifications, à savoir que le *fichier existe* et que le *processus est opérationnel*. Chaque test dispose de ses propres résultats de réussite et d'échec.



Toutes les règles de logiciel antivirus/anti-espion définies disposent de vérifications et de tests standard prédéfinis. Des tests supplémentaires peuvent être ajoutés à la règle d'intégrité.

Plusieurs tests s'exécutent selon l'ordre entré ici. Le premier test doit être terminé avant l'exécution du suivant.

Pour créer un test d'intégrité :

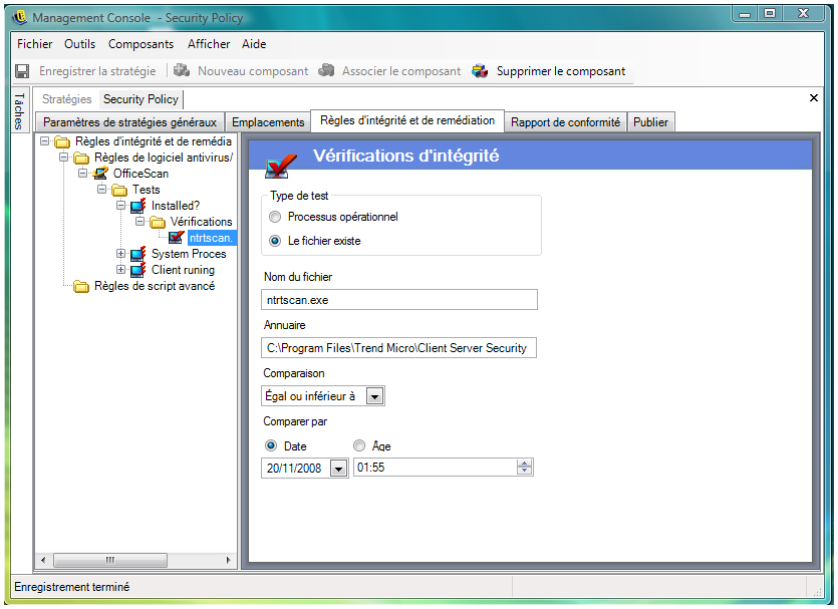
1. Sélectionnez *Tests d'intégrité* dans l'arborescence des composants, cliquez sur le signe + en regard du rapport souhaité pour visualiser la liste complète, cliquez avec le bouton droit sur *Tests*, puis cliquez sur *Ajouter de nouveaux tests*.
2. Nommez le test et décrivez-le.
3. Spécifiez le texte de rapport de réussite du test.
4. Définissez les paramètres suivants en cas d'échec du test :
   - **Continuer en cas d'échec:** cochez cette case si l'utilisateur peut toujours avoir accès au réseau en cas d'échec du test ou s'il doit être recommencé.
   - **Pare-feu :** ce paramètre sera appliqué en cas d'échec du test. Un paramètre de pare-feu Tous - Fermé, Intégrité non conforme ou un paramètre de quarantaine personnalisé empêche l'utilisateur de se connecter au réseau.
   - **Message :** sélectionnez un message utilisateur personnalisé à afficher en cas d'échec du test. Il peut inclure une procédure de remédiation pour l'utilisateur final.
   - **Rapport :** entrez le rapport d'échec qui sera envoyé au service de rapport.
5. Entrez un message d'échec. Ce message s'affiche uniquement en cas d'échec d'une ou plusieurs vérifications. Cochez la case, puis entrez les informations du message dans les zones prévues.
6. Un lien hypertexte peut être ajouté pour proposer des solutions de remédiation. Il peut s'agir d'un lien visant à fournir un complément d'informations ou à proposer le téléchargement d'un correctif ou d'une mise à jour en cas d'échec du test (reportez-vous à la rubrique Section , « Liens hypertexte », page 71.)
7. Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

8 Définissez les vérifications d'intégrité.

9 Au besoin, répétez la procédure ci-dessus pour créer un nouveau test de logiciel antivirus/anti-espion.

Vérifications d'intégrité

Les vérifications pour chaque test déterminent si un ou plusieurs des processus de logiciel antivirus/anti-espion sont en cours d'exécution ou si des fichiers essentiels existent. Pour qu'un test d'intégrité s'exécute, vous devez au moins définir une vérification.



Pour créer une nouvelle vérification, cliquez avec le bouton droit sur *Vérifications d'intégrité* dans l'arborescence de stratégie à gauche, puis cliquez sur*Ajouter de nouvelles vérifications d'intégrité*. Sélectionnez un des deux types de vérification et entrez les informations décrites ci-dessous :

Processus opérationnel : détermine si le logiciel est en cours d'exécution au déclenchement de l'événement (par exemple, le client AV). La seule information requise pour cette vérification est le nom exécutable.

Fichier existant: cette vérification est utilisée pour déterminer si le logiciel est actualisé et mis à jour lors du déclenchement de l'événement.

Entrez les informations suivantes dans les champs proposés :

- **Nom de fichier:** spécifiez le nom de fichier que vous souhaitez vérifier.
- **Répertoire du fichier :** spécifiez le répertoire dans lequel se trouve le fichier.
- **Comparaison de fichiers :** sélectionnez une comparaison de dates dans la liste déroulante :
  - Aucun
  - Égal

- Égal ou supérieur
- Égal ou inférieur

- **Comparer par:** spécifiez *Âge* ou *Date*.
  - L'option *Date* garantit que le fichier n'est pas postérieur à une date ni une heure spécifiée (par exemple, la date de la dernière mise à jour).
  - L'option *Âge* garantit que le fichier ne dépasse pas la durée spécifique indiquée en jours.

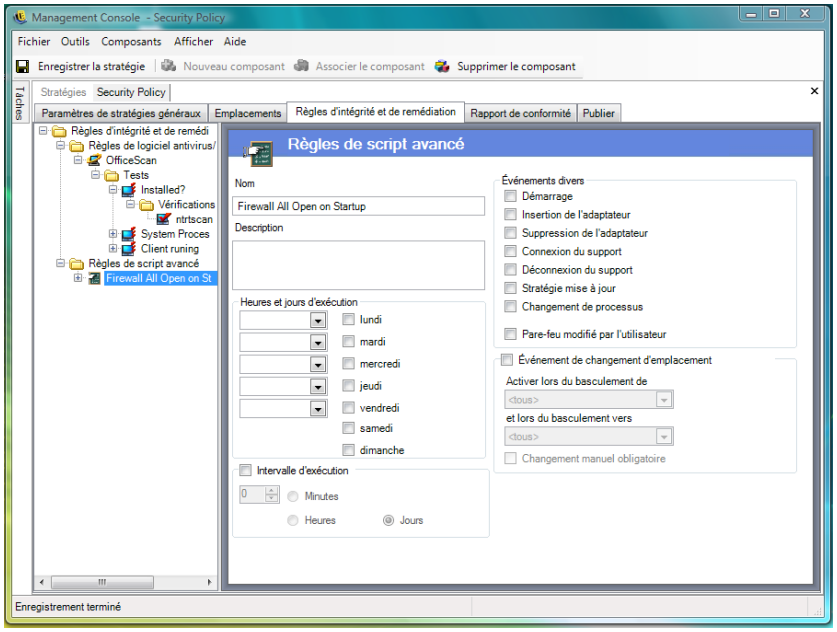
Remarque : La comparaison de fichier « Égal » est traitée comme « Égal ou inférieur à » pour la vérification *Âge*.

Les vérifications sont exécutées dans l'ordre de leur saisie.

Règles de script avancé

ZENworks Endpoint Security Management inclut un outil de script de règle avancé qui permet aux administrateurs de créer des règles extrêmement flexibles et complexes et d'effectuer des actions de remédiation.

Pour accéder à ce contrôle, cliquez sur l'onglet *Règles d'intégrité et de remédiation*, puis sur l'icône *Règles de script avancé* dans l'arborescence de stratégie à gauche.



L'outil de script utilise les langages de script courants tels que VBScript ou JScript pour créer des règles qui contiennent à la fois un déclencheur (le moment de l'exécution de la règle) et le script réel (la logique de la règle). L'administrateur n'est pas limité quant au type de script à exécuter.

Le script avancé est mis en oeuvre séquentiellement, tout comme d'autres règles d'intégrité. Par conséquent, un script à long terme empêche d'autres règles (y compris les règles programmées) de s'exécuter tant que ce script n'est pas terminé.

Pour créer une règle de script avancé :

1. Cliquez avec le bouton droit sur *Règles de script avancé* dans l'arborescence de composants, puis cliquez sur *Ajouter de nouvelles règles de script*.
2. Nommez la règle et décrivez-la.
3. Spécifiez les événements déclencheurs
   - **Heures et jours d'exécution :** spécifiez jusqu'à cinq moments différents pour l'exécution du script. Le script s'exécute sur une base hebdomadaire, les jours sélectionnés.
   - **Intervalle d'exécution :** spécifiez l'intervalle d'exécution.
   - **Événements divers :** spécifiez les événements sur le noeud d'extrémité qui déclenchent le script.
   - **Événement de changement d'emplacement :** spécifiez l'événement de changement d'emplacement qui déclenche le script. Ces événements ne sont pas indépendants. Ils viennent s'ajouter à l'événement précédent.
     - **Événement de vérification d'emplacement :** le script s'exécute lors de tous les changements d'emplacement.
     - **Activer lors du basculement de :** le script s'exécute uniquement lorsque l'utilisateur quitte cet emplacement (spécifié) pour un autre.
     - **Activer lors du basculement vers :** le script s'exécute lorsque l'utilisateur accède à cet emplacement spécifié au départ d'un autre. Si un paramètre d'emplacement a été attribué à *Activer lors du basculement de*, par exemple, Bureau, le script s'exécute uniquement lorsque l'emplacement bascule du bureau vers l'emplacement spécifié.
     - **Changement manuel obligatoire :** le script s'exécute uniquement lorsque l'utilisateur bascule manuellement d'un ou vers un emplacement.
4. Créez des variables de script. Pour plus d'informations, reportez-vous à « Variables de script » page 105.
5. Écrivez le texte du script. Pour plus d'informations, reportez-vous à « Texte de script » page 106.
6. Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Pour associer une règle de script avancé existante :

1. Sélectionnez *Règles de script avancé* dans l'arborescence de composants et cliquez sur *Associer un nouveau/une nouvelle*,
2. sélectionnez les règles souhaitées dans la liste.
3. Redéfinissez l'événement déclencheur, les variables ou le script, si nécessaire.

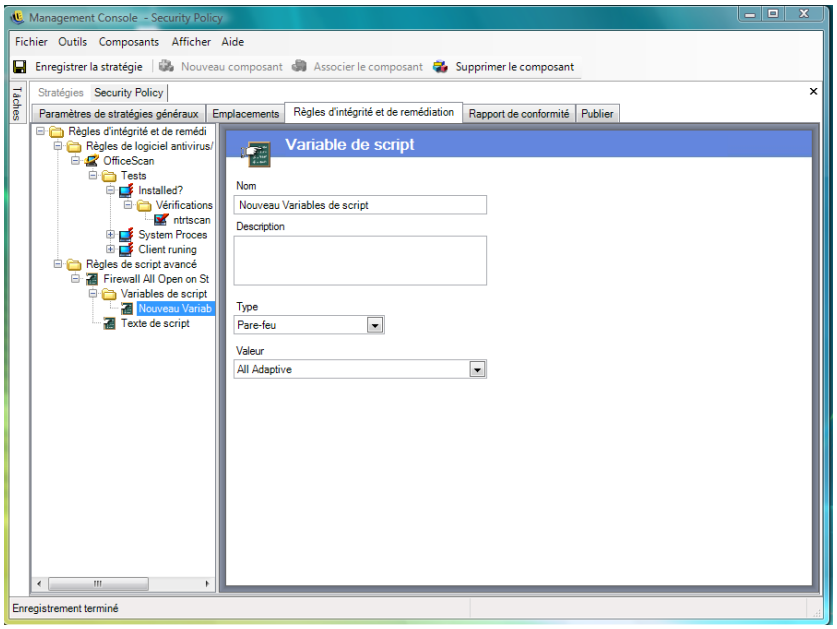
   Remarque : La modification des paramètres d'un composant partagé affecte toutes les autres instances de ce même composant. Utilisez la commande *Afficher l'utilisation* pour afficher toutes les autres stratégies associées à ce composant.

   ---

4. Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Variables de script

Il s'agit d'un paramètre facultatif qui permet à l'administrateur de définir une variable (var) pour le script et d'utiliser soit la fonctionnalité ZENworks Endpoint Security Management (permettant par exemple d'envoyer des messages utilisateur personnalisés ou de démarrer des liens hypertextes définis, de basculer vers un emplacement ou un paramètre de pare-feu déterminé), soit de modifier la valeur d'une variable sans devoir modifier le script proprement dit.



Pour créer une variable de script :

1. Cliquez avec le bouton droit sur *Variables de script* dans l'arborescence de composants, puis cliquez sur *Ajouter de nouvelles variables*.
2. Nommez la variable et décrivez-la.
3. Sélectionnez un type de variable :
   - **Messages utilisateur personnalisés:** définit un message utilisateur personnalisé qui peut se lancer en tant qu'action.
   - **Pare-feu :** définit un paramètre de pare-feu qui peut être appliqué comme une opération.
   - **Liens hypertexte :** définit un lien hypertexte qui peut être exécuté comme une opération.
   - **Emplacement :** définit un emplacement qui peut être appliqué comme une opération.
   - **Numéro :** définit une valeur numérique.
   - **Chaîne :** définit une valeur de chaîne.
4. Spécifiez la valeur de la variable :
   - Tous - Adaptatif
   - Tous - Fermé
   - Tous - Ouvert

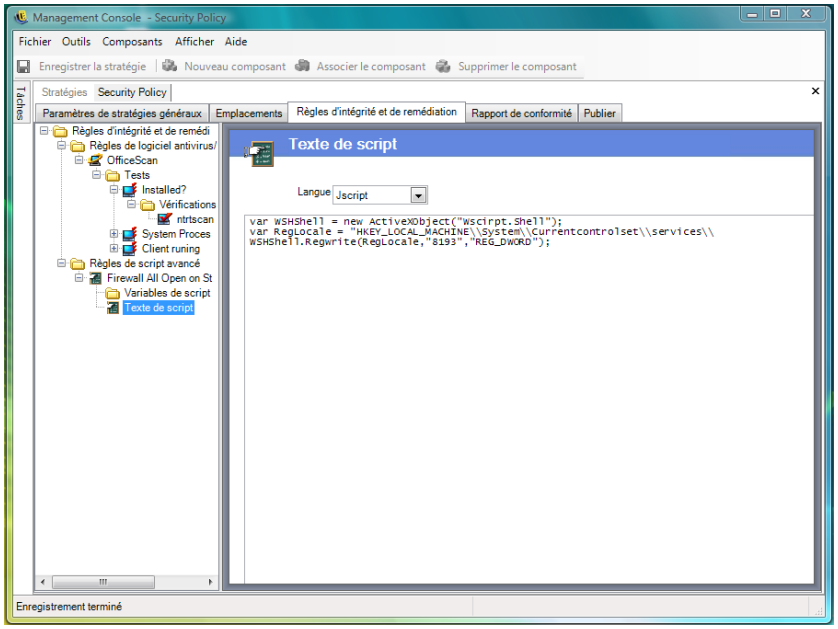
- Nouveaux paramètres de pare-feu
- Intégrité non conforme

5 Cliquez sur *Enregistrer la stratégie*. Si votre stratégie comporte des erreurs, reportez-vous à Section 2.2.6, « Notification d'erreur », page 110.

Texte de script

L'administrateur de ZENworks Endpoint Security Management n'est pas limité quant au type de script que ZENworks Security Client peut exécuter. Il est recommandé de tester tous les scripts avant de distribuer la stratégie.

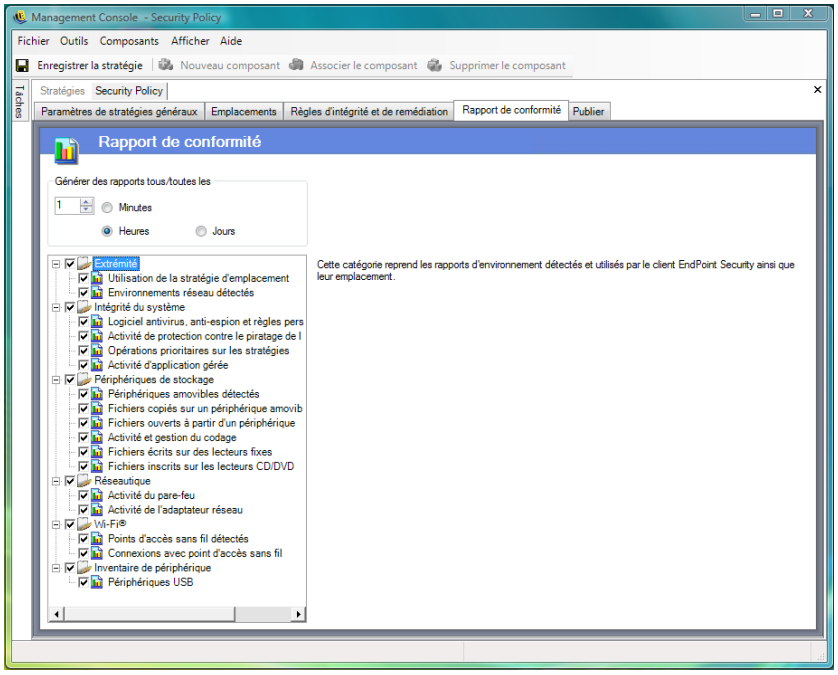
Sélectionnez le type de script (Jscript ou VBscript) et entrez le texte du script dans le champ prévu à cet effet. Le script peut être copié à partir d'une autre source et collé dans le champ.



2.2.4 Rapport de conformité

étant donné le niveau et l'accès des pilotes de ZENworks Security Client, presque toutes les transactions qu'effectue le noeud d'extrémité peuvent faire l'objet d'un rapport. Chaque inventaire système facultatif peut s'exécuter sur le noeud d'extrémité à des fins de création de stratégie et de dépannage. Pour accéder à ces rapports, cliquez sur l'onglet *Rapport de conformité*.

Remarque : Les rapports ne sont pas disponibles lorsque la console de gestion est exécutée en mode autonome.



Pour exécuter un rapport de conformité pour cette stratégie :

1. Indiquez la fréquence à laquelle vous souhaitez générer des rapports. Il s'agit de la fréquence à laquelle les données seront téléchargées à partir de ZENworks Security Client sur le service de distribution de stratégie.
2. Cochez chaque catégorie ou type de rapport que vous souhaitez capturer.

Les rapports suivants sont disponibles :

Noeud d'extrémité

- **Utilisation de la stratégie d'emplacement :** ZENworks Security Client signale toutes les stratégies d'emplacement appliquées et la durée de leur application.
- **Environnements réseau détectés :** ZENworks Security Client signale tous les paramètres d'environnement réseau détectés.

Intégrité du système

- **Logiciels antivirus, anti-espion et règles personnalisées:** ZENworks Security Client signale les messages d'intégrité configurés en fonction des résultats de test.
- **Activité de protection contre la falsification du noeud d'extrémité :** ZENworks Security Client signale toutes les tentatives de falsification du client de sécurité.
- **Opérations prioritaires sur les stratégies :** ZENworks Security Client signale toutes les tentatives d'octroi de la priorité administrative sur le client de sécurité.
- **Activité d'application gérée :** ZENworks Security Client signale toutes les activités d'application gérée.

Périphériques de stockage

- **Périphériques amovibles détectés :** ZENworks Security Client signale tous les périphériques de stockage amovibles détectés par le client de sécurité.
- **Fichiers copiés sur un périphérique amovible :** ZENworks Security Client signale les fichiers copiés sur un périphérique de stockage amovible.
- **Fichiers ouverts à partir d'un périphérique amovible :** ZENworks Security Client signale les fichiers ouverts à partir d'un périphérique de stockage amovible.
- **Activité et gestion du codage :** ZENworks Security Client signale les activités de codage/décodage utilisant ZENworks Storage Encryption Solution.
- **Fichiers inscrits sur des unités fixes :** ZENworks Security Client signale le nombre de fichiers inscrits sur les unités fixes du système.
- **Fichiers inscrits sur les unités CD/DVD :** ZENworks Security Client signale le nombre de fichiers inscrits sur les unités CD/DVD du système.

Réseautique

- **Activité du pare-feu :** ZENworks Security Client signale tout blocage de trafic par le pare-feu configuré pour la stratégie d'emplacement appliquée.

  Important : L'activation de ce rapport peut donner lieu à la collecte de gros volumes de données. Les données peuvent très rapidement submerger une base de données. Un test effectué sur un seul client ZENworks Security Client a signalé 1 115 téléchargements de données de paquets bloqués sur une période de 20 heures. Avant un déploiement à grande échelle, mieux vaut prévoir une période de surveillance et d'adaptation avec un client de test dans l'environnement concerné.

- **Activité de l'adaptateur réseau :** ZENworks Security Client signale tout le trafic passant par un périphérique réseau géré.

Wi-Fi

- **Points d'accès sans fil détectés :** ZENworks Security Client signale tous les points d'accès détectés.
- **Connexions avec point d'accès sans fil :** ZENworks Security Client signale toutes les connexions avec point d'accès du noeud d'extrémité.

Inventaire du périphérique

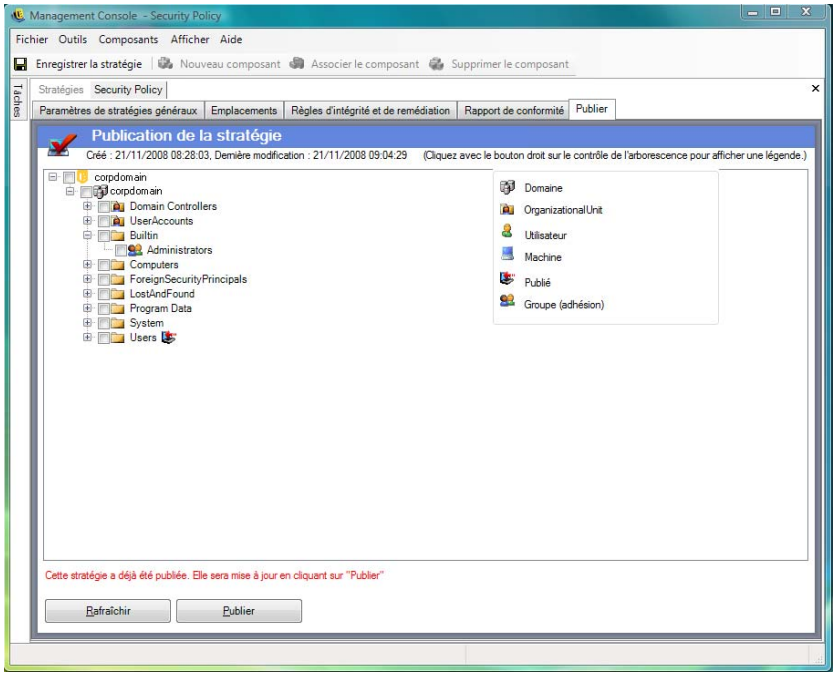
- **Périphériques USB :** ZENworks Security Client signale tous les périphériques USB du système détectés.

2.2.5 Publication

Les stratégies de sécurité terminées sont envoyées aux utilisateurs à l'aide du mécanisme de publication. Une fois publiée, une stratégie peut encore être actualisée, les utilisateurs recevant ces mises à jour au moment de leurs enregistrements planifiés. Pour publier une stratégie, cliquez sur l'onglet *Publier*. Les informations suivantes sont affichées :

- l'arborescence Annuaire actuelle ;

- les dates de création et de modification de la stratégie ;
- les boutons *Rafraîchir* et *Publier*.



En fonction des autorisations de publication de l'utilisateur actuel, l'arborescence Annuaire peut afficher en rouge une ou plusieurs sélections. Les utilisateurs ne sont pas autorisés à publier pour les utilisateurs/groupes affichés en rouge.

Les utilisateurs et leurs groupes associés ne s'affichent pas tant qu'ils ne se sont pas authentifiés auprès du service de gestion. Il se peut que les modifications apportées au service Annuaire de l'entreprise ne s'affichent pas immédiatement dans la console de gestion. Cliquez sur *Rafraîchir* pour mettre à jour l'arborescence Annuaire pour le service de gestion.

Les sections suivantes contiennent davantage d'informations :

- « Publication d'une stratégie » page 109
- « Mise à jour d'une stratégie publiée » page 110

Publication d'une stratégie

1. Sélectionnez un groupe d'utilisateurs (ou des utilisateurs individuels) dans l'arborescence Annuaire à gauche. Double-cliquez sur les utilisateurs pour les sélectionner (si un groupe d'utilisateurs est sélectionné, tous les utilisateurs sont inclus).

   L'icône s'affichera en regard du nom des utilisateurs n'ayant pas reçu la stratégie. Si un utilisateur ou un groupe a déjà reçu la stratégie, l'icône s'affiche en regard du nom des entrées dans l'arborescence Annuaire.

   Pour désélectionner un utilisateur ou un groupe, double-cliquez sur leur nom pour supprimer l'icône .
2. Cliquez sur *Publier* pour envoyer la stratégie au service de distribution de stratégies.

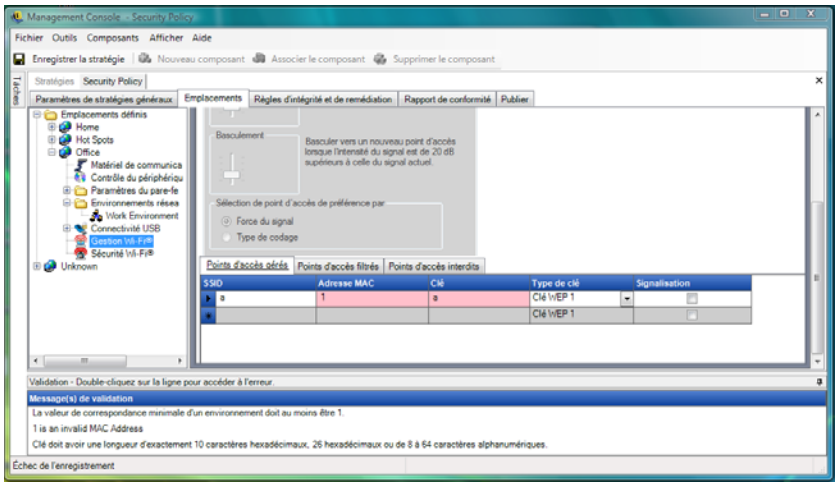
Mise à jour d'une stratégie publiée

Une fois la stratégie publiée pour des utilisateurs, les mises à jour simples peuvent s'effectuer en éditant les composants de la stratégie, puis en la republiant. Par exemple, si l'administrateur ZENworks Endpoint Security Management doit modifier la clé WEP pour un point d'accès, il a simplement besoin d'éditer la clé, enregistrer la stratégie et cliquer sur *Publier*. Les utilisateurs affectés reçoivent la stratégie mise à jour (et la nouvelle clé) lors de leur prochain enregistrement.

2.2.6 Notification d'erreur

Lorsque l'administrateur tente d'enregistrer une stratégie avec des données incomplètes ou incorrectes dans un composant, le volet de validation s'affiche au bas de la console de gestion et signale chaque erreur. Toutes les erreurs doivent être corrigées avant d'enregistrer la stratégie.

Double-cliquez sur chaque ligne de validation pour afficher l'erreur à l'écran. Les erreurs sont mises en surbrillance comme illustré sur la figure ci-dessous.

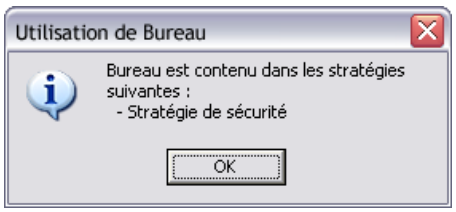


2.2.7 Afficher l'utilisation

Les modifications apportées aux composants de stratégie partagés affectent toutes les stratégies auxquelles ils sont associés. Avant de mettre à jour ou de modifier un composant de stratégie, il est recommandé d'exécuter la commande*Afficher l'utilisation* pour déterminer les stratégies affectées par la modification.

1 Cliquez avec le bouton droit sur le composant, puis cliquez sur *Afficher l'utilisation*.

Une fenêtre contextuelle affiche chaque instance de ce composant dans d'autres stratégies.



2.3 Importation et exportation de stratégies

Les sections suivantes contiennent un complément d'informations :

2.3.1 Importation de stratégies

Une stratégie peut être importée à partir de n'importe quel emplacement de fichiers sur le réseau disponible.

1. Dans la console de gestion, cliquez sur *Fichier* > *Importer stratégie*.

   Si vous éditez ou rédigez une stratégie, l'éditeur ferme la stratégie (en vous invitant à l'enregistrer) avant d'ouvrir la fenêtre d'importation.
2. Effectuez une recherche pour déterminer l'emplacement du fichier et spécifier son nom dans le champ prévu à cet effet.

Une fois la stratégie importée, elle peut encore être éditée ou publiée immédiatement.

2.3.2 Exportation d'une stratégie

Les stratégies peuvent être exportées à partir de la console de gestion et distribuées via la messagerie ou un partage réseau. Cette technique peut être utilisée pour distribuer des stratégies au niveau de l'entreprise dans des environnements où sont déployés plusieurs services de gestion et éditeurs de stratégie.

Pour exporter une stratégie de sécurité :

1. Dans la console de gestion, cliquez sur *Fichier* > *Exporter*.
2. Spécifiez une destination et attribuez à la stratégie un nom portant l'extension `.sen` (par exemple, `C:\Bureau\stratégiedevente.sen`) Vous pouvez cliquer sur le bouton de navigation pour accéder à un emplacement.
3. Cliquez sur *Exporter*.

Deux fichiers sont exportés. Le premier contient la stratégie (fichier `*.sen`). Le second est le fichier `setup.sen` nécessaire au décodage de la stratégie lors de l'importation.

Les stratégies exportées doivent être importées dans une console de gestion avant d'être publiées pour les utilisateurs gérés.

2.3.3 Exportation de stratégies vers des utilisateurs non gérés

Si des clients ZENworks Security Client non gérés ont été déployés au sein de l'entreprise, une console de gestion exécutée en mode autonome doit être installée pour créer des stratégies. Pour plus d'informations, reportez-vous au « Guide d'installation de ZENworks Endpoint Security Management ».

Pour distribuer des stratégies non gérées :

1. Localisez et copiez le fichier `setup.sen` de la console de gestion dans un dossier distinct.

   Le fichier `setup.sen` est généré lors de l'installation de la console de gestion et enregistré dans le répertoire `\Program Files\Novell\Console de gestion ESM\`.

2. Créez une stratégie dans la console de gestion. Pour plus d'informations, reportez-vous à Section 2.2, « Création de stratégies de sécurité », page 49.

3. Utilisez la commande *Exporter* pour exporter la stratégie vers le même dossier contenant le fichier `setup.sen`.

   Pour être acceptées par ZENworks Security Client, toutes les stratégies distribuées doivent porter le nom `policy.sen`.

4. Distribuez les fichiers `policy.sen` et `setup.sen`. Ces fichiers doivent être copiés dans le répertoire `\Program Files\Novell\ZENworks Security Client\` pour tous les clients non gérés.

Le fichier `setup.sen` ne doit être copié qu'une seule fois dans les clients ZENworks Security Client non gérés, avec la première stratégie. Par la suite, seules les nouvelles stratégies doivent être distribuées.