AUTHORIZED DOCUMENTATION

Guide de l'utilisateur de Endpoint Security Client 3.5

December 22, 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

À propos de ce guide 7

1 Introduction 9

1.1 Sécurité appliquée aux ordinateurs portables 9
1.2 Protection de la couche NDIS via un pare-feu 10

2 Présentation de Endpoint Security Client 3.5 11

2.1 Terminologie ESM 11
2.2 Login à Endpoint Security Client 3.5 12

3 Utilisation de Endpoint Security Client 3.5 15

3.1 Déplacement au sein des environnements réseau 15
3.2 Changement d'emplacement 16
3.2.1 Enregistrement d'un environnement réseau 16
3.2.2 Enregistrement d'un environnement Wi-Fi. 17
3.2.3 Suppression d'un environnement enregistré 18
3.3 Modification des paramètres de pare-feu. 18
3.4 Codage de données. 19
3.4.1 Gestion de fichiers sur des disques fixes 19
3.4.2 Gestion de fichiers sur un support de stockage amovible 19
3.5 Mise à jour des stratégies 22
3.6 Affichage de l'aide 23
3.7 Octroi d'un mot de passe prioritaire 23
3.8 Diagnostics. 24

À propos de ce guide

Ce *guide de l'utilisateur de Novell® ZENworks® Endpoint Security Client 3.5* explique à l'utilisateur final le fonctionnement de Endpoint Security Client 3.5 pour Windows* XP* et Windows Server 2000*.

Il est organisé de la manière suivante :

- Chapitre 1, « Introduction », page 9
- Chapitre 2, « Présentation de Endpoint Security Client 3.5 », page 11
- Chapitre 3, « Utilisation de Endpoint Security Client 3.5 », page 15

Public

Il peut être envoyé à tous les employés de l'entreprise pour leur apprendre à utiliser Endpoint Security Client 3.5.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires au bas de chaque page de la documentation en ligne ou accédez au site Novell de commentaires sur la documentation (http://www.novell.com/documentation/feedback.html) pour entrer vos commentaires.

Documentation complémentaire

D'autres manuels (aux formats PDF et HTML) viennent compléter la documentation relative à ZENworks Endpoint Security Management. Ils facilitent l'apprentissage et la mise en oeuvre de ce produit : Pour d'autres documents, reportez-vous au site Web de documentation de ZENworks Endpoint Security Management 3.5 (http://www.novell.com/documentation/zesm35).

Conventions relatives à la documentation

Dans la documentation Novell, le symbole « supérieur à » (>) est utilisé pour séparer deux opérations dans une étape de procédure, ainsi que deux éléments dans un chemin de références croisées.

Un symbole de marque déposée (®, ™, etc.) indique qu'il s'agit d'une marque de Novell. Un astérisque (*) indique une marque commerciale de fabricant tiers.

Lorsqu'un nom de chemin peut s'écrire avec une barre oblique pour certaines plates-formes et une barre oblique inverse pour d'autres, il sera toujours présenté avec une barre oblique inverse. Les utilisateurs des plates-formes nécessitant l'utilisation de barres obliques (Linux*, par exemple) doivent les utiliser en fonction de leurs logiciels.

Introduction

1

Novell® ZENworks® Endpoint Security Management (ESM) est conçu pour protéger les données des entreprises grâce à l'outil de gestion centralisée Endpoint Security Client. Endpoint Security Client 3.5 est installé sur des ordinateurs d'entreprise exécutant Windows XP et Windows 2000. Il applique des stratégies de sécurité écrites et envoyées via le système de distribution et de gestion ESM. Quelle que soit leur taille, les entreprises peuvent ainsi créer, déployer, appliquer et contrôler les stratégies de sécurité des ordinateurs situés tant à l'intérieur qu'à l'extérieur de leur périmètre de sécurité.

Pour les ordinateurs exécutant Windows Vista et Windows 2008, consultez le *guide de l'utilisateur de ZENworks Endpoint Security Client 4.0*.

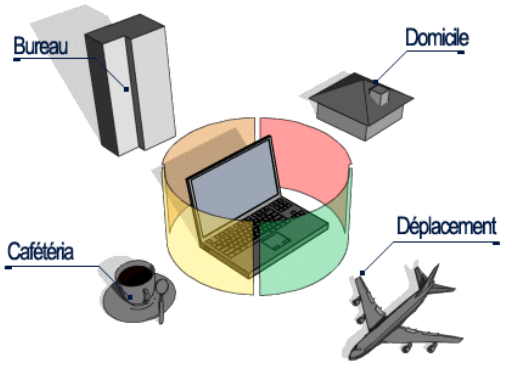
Les sections suivantes contiennent des informations supplémentaires :

- Section 1.1, « Sécurité appliquée aux ordinateurs portables », page 9
- Section 1.2, « Protection de la couche NDIS via un pare-feu », page 10

1.1 Sécurité appliquée aux ordinateurs portables

La sécurité est appliquée de manière générale et par emplacement réseau. Chaque emplacement indiqué dans une stratégie de sécurité détermine les autorisations accordées à l'utilisateur dans cet environnement réseau, ainsi que les paramètres activés du pare-feu. Les paramètres du pare-feu déterminent les ports, les adresses réseau et les applications bénéficiant d'un accès au réseau mais également leur mode d'accès.

Figure 1-1 *ESM règle les paramètres de sécurité en fonction de l'environnement réseau détecté.*

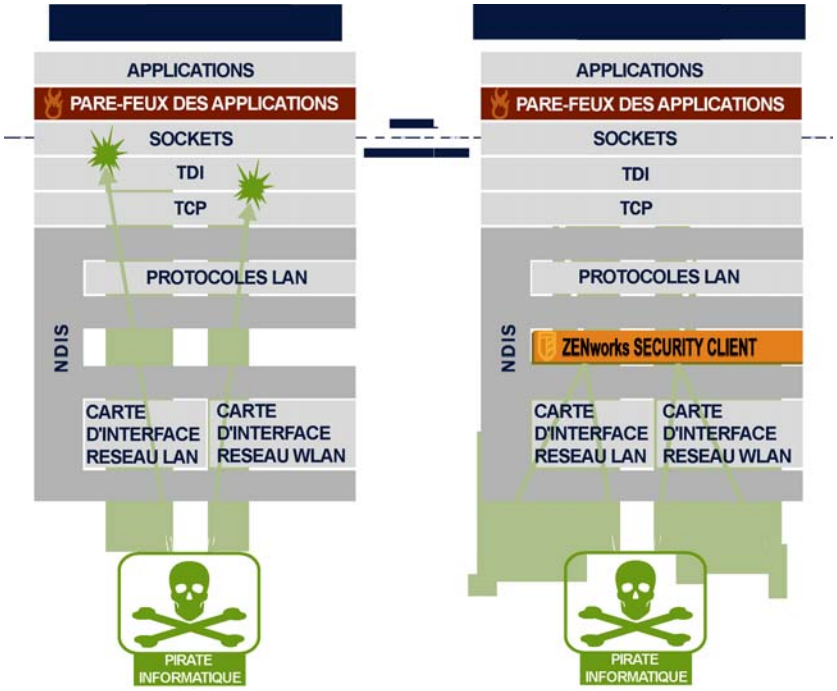


Une fois les environnements réseau définis, les opérations normales de Endpoint Security Client 3.5 sont transparentes pour l'utilisateur. Les mesures de protection de Endpoint Security Client 3.5 peuvent parfois interrompre le déroulement normal des opérations. Dans ce cas, des messages et des liens hypertexte informent l'utilisateur de la stratégie de sécurité, des étapes de protection entreprises et l'invitent à consulter d'autres informations pour l'aider à résoudre le problème.

1.2 Protection de la couche NDIS via un pare-feu

En termes de sécurisation des périphériques mobiles, ESM surclasse les technologies classiques de pare-feu personnel qui interviennent exclusivement au niveau de la couche applicative ou en tant que pilote de pare-feu. La sécurité du client ESM est intégrée au pilote NDIS (Network Driver Interface Specification) pour toutes les cartes d'interface réseau, ce qui assure une protection dès l'instant où les paquets de données pénètrent dans l'ordinateur. Les différences entre ESM, d'une part et les pare-feux de la couche Application et les pilotes de filtre, d'autre part sont illustrées à la Figure 1-2, « Efficacité d'un pare-feu de la couche NDIS », page 10.

Figure 1-2 *Efficacité d'un pare-feu de la couche NDIS*



Les décisions et les performances du système sont optimisées quand les déploiements de sécurité fonctionnent sur la couche appropriée la plus basse de la pile de protocoles. Avec Endpoint Security Client 3.5, le trafic non sollicité est interrompu aux niveaux inférieurs de la pile de pilotes NDIS, via l'application de la technologie Adaptive Port Blocking (inspection des paquets avec état). Cette approche offre une protection contre les attaques basées sur les protocoles, notamment les analyses de ports non autorisées ainsi que les attaques SYN Flood, etc.

Vous devez respecter toutes les recommandations d'utilisation et de maintenance indiquées dans le présent document afin de garantir la sécurité de l'environnement jusqu'à ses noeuds d'extrémité.

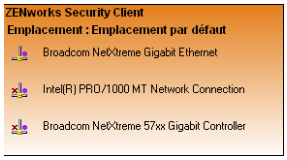
Présentation de Endpoint Security Client 3.5

2

ZENworks® Security Client protège les ordinateurs des attaques de données dans le cadre privé et professionnel, et lors de déplacements grâce à l'application de stratégies de sécurité créées par l'administrateur Endpoint Security Management (ESM) de l'entreprise. Les paramètres de pare-feu attribués à des emplacements individuels sont adaptés automatiquement lorsque les utilisateurs d'ordinateurs portables passent du réseau d'entreprise à leur réseau personnel ou sont en déplacement et se loguent à un réseau public ou ouvert.

Des niveaux de sécurité sont appliqués à plusieurs emplacements utilisateur sans nécessiter pour autant de compétences ou de connaissances en matière de sécurité réseau, de configurations de ports, de fichiers partagés masqués ou d'autres détails techniques. Vous pouvez accéder instantanément à des informations sur l'emplacement et le paramètre du pare-feu de Endpoint Security Client 3.5 et sur les adaptateurs actuellement actifs ou autorisés en passant simplement le pointeur de la souris sur l'icône de la barre des tâches pour afficher l'info-bulle Endpoint Security Client (voir Figure 2-1).

Figure 2-1 *Info-bulle Endpoint Security Client*



Les sections suivantes contiennent des informations supplémentaires :

- Section 2.1, « Terminologie ESM », page 11
- Section 2.2, « Login à Endpoint Security Client 3.5 », page 12

2.1 Terminologie ESM

La terminologie suivante est fréquemment utilisée dans cette documentation :

Emplacements : il s'agit de définitions simples qui permettent aux utilisateurs d'identifier l'environnement réseau dans lequel ils se trouvent, de fournir des paramètres de sécurité immédiats (définis par l'administrateur), et qui autorisent l'utilisateur à enregistrer l'environnement réseau et à modifier les paramètres de pare-feu appliqués.

Chaque emplacement se voit attribuer des paramètres de sécurité uniques qui permettent de bloquer l'accès à certaines fonctionnalités réseau et équipements dans des environnements réseau plus hostiles et, au contraire, d'autoriser un accès plus large au sein d'environnements approuvés. Les emplacements définissent les informations suivantes :

- la fréquence à laquelle Endpoint Security Client 3.5 recherche une mise à jour des stratégies dans cet emplacement ;
- les autorisations de gestion des emplacements accordées à un utilisateur ;
- les paramètres de pare-feu utilisés à cet emplacement ;

- le matériel de communication pouvant être connecté ;
- la procédure de gestion de la sécurité et de la connectivité Wi-Fi à cet emplacement ;
- le niveau auquel l'utilisateur est autorisé à utiliser des périphériques de stockage amovibles (comme les clés USB et les cartes mémoire) et les lecteurs CD/DVD-RW ;
- tout environnement réseau permettant de définir l'emplacement.

Paramètres de pare-feu : les paramètres de pare-feu contrôlent la connectivité de tous les ports réseau (1-65535), paquets réseau (ICMP, ARP, etc.), adresses réseau (IP ou MAC) et les applications réseau (partage de fichiers, logiciel de messagerie instantanée, etc.) qui sont autorisées à se connecter au réseau lorsque le paramètre est appliqué. ESM comporte trois paramètres de pare-feu par défaut qui peuvent être définis dans un emplacement. L'administrateur ESM peut également créer des paramètres de pare-feu spécifiques que nous n'énumérerons pas ici.

- **Tous - Adaptatif :** ce paramètre de pare-feu définit tous les ports réseau en leur attribuant un 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 :** ce paramètre de pare-feu définit tous les ports réseau comme ouverts (tout le trafic réseau est autorisé). Tous les types de paquets sont autorisés. Toutes les applications réseau sont autorisées à se connecter au réseau.
- **Tous - Fermé :** ce paramètre de pare-feu ferme tous les ports réseau et limite les types de paquets.

Adaptateurs : fait référence à trois adaptateurs de communication situés normalement sur un noeud d'extrémité :

- adaptateurs filaires (connexions LAN) ;
- adaptateurs Wi-Fi (cartes PCMCIA Wi-Fi et radios Wi-Fi intégrées).
- Adaptateurs pour connexion à distance (modems interne et externe)

Fait également référence aux autres équipements de communication qui peuvent être utilisés sur un ordinateur, comme des ports infrarouge, Bluetooth*, Firewire* et ports parallèles et série.

Périphériques de stockage : désigne les périphériques de stockage externes qui peuvent représenter une menace en matière de sécurité lorsque des données sont copiées sur ces périphériques ou transférées depuis ces derniers au niveau d'un noeud d'extrémité. L'accès aux clés USB, aux cartes mémoire flash et SCSI PCMCIA, ainsi qu'aux lecteurs zip*, lecteurs de disquettes et CD-R externes classiques et lecteurs de CD/DVD installés (notamment CD-ROM, CD-R/RW, DVD, DVD R/RW) peut être bloqué, autorisé ou limité en lecture seule à un emplacement unique.

Environnements réseau : il s'agit d'un ensemble de services réseau et d'adresses de service requis pour identifier un emplacement réseau (reportez-vous à la section Section 3.2.1, « Enregistrement d'un environnement réseau », page 16).

2.2 Login à Endpoint Security Client 3.5

Si vous êtes membre du domaine d'entreprise, le client Endpoint Security Client 3.5 utilise votre nom d'utilisateur et votre mot de passe Windows* pour vous loguer au service de distribution de stratégies (Policy Distribution Service) sans afficher de fenêtre contextuelle. Si vous n'êtes pas

membre du domaine qui héberge le service de distribution de stratégies, Endpoint Security Client 3.5 vous invite à entrer votre nom d'utilisateur et votre mot de passe pour ce domaine (voir Figure 2-2).

Figure 2-2 *Login à Endpoint Security Client 3.5*

Entrez votre nom d'utilisateur et mot de passe pour ce domaine, puis cliquez sur *OK*.

Remarque : le login à Endpoint Security Client 3.5 n'est pas nécessaire lorsqu'il est exécuté en mode Non géré. L'administrateur ESM dispose d'une autre méthode pour fournir des stratégies aux utilisateurs non gérés.

Utilisation de Endpoint Security Client 3.5

3

Les sections suivantes contiennent un complément d'informations sur les opérations réalisables à l'aide de l'application destinée aux utilisateurs finaux de Novell® ZENworks® Endpoint Security, à savoir Endpoint Security Client 3.5 :

- Section 3.1, « Déplacement au sein des environnements réseau », page 15
- Section 3.2, « Changement d'emplacement », page 16
- Section 3.3, « Modification des paramètres de pare-feu », page 18
- Section 3.4, « Codage de données », page 19
- Section 3.5, « Mise à jour des stratégies », page 22
- Section 3.6, « Affichage de l'aide », page 23
- Section 3.7, « Octroi d'un mot de passe prioritaire », page 23
- Section 3.8, « Diagnostics », page 24

Remarque : l'administrateur est autorisé à limiter les opérations susmentionnées à n'importe quel emplacement.

3.1 Déplacement au sein des environnements réseau

Chaque réseau parcouru par un utilisateur final peut nécessiter des mesures de sécurité différentes. Endpoint Security Client 3.5 sécurise et protège les emplacements identifiés par des connexions réseau disponibles. Endpoint Security Client 3.5 détecte les paramètres de l'environnement réseau et bascule vers l'emplacement approprié, en appliquant les niveaux de protection nécessaires en fonction de la stratégie de sécurité actuelle.

Les informations d'un environnement réseau peuvent être définies comme étant Stored (Stockées) ou Preset (Prédéfinies) au sein même d'un emplacement. Cela permet à Endpoint Security Client 3.5 de basculer automatiquement vers un emplacement une fois les paramètres de l'environnement détectés.

- **Environnements stockés :** définis par l'utilisateur (reportez-vous à la section Section 3.2.1, « Enregistrement d'un environnement réseau », page 16).
- **Environnements prédéfinis :** définis par l'administrateur ESM de l'entreprise via une stratégie de sécurité publiée

Lorsque l'utilisateur entre dans un nouvel environnement réseau, le client compare l'environnement réseau détecté aux valeurs Stored (Stocké) et Preset (Prédéfini) dans la stratégie de sécurité. Si une correspondance est trouvée, Endpoint Security Client 3.5 active l'emplacement attribué. Si l'environnement détecté ne peut pas être identifié comme un environnement stocké ou prédéfini, le client active l'emplacement Inconnu par défaut.

Les valeurs prédéfinies de l'emplacement Inconnu sont les suivantes :

- Change Locations = Permitted (Changer d'emplacement = Autorisé)
- Change Firewall Settings = Not permitted (Modifier les paramètres de pare-feu = Non autorisé)
- Save Location = Not permitted (Enregistrer un emplacement = Non autorisé)
- Update Policy = Permitted (Mettre à jour une stratégie = Autorisé)
- Paramètres de pare-feu par défaut = Tous - Adaptatif

Les trois types d'adaptateurs (Wi-Fi, filaires et pour connexion à distance) sont autorisés dans l'emplacement Inconnu. Cela permet à l'ordinateur de se connecter à son environnement réseau via des périphériques et d'essayer d'associer une stratégie d'emplacement comme décrit ci-dessus.

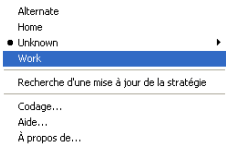
3.2 Changement d'emplacement

Au démarrage, Endpoint Security Client 3.5 bascule vers l'emplacement Inconnu. Il tente ensuite de détecter l'environnement réseau actuel et de changer automatiquement d'emplacement. Si l'environnement réseau n'est pas reconnu ou s'il n'a pas été prédéfini ou enregistré (reportez-vous à la section Section 3.2.1, « Enregistrement d'un environnement réseau », page 16), vous devrez changer d'emplacement manuellement.

Si vous n'avez pas pu effectuer cette procédure, il se peut que votre administrateur ZENworks Endpoint Security Management vous ait interdit de changer les emplacements manuellement.

Pour changer d'emplacement :

1. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu souhaité.



2. Cliquez sur l'emplacement approprié.

3.2.1 Enregistrement d'un environnement réseau

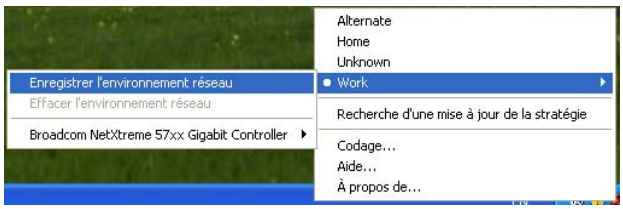
Un environnement réseau doit être prédéfini dans la stratégie de sécurité ou enregistré par l'utilisateur final avant que Endpoint Security Client 3.5 puisse changer automatiquement d'emplacement. L'enregistrement d'un environnement réseau permet de sauvegarder les paramètres réseau à l'emplacement actuel et autorise Endpoint Security Client 3.5 à basculer automatiquement vers cet emplacement lors de la connexion suivante de l'utilisateur à l'environnement réseau. Appliqué dans un environnement réseau Wi-Fi, Endpoint Security Client 3.5 détecte le point d'accès unique sélectionné (LockOn™).

Pour enregistrer un environnement :

1. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu.

2 Cliquez sur l'emplacement auquel vous souhaitez accéder.

3 Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client*, placez le curseur sur l'emplacement actuel pour afficher le sous-menu, puis cliquez sur Enregistrer l'environnement réseau.



Si cet environnement réseau a déjà été enregistré à un autre emplacement, Endpoint Security Client 3.5 demande à l'utilisateur s'il souhaite enregistrer le nouvel emplacement. Cliquez sur *Oui* pour enregistrer l'environnement à l'emplacement actuel et effacer l'environnement de son ancien emplacement ou sur *Non* pour laisser l'environnement à l'emplacement précédent.

Remarque : la fonction *Enregistrer l'environnement réseau* peut être limitée par l'administrateur ESM à n'importe quel emplacement.

D'autres environnements réseau peuvent être enregistrés par la suite au même emplacement. Par exemple, si un emplacement défini comme « Aéroport » fait partie de la stratégie actuelle, chaque aéroport où l'utilisateur mobile s'est rendu peut être enregistré comme environnement réseau pour cet emplacement. Ainsi, chaque fois qu'un utilisateur mobile revient dans un environnement « Aéroport » enregistré, Endpoint Security Client 3.5 bascule automatiquement vers l'emplacement Aéroport.

3.2.2 Enregistrement d'un environnement Wi-Fi

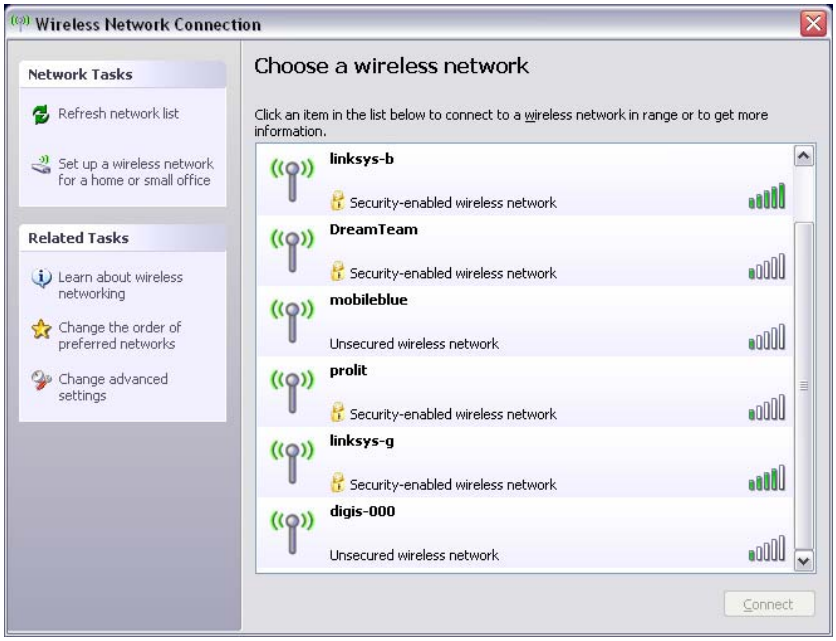
Lorsque les utilisateurs activent leurs adaptateurs Wi-Fi, des dizaines de points d'accès peuvent être disponibles. Il se peut que l'adaptateur Wi-Fi détecte d'abord un seul point d'accès, mais si d'autres points d'accès se trouvent à proximité de l'adaptateur, le premier point d'accès peut être abandonné et le gestionnaire de la connexion sans fil peut demander à l'adaptateur de basculer vers le point d'accès dont le signal est le plus fort. Dans ce cas, l'activité réseau actuelle est arrêtée, obligeant ainsi souvent un utilisateur à renvoyer certains paquets et à reconnecter son réseau privé virtuel au réseau de l'entreprise.

Si un point d'accès est enregistré comme paramètre d'environnement réseau à un emplacement, l'adaptateur détecte ce point d'accès et conserve sa connexion tant qu'il ne s'éloigne pas physiquement du point d'accès. De retour au point d'accès, l'adaptateur s'associe automatiquement à celui-ci, l'emplacement change et le logiciel de gestion des connexions sans fil n'affiche plus tous les autres points d'accès.

Pour enregistrer un environnement Wi-Fi :

1 Lancez le logiciel de gestion des connexions et sélectionnez le point d'accès souhaité.

Remarque : le logiciel de gestion des connexions peut être remplacé en fonction de l'emplacement si la stratégie de sécurité de ESM est définie pour gérer votre connectivité sans fil.



2 Spécifiez toute information nécessaire relative à la sécurité (clé WEP ou autre clé de sécurité), puis cliquez sur *Connecter*.

3 Effectuez la procédure indiquée à la section Section 3.2.1, « Enregistrement d'un environnement réseau », page 16 pour enregistrer cet environnement.

3.2.3 Suppression d'un environnement enregistré

Pour supprimer un environnement réseau enregistré d'un emplacement :

1 Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu.

2 Accédez à l'emplacement approprié.

3 Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client*, puis sélectionnez l'emplacement actuel pour afficher le sous-menu.

4 Cliquez sur *Effacer l'environnement réseau* pour l'effacer.

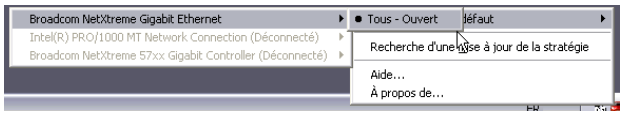
Remarque : cette opération permet d'effacer tous les environnements réseau enregistrés à cet emplacement.

3.3 Modification des paramètres de pare-feu

Chaque emplacement peut se voir attribuer plusieurs paramètres de pare-feu. La modification des paramètres de pare-feu peut ouvrir ou fermer des ports réseau et autoriser ou refuser certains types de réseautique à un emplacement donné.

Pour modifier les paramètres de pare-feu :

1. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu.
2. Placez le curseur de la souris sur l'emplacement actuel pour afficher le sous-menu, puis cliquez sur la sélection pour modifier le paramètre de pare-feu.



Remarque : le nombre de paramètres de pare-feu disponibles à un emplacement est déterminé par la stratégie.

3.4 Codage de données

Après activation via la stratégie, Endpoint Security Client 3.5 gère le codage des fichiers placés dans un répertoire spécifique sur le noeud d'extrémité et de ceux qui se trouvent sur des périphériques de stockage amovibles.

Les instructions suivantes vous permettront d'utiliser ZENworks Endpoint Security Management sur le noeud d'extrémité.

- Section 3.4.1, « Gestion de fichiers sur des disques fixes », page 19
- Section 3.4.2, « Gestion de fichiers sur un support de stockage amovible », page 19

3.4.1 Gestion de fichiers sur des disques fixes

Les disques fixes sont définis comme toutes les unités de disque dur installées sur l'ordinateur et toutes les partitions d'un disque dur. Chaque disque fixe sur le noeud d'extrémité comporte un dossier `Fichiers codés` placé dans le répertoire racine. Tous les fichiers contenus dans ce dossier sont codés à l'aide de la clé de codage actuelle. Seuls les utilisateurs autorisés sur cet ordinateur peuvent décoder ces fichiers.

Lors de l'enregistrement d'un fichier, sélectionnez le dossier `Fichiers codés` dans les dossiers disponibles sur l'unité souhaitée.

3.4.2 Gestion de fichiers sur un support de stockage amovible

Le stockage amovible est défini comme tout périphérique de stockage « connecté » à un ordinateur. Par exemple, il peut s'agir entre autres de clés USB, de cartes mémoire flash et PCMCIA, de lecteurs zip, de lecteurs de disquettes et CD-R externes classiques, d'appareils photo numériques avec capacité de stockage et de lecteurs MP3.

Lorsque ZENworks Endpoint Security Management est en cours d'exécution, les fichiers stockés sur ces périphériques sont codés lorsque le système d'exploitation ou l'utilisateur y accède. Les fichiers copiés sur le périphérique sont immédiatement codés. Si le périphérique de stockage amovible est connecté à un ordinateur qui n'est pas géré par le système ZENworks Endpoint Security Management, les fichiers resteront codés et ne pourront pas être décodés.

Le codage du support de stockage amovible est effectué au moment de la connexion du périphérique (voir « Que faire si je ne souhaite pas coder le périphérique ? » page 21). Toutefois, les fichiers ajoutés sur un périphérique de stockage amovible codé sur une autre machine ne sont pas codés et doivent l'être manuellement.

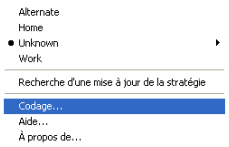
Les sections suivantes contiennent davantage d'informations :

- « Codage de fichiers » page 20
- « Que faire si je ne souhaite pas coder le périphérique ? » page 21
- « Utilisation du dossier Fichiers partagés » page 21
- « Modification du mot de passe des fichiers dans le dossier Fichiers partagés » page 21

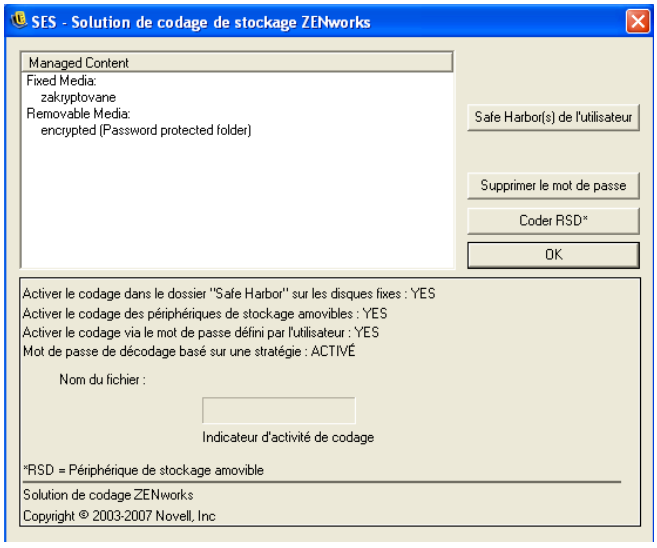
Codage de fichiers

Pour coder des fichiers ajoutés sur un périphérique de stockage amovible, procédez comme suit :

1. Raccordez le périphérique de stockage au port approprié de votre ordinateur.
2. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches.
3. Sélectionnez *Codage* dans le menu.



4. Cliquez sur *Coder RSD*. Cette opération code tous les fichiers sur le périphérique de stockage amovible à l'aide de la clé de codage actuelle.

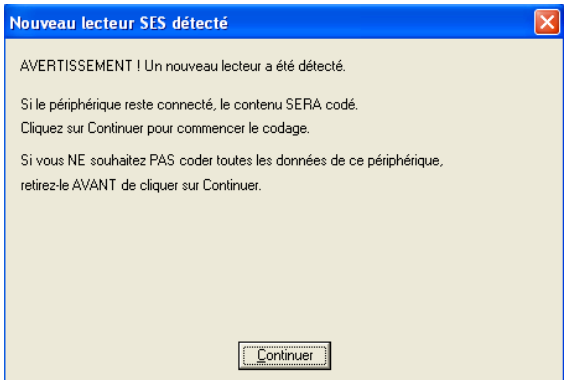


La durée nécessaire pour le codage des fichiers dépend de la quantité de données stockées sur le périphérique.

Que faire si je ne souhaite pas coder le périphérique ?

Lors de la connexion d'un périphérique de stockage amovible, Endpoint Security Client vous demande si vous souhaitez coder le périphérique ou si vous préférez le retirer et ne pas coder la totalité des fichiers.

Figure 3-1 *Message d'avertissement de codage lors de la connexion d'un nouveau périphérique*



Pour ne pas coder le contenu de cette unité, retirez-la avant de cliquer sur *Continuer*. Cliquez sur *Continuer* pour coder l'unité ou pour fermer la fenêtre après le retrait de l'unité.

Utilisation du dossier Fichiers partagés

Lorsque la stratégie le rend accessible, un dossier `Fichiers partagés` est créé sur n'importe quel périphérique de stockage amovible relié à l'ordinateur exécutant ZENworks Endpoint Security Management. Des utilisateurs peuvent accéder aux fichiers de ce dossier dans d'autres groupes de stratégies à l'aide d'un mot de passe qu'ils ont créé. Les utilisateurs qui n'exécutent pas ZENworks Endpoint Security Management accèdent à ces fichiers à l'aide de l'utilitaire de décodage de fichiers ZENworks et d'un mot de passe.

Remarque : les mots de passe sont effacés à chaque redémarrage. Vous êtes invité à entrer un mot de passe pour les fichiers ajoutés au dossier `Fichiers partagés` après un redémarrage.

Pour utiliser le dossier `Fichiers partagés` :

1. Déplacez ou enregistrez un fichier dans le dossier `Fichiers partagés`.
2. Lorsque vous y êtes invité, entrez le mot de passe et confirmez-le.
3. Entrez un indice pour le mot de passe.

Les utilisateurs ZENworks Endpoint Security Management non gérés par votre stratégie peuvent accéder à ces fichiers en entrant ce mot de passe. Les utilisateurs non gérés par ZENworks Endpoint Security Management doivent utiliser l'utilitaire de décodage de fichiers ZENworks ainsi que le mot de passe pour accéder aux fichiers.

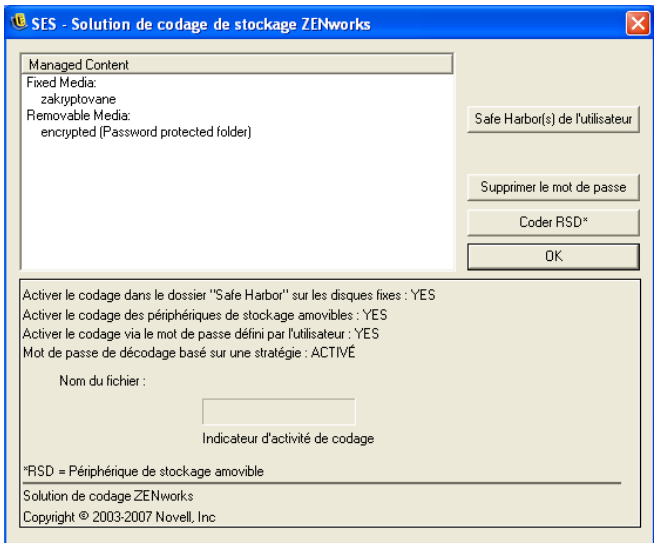
Modification du mot de passe des fichiers dans le dossier Fichiers partagés

Vous pouvez utiliser la commande de codage pour modifier le mot de passe des fichiers ajoutés au dossier `Fichiers partagés`.

Remarque : cette commande ne modifie pas les mots de passe existants, elle s'applique uniquement au mot de passe des fichiers ajoutés.

Pour modifier le mot de passe :

1. Raccordez le périphérique de stockage au port approprié de votre ordinateur.
2. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches.
3. Sélectionnez *Codage* dans le menu.
4. Cliquez sur *Effacer le mot de passe*.



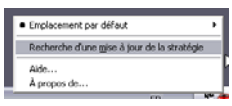
5. Faites glisser un fichier vers le dossier `Fichiers partagés` et entrez le nouveau mot de passe et son indice.

Le nouveau mot de passe est désormais nécessaire pour accéder à tous les nouveaux fichiers ajoutés au dossier.

3.5 Mise à jour des stratégies

Les nouvelles stratégies de sécurité sont envoyées aux utilisateurs gérés dès leur publication. Endpoint Security Client reçoit automatiquement les mises à jour aux intervalles déterminés par l'administrateur ESM. Toutefois, l'utilisateur géré peut rechercher des mises à jour des stratégies lorsqu'il accède à un nouvel emplacement.

1. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu.
2. Cliquez sur *Recherche d'une mise à jour des stratégies*.



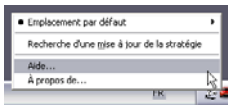
Remarque : Les fonctions de mises à jour automatiques et de recherche de mises à jour des stratégies ne sont pas disponibles si Endpoint Security Client 3.5 est exécuté en mode Non géré. L'administrateur ESM dispose d'une autre méthode pour fournir des mises à jour des stratégies à ces utilisateurs.

Endpoint Security Client 3.5 avertit l'utilisateur en cas de mise à jour de la stratégie.

Remarque : le message `Stratégie mise à jour` s'affichera parfois en changeant de carte d'accès sans fil. La stratégie n'a pas été mise à jour pour autant, Endpoint Security Client 3.5 compare simplement le périphérique aux restrictions figurant dans la stratégie actuelle.

3.6 Affichage de l'aide

1. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu.
2. Cliquez sur *Aide*.



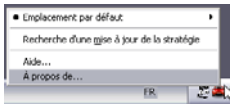
3.7 Octroi d'un mot de passe prioritaire

Il peut arriver que les utilisateurs soient confrontés à des interruptions de productivité résultant des restrictions appliquées à la connectivité, aux logiciels ou aux clés USB qui sont associées à la stratégie de sécurité appliquée par Endpoint Security Client 3.5. 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 à tous les paramètres de pare-feu. Dans pareils cas, les restrictions doivent être temporairement éliminées pour éviter toute interruption de productivité.

Endpoint Security Client 3.5 dispose de la fonction Mot de passe prioritaire qui désactive temporairement la stratégie de sécurité actuelle pour autoriser les activités nécessaires. L'administrateur de sécurité ne distribue une clé de mot de passe à usage unique qu'en cas de besoin et doit être informé de tous les problèmes liés à la stratégie de sécurité. Une fois le délai de la clé de mot de passe expiré, la stratégie de sécurité protégeant le noeud d'extrémité est restaurée. Le redémarrage du noeud d'extrémité restaure également les paramètres de sécurité.

Pour activer la fonction Mot de passe prioritaire :

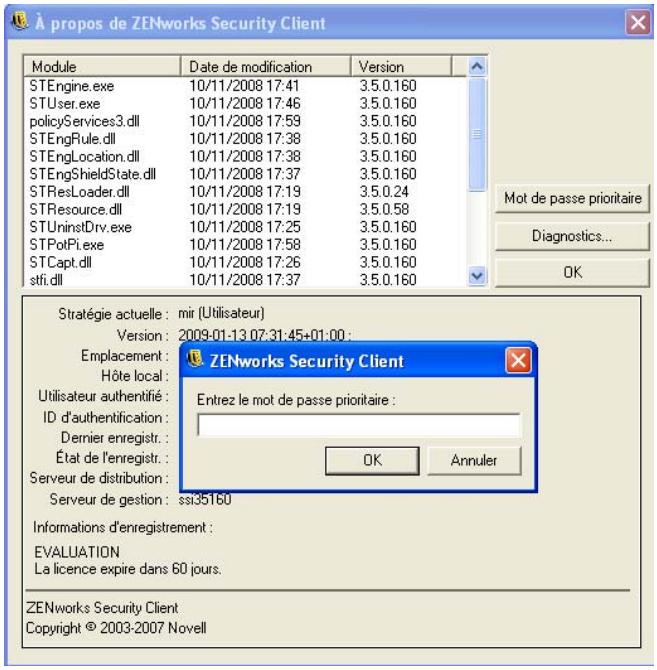
1. Contactez l'administrateur ESM de votre société pour obtenir la clé de mot de passe
2. Cliquez avec le bouton droit de la souris sur l'icône *Endpoint Security Client* dans la barre des tâches pour afficher le menu, puis cliquez sur *À propos de*.



3. Cliquez sur *Mot de passe prioritaire* pour afficher la fenêtre de mot de passe

Remarque : si le bouton *Mot de passe prioritaire* n'apparaît pas sur cet écran, cela signifie que votre stratégie actuelle ne dispose pas de cette fonction.

Figure 3-2 *Fenêtre de mot de passe*



4 Entrez la clé de mot de passe fournie par votre administrateur ZENworks Endpoint Security Management.

5 Cliquez sur *OK*. La stratégie actuelle sera remplacée par une stratégie par défaut Tous - Ouvert pendant la durée spécifiée.

Si vous cliquez sur *Charger la stratégie* (qui remplace le bouton *Mot de passe prioritaire*) dans la fenêtre *À propos de*, la stratégie précédente sera restaurée. Si votre administrateur a mis à jour votre stratégie pour résoudre les problèmes existants, vous devrez plutôt utiliser l'option *Recherche d'une mise à jour des stratégies* pour télécharger immédiatement la nouvelle stratégie.

3.8 Diagnostics

Novell propose des outils de diagnostic pour permettre à l'administrateur de résoudre les problèmes liés à Endpoint Security Client 3.5. Votre administrateur ZENworks Endpoint Security Management vous guide tout au long du processus de diagnostic.