conpal LAN Crypt

intelligent
hautement sécurisé
persistant

Manuel admin

Version du produit: 3.97
Date du document: Mai 2019

Table des matières

1 Aperçu

1.1 Qu'est-ce que conpal LAN Crypt ?

conpal LAN Crypt fournit un chiffrement transparent des fichiers. Il a été conçu pour permettre l'échange confidentiel de données entre utilisateurs au sein d'une grande entreprise. Dans ce cas, les fichiers chiffrés peuvent être stockés de façon locale, sur le disque dur de l'utilisateur ou sur un support amovible, voire sur un lecteur réseau.

Le processus de chiffrement reste transparent du point de vue de l'utilisateur. Il se produit de façon automatique lorsque les fichiers sont créés ou enregistrés. Ces fichiers sont également déchiffrés de façon transparente lorsque leurs données sont lues. Ce processus est exécuté par un pilote de filtre qui est intégré dans le système de fichiers de Windows. Le pilote de filtre conpal LAN Crypt fonctionne de la même façon qu'un antivirus : il identifie les fichiers auxquels accéder et réalise sur ceux-ci l'opération de chiffrement ou de déchiffrement appropriée.

Chaque fois qu'un utilisateur déplace un fichier dans un répertoire sécurisé, ce fichier est chiffré dans l'ordinateur de l'utilisateur et chaque fois qu'un autre utilisateur digne de confiance, membre du groupe, lit le fichier à partir de ce répertoire, il est transféré à cet utilisateur sous forme chiffrée. Le fichier n'est pas déchiffré jusqu'à son transfert dans l'ordinateur cible où l'utilisateur peut le modifier. Il est ensuite de nouveau chiffré avant son retour dans le répertoire chiffré.

Les fichiers chiffrés ne sont pas "assignés" à des utilisateurs individuels. Tout utilisateur qui possède la bonne clé peut accéder au fichier chiffré. Les administrateurs peuvent ainsi créer des groupes d'utilisateurs logiques bénéficiant d'un accès partagé aux fichiers chiffrés. Cette procédure est comparable au jeu de clés dont vous vous servez tous les jours : conpal LAN Crypt offre aux utilisateurs et groupes d'utilisateurs un jeu de clés et chaque clé sert à ouvrir une porte ou un coffre-fort particulier.

Les utilisateurs non autorisés peuvent accéder physiquement aux fichiers chiffrés, mais uniquement à partir de postes de travail non équipés de conpal LAN Crypt. Cependant, sans autorisation conpal LAN Crypt, ils ne pourront pas les lire.

Par conséquent, un fichier est toujours protégé même si aucune protection d'accès n'est définie pour le système de fichiers lui-même, en cas d'attaque du réseau ou du non-respect de la stratégie de sécurité de l'entreprise.

Si vous devez protéger votre propriété intellectuelle, stockée sur fichiers, d'un accès non autorisé via le réseau local, sur des serveurs de fichiers, des disques locaux ou même des supports amovibles, conpal LAN Crypt est le produit idéal.

Le responsable de la sécurité peut spécifier les fichiers et les dossiers à protéger avec conpal LAN Crypt, de façon centralisée, en définissant une ou plusieurs règles de chiffrement. Par exemple, pour s'assurer que tous les documents Word sont protégés, le SO peut définir la règle *.doc. Dès que cette règle sera déployée sur le système du client dans le cadre d'un fichier de

stratégie, tous les documents Word seront chiffrés, quel que soit leur lieu de stockage. Si nécessaire, plusieurs règles de chiffrement peuvent être associées pour former un profil de chiffrement.

Dans cet exemple, trois règles ont été réunies dans un profil :

Règle	Clé	Description
*.doc	Clé1	Chiffre tous les documents Word avec clé1, quel que soit leur lieu de stockage.
D:\Données*.*	Clé2	Chiffre tous les fichiers du dossier spécifié avec clé2.
\\Serveur1\Partage1\Personnel*.xls	Clé3	Chiffre tous les fichiers Excel du dossier serveur spécifié avec clé3.

Avec conpal LAN Crypt, le responsable de la sécurité est en mesure de définir des règles complexes pour s'assurer que seules les données requises soient chiffrées à des emplacements spécifiques. Ces règles sont déployées sous forme de fichiers de stratégie qui peuvent être stockés sur un serveur de fichiers ou dans le dossier Netlogon d'un contrôleur de domaine Windows. Le responsable de la sécurité peut adapter la stratégie en fonction de l'utilisateur en cliquant simplement sur un bouton. Cette stratégie regroupe toutes les clés et les règles qui s'appliquent à cet utilisateur.

L'interface graphique conpal LAN Crypt Administration permet au responsable de la sécurité de créer et gérer ces fichiers de stratégie. Ensuite, MMC (Microsoft Management Console) sert d'interface pour les fichiers ainsi créés. Les composants logiciels enfichables offrent au responsable de la sécurité toute une gamme d'outils qui permettent de lui faciliter la tâche.

Les fichiers de stratégie sont chiffrés au cas par cas, par l'intermédiaire de certificats, pour chaque utilisateur. Ce processus a recours à l'infrastructure de clés publiques (PKI), qui est déjà en place dans l'entreprise. En outre, le responsable de la sécurité peut également créer des certificats à l'aide de conpal LAN Crypt.

Les données d'administration de conpal LAN Crypt sont alors stockées dans la base de données SQL. Naturellement, tous les enregistrements de données importantes sont chiffrés dans la base de données SQL, notamment les données relatives aux clés. Dans la mesure où la base de données utilisée ici ne dépend pas de la fonctionnalité d'administration du système, il reste possible de compartimenter les fonctionnalités de sécurité et d'administration du système. conpal LAN Crypt permet également de configurer plusieurs rôles de responsable de la sécurité, dont les autorisations peuvent être adaptées en fonction des tâches à accomplir.

Le responsable principal de la sécurité est la seule personne qui dispose de toutes les autorisations. En outre, le responsable de la sécurité peut également déléguer les autorisations requises pour

gérer conpal LAN Crypt et par conséquent mettre en place une hiérarchie administrative adaptée à la structure organisationnelle de l'entreprise.

1.2 Protection des données avec conpal LAN Crypt

conpal LAN Crypt garantit que les fichiers sensibles peuvent être stockés en toute sécurité sur des serveurs de fichiers et des postes de travail. Les données sont transférées de manière sécurisée sur des réseaux LAN ou WAN et les processus de chiffrement et de déchiffrement sont exécutés dans la mémoire RAM du poste de travail client. Il n'est pas nécessaire d'installer un logiciel de sécurité spécial sur le serveur de fichiers lui-même.

Les fichiers de stratégie contiennent l'ensemble des règles, droits d'accès et clés nécessaires à un chiffrement transparent.
Avant que les utilisateurs ne puissent chiffrer/déchiffrer les données à l'aide du logiciel conpal LAN Crypt installé sur le poste de travail client, ils doivent pouvoir accéder au fichier de stratégie. Ce fichier est sécurisé par l'intermédiaire d'un certificat. Pour accéder au fichier de stratégie, l'utilisateur doit disposer de la clé privée du certificat approprié.

Toutes les tâches de chiffrement/déchiffrement sont exécutées de manière transparente sur le poste de travail client avec le minimum d'interaction de l'utilisateur.

conpal LAN Crypt permet d'organiser les utilisateurs de confiance en plusieurs groupes du même type. Il s'agit de définir des droits d'accès différents aux répertoires et aux fichiers. Ces droits sont regroupés dans des profils de chiffrement destinés aux utilisateurs. L'utilisateur peut accéder au fichier de stratégie contenant le profil de chiffrement s'il dispose de la clé privée assignée au certificat.

Tous les utilisateurs conpal LAN Crypt dont le fichier de stratégie contient le même profil de chiffrement sont membres d'un groupe de confiance. Ils n'ont pas à se préoccuper du chiffrement ni de l'échange de la clé. Ils doivent simplement pouvoir accéder aux fichiers de stratégie pour que leurs données soient chiffrées ou déchiffrées en toute transparence, à l'ouverture ou à la fermeture.

Du fait que les profils de chiffrement sont répartis via des fichiers de stratégie, toutes les formes organisationnelles peuvent être cartographiées depuis un modèle LAN centralisé dans lequel les utilisateurs sont administrés de manière centrale, vers un modèle distant dans lequel les utilisateurs travaillent sur des ordinateurs portables.

conpal LAN Crypt Administration et Administration Windows

Un ordinateur d'administration distinct est utilisé pour configurer conpal LAN Crypt et gérer les profils de chiffrement. Pour établir une distinction nette entre l'administration Windows et l'administration conpal LAN Crypt, il faut définir le rôle du responsable de la sécurité. Le responsable de la sécurité définit les profils de chiffrement des fichiers de stratégie afin d'indiquer

quelles données chiffrées doivent être stockées dans des répertoires particuliers et qui est autorisé à accéder à ces données. Une fois les fichiers de stratégie créés sur la station d'administration, le responsable de la sécurité les déploie.

Un outil Windows standard, la console de gestion MMC de Microsoft, sert à administrer conpal LAN Crypt. L'interface utilisateur de conpal LAN Crypt Administration comprend les composants logiciels enfichables pour la console MMC. conpal LAN Crypt Administration stocke la plupart des objets à administrer (données utilisateur, clés, chemins de chiffrement, etc.) dans leurs propres bases de données.

L'utilisation des bases de données présente deux avantages notables par rapport aux outils Windows du type Active Directory :

- Il est possible de maintenir strictement séparées l'administration du système et l'administration de la sécurité. Cela s'explique par le fait que conpal LAN Crypt utilise une base de données dédiée et se révèle totalement indépendant de l'administration du système. La base de données conpal LAN Crypt est alors chiffrée, puis protégée contre tout accès non autorisé. En outre, cette base de données prévient les changements non intentionnels du système conpal LAN Crypt (par exemple si l'administrateur système supprime un objet de sécurité nécessaire).

- D'autre part, il n'est pas toujours judicieux de laisser des personnes, autres que les administrateurs dédiés, modifier la configuration du système. L'assignation d'une autorisation d'écriture de données dans le cadre d'une administration de système pose évidemment un véritable problème. Il existe une autre bonne raison justifiant le stockage des données spécifiques à conpal LAN Crypt dans une base de données séparée.

Pour offrir la meilleure protection possible, les fonctions conpal LAN Crypt sont divisées en deux parties :

- Fonctions d'utilisateur conpal LAN Crypt

  Concernant les données, les fonctions d'utilisateur conpal LAN Crypt intègrent le chiffrement et le déchiffrement des informations.
  Celles-ci servent aux tâches qui utilisent conpal LAN Crypt au quotidien. Dès qu'un utilisateur est autorisé à accéder aux informations de chiffrement, les fichiers sont chiffrés et déchiffrés de manière transparente. Aucune autre interaction utilisateur n'est requise.
  Par ailleurs, conpal LAN Crypt possède un large éventail de fonctions d'affichage permettant aux utilisateurs de visualiser "leur" profil de chiffrement.

- Fonctions de responsable de la sécurité conpal LAN Crypt

  conpal LAN Crypt Administration possède des fonctions réservées aux responsables de la sécurité.
  Une condition préalable à la création de profils de chiffrement et à l'administration des profils de chiffrement existants est de disposer d'un certificat de responsable de la sécurité.
  Le composant conpal LAN Crypt Administration peut être installé séparément de l'application de l'utilisateur du fait que seul un responsable de la sécurité doit pouvoir y accéder.

Lorsque vous installez conpal LAN Crypt, vous pouvez sélectionner les composants souhaités (administration et/ou utilisateur).

1.3 Chiffrement transparent

Pour l'utilisateur, le chiffrement transparent signifie que toutes les données stockées sous forme chiffrée (dans des répertoires ou lecteurs sécurisés) sont automatiquement déchiffrées dans la mémoire RAM lorsqu'elles sont ouvertes par une application. Lorsque le fichier est enregistré, il est automatiquement chiffré à nouveau.

- Chaque fichier associé à une règle de chiffrement fait l'objet d'un chiffrement automatique.
- Si des fichiers sont copiés ou déplacés vers un répertoire sécurisé, ils sont chiffrés conformément à la règle de chiffrement applicable à ce répertoire. Vous pouvez naturellement définir des règles de chiffrement différentes pour des extensions ou des noms de fichiers différents dans le même répertoire. Le chiffrement n'est pas spécifique aux répertoires. Il dépend totalement des règles de chiffrement !
- Lorsque des fichiers chiffrés sont renommés, ils restent chiffrés (sous réserve de la présence d'une règle de chiffrement différente ou de l'absence de règle pour le nouveau nom/la nouvelle extension de fichier).
- Si vous copiez ou déplacez des fichiers chiffrés vers un emplacement où ne s'applique plus la règle de chiffrement en cours, ils resteront chiffrés si un chiffrement persistant est activé par défaut.
- Si vous copiez ou déplacez des fichiers chiffrés vers un emplacement où s'applique une règle de chiffrement différente de celle en cours, ces fichiers seront tout d'abord déchiffrés puis chiffrés à nouveau d'après la nouvelle règle de chiffrement.
- Le chiffrement transparent s'applique à toutes les opérations sur fichiers. L'utilisateur ignore totalement ces procédés pendant qu'il travaille avec les données chiffrées parce qu'ils sont tous exécutés en arrière-plan.
- Le chiffrement persistant peut permettre d'éviter tout déchiffrement accidentel lors de la copie ou du déplacement de fichiers, avec l'Explorateur Windows, vers un dossier ne disposant pas de règle de chiffrement. Cependant, ce mécanisme n'entre pas en jeu lorsque le fichier est copié ou déplacé avec tout autre outil que l'Explorateur.

1.3.1 Accès aux données chiffrées

Si l'utilisateur ne dispose pas de la clé appropriée, il n'a pas accès aux données chiffrées du répertoire. L'utilisateur ne peut pas lire, copier, déplacer, renommer les fichiers de ce répertoire ni même avoir une interaction quelconque.

Cependant, l'utilisateur peut accéder à ces fichiers s'il possède la clé ayant servi à les chiffrer même si son profil de chiffrement ne contient pas de règle de chiffrement pour ces fichiers.

Remarque : Dans le cas de fichiers ouverts uniquement avec la clé disponible (sans règle de chiffrement), vous pouvez les stocker en les enregistrant sous forme de données non chiffrées. Cela se produit lorsque des applications créent un fichier temporaire, détruisent le fichier source puis renomment le fichier temporaire au moment de son enregistrement. Comme il n'existe pas de règle de chiffrement pour le nouveau fichier, ses données sont enregistrées sans être chiffrées.

1.3.2 Changement de nom ou déplacement des répertoires

Pour des raisons de performance, conpal LAN Crypt ne modifie pas le statut de chiffrement lorsque des répertoires entiers sont déplacés avec l'Explorateur Windows. Par conséquent, aucune procédure de chiffrement/déchiffrement/rechiffrement n'est effectuée en cas de déplacement d'un répertoire.

Les fichiers chiffrés le restent lorsqu'ils sont déplacés vers un nouveau répertoire ou un nouvel emplacement mémoire. Si l'utilisateur détient la clé adéquate, il peut continuer de travailler avec ces fichiers comme d'habitude.

Déplacement des fichiers et répertoires en toute sécurité

conpal LAN Crypt est également capable de déplacer les fichiers et répertoires de manière sécurisée. Dans ce cas, les fichiers et répertoires sont chiffrés, déchiffrés puis rechiffrés conformément aux règles de chiffrement en cours. Les fichiers sources sont supprimés ("nettoyés") en toute sécurité après avoir été déplacés.

Cette fonction est accessible via la commande **Déplacement sécurisé** dans le menu contextuel de l'Explorateur Windows. Dans la boîte de dialogue vous sélectionnez l'emplacement vers lequel les fichiers seront déplacés.

1.3.3 Déchiffrement explicite des fichiers

Pour déchiffrer un fichier, il suffit de le copier ou le déplacer vers un répertoire ne comportant pas de règle de chiffrement. Le fichier est automatiquement déchiffré.

Cependant, cela se produit uniquement si :

- un profil de chiffrement adapté a été chargé ;
- l'utilisateur possède la bonne clé ;
- aucune règle de chiffrement pour le nouvel emplacement n'existe dans le profil de chiffrement actif ;
- le chiffrement persistant est désactivé.

1.3.4 Suppression des fichiers chiffrés - Corbeille Windows

Si votre profil de chiffrement est chargé, vous pouvez supprimer tout fichier chiffré dont vous possédez la clé.

Remarque : la suppression des fichiers signifie que vous les envoyez dans la Corbeille Windows. Pour offrir le niveau de sécurité le plus élevé, les fichiers chiffrés par conpal LAN Crypt restent chiffrés dans la Corbeille. Aucune touche n'est nécessaire pour vider la Corbeille.

1.3.5 Fichiers/répertoires exclus du chiffrement

Les fichiers et répertoires suivants sont automatiquement exclus du chiffrement (même si une règle de chiffrement a été définie pour ces fichiers) :

- Fichiers dans le répertoire d'installation conpal LAN Crypt
- Fichiers dans le répertoire d'installation Windows
- Cache du fichier de stratégie
  L'emplacement est indiqué dans conpal LAN Crypt Administration et il est affiché sur l'onglet **Profil** de la boîte de dialogue **État**.
- Répertoire racine du lecteur Système. Les sous-dossiers ne sont pas exclus.
- Emplacements indexés (search-ms)

1.3.6 Chiffrement persistant

Un responsable de la sécurité peut configurer le chiffrement persistant pour conpal LAN Crypt. Les fichiers demeurent chiffrés tant qu'ils sont soumis à une règle de chiffrement.

Par exemple, si un utilisateur copie un fichier chiffré dans un dossier qui n'est associé à aucune règle de chiffrement, ce fichier sera enregistré en clair dans le dossier cible. En activant le chiffrement persistant, vous êtes sûr que les fichiers restent chiffrés lorsqu'ils sont déplacés ou copiés.

Pour éviter la création non intentionnelle de copies brutes de fichiers chiffrés, les copies des fichiers chiffrés seront créées chiffrées même si elles sont créées dans des emplacements non couverts par une règle de chiffrement.

Les responsables de la sécurité peuvent désactiver ce comportement dans conpal LAN Crypt Configuration. S'il est désactivé, les fichiers sont créés en texte brut lorsqu'ils sont copiés/déplacés dans un emplacement non couvert par une règle de chiffrement.

Pour le chiffrement persistant, les règles suivantes s'appliquent :

- Le pilote conpal LAN Crypt conserve uniquement le nom du fichier sans aucune information sur le chemin. Ce nom peut uniquement être utilisé à des fins de comparaison. Par conséquent, ils détecteront uniquement les situations dans lesquelles les noms du fichier source et du fichier cible sont identiques. Si le fichier est renommé pendant la copie, le fichier copié est considéré comme étant un fichier 'différent'. Il n'est donc pas soumis au chiffrement persistant.
- Lorsqu'un utilisateur enregistre un fichier chiffré avec Enregistrer sous sous un nom de fichier différent dans un emplacement non couvert par une règle de chiffrement, le fichier sera en texte brut.
- Les informations sur les fichiers sont conservées pendant une durée de temps limitée uniquement. Si l'opération dure trop longtemps (plus de 15 secondes) le nouveau fichier créé est considéré comme étant un fichier différent et ne sera donc pas soumis au chiffrement persistant.

1.3.6.1 Chiffrement persistant et règle de chiffrement

Comme mentionné précédemment, le chiffrement persistant s'assure qu'un fichier chiffré conserve son état de chiffrement (par exemple, sa clé de chiffrement originale). Ceci est parfaitement normal si le fichier est déplacé dans un dossier sur lequel aucune stratégie de chiffrement ne s'applique. En revanche, si le fichier est copié ou déplacé à un endroit sur lequel s'applique une stratégie de chiffrement, cette dernière est prioritaire et prévaut sur le chiffrement persistant. Le fichier va donc être chiffré à l'aide de la clé définie dans la règle de chiffrement et non pas avec celle utilisée la première fois.

1.3.6.2 Chiffrement persistant et règle Ignorer le chemin

Une règle Ignorer le chemin remplace également le chiffrement persistant. De cette manière, les fichiers chiffrés copiés dans un dossier avec une règle Ignorer le chemin applicable sont archivés en text clair.

Une règle Ignorer le chemin est généralement activée pour les fichiers utilisés très fréquemment et qui ne nécessitent pas de chiffrement. Elle accroît les performances du système.

1.3.6.3 Chiffrement persistant et règle Exclure le chemin

Une règle Exclure le chemin remplace également le chiffrement persistant. De cette manière, les fichiers chiffrés copiés dans un dossier avec une règle Exclure le chemin applicable sont archivés en texte clair.

1.3.7 Limites du chiffrement persistant

Pour des raisons techniques, le chiffrement persistant présente certaines limites. En d'autres termes, le résultat du chiffrement persistant ne répond pas toujours aux attentes de l'utilisateur.

Retrouvez quelques-uns des cas de figure les plus usuels au cours desquels le chiffrement persistant atteint ses limites.

Les fichiers qui ne sont pas supposés rester clairs sont chiffrés

- Les fichiers CLAIRS sont copiés à divers endroits en appliquant ou pas les règles de chiffrement.

  Si un fichier en texte clair est copié à divers endroits en même temps et qu'une règle de chiffrement s'applique sur l'un de ces endroits, il se peut que les autres copies du même fichier soient également chiffrées même si le fichier d'origine ne l'est pas. Si le fichier est copié à un endroit chiffré en premier lieu, ce fichier est ajouté à la liste interne de pilotes. Lorsque la seconde copie est créée à un autre endroit, le pilote retrouve le nom du fichier dans sa liste et chiffre également la seconde copie.

- Création d'un fichier avec le même nom après accès à un fichier chiffré

  Si un fichier chiffré est ouvert (accédé) et qu'un nouveau fichier portant le même nom est créé peu de temps après, le nouveau fichier sera chiffré avec la même clé que celle du premier fichier ouvert.

  Remarque : ceci s'applique uniquement si la même application ou le même thread est utilisé pour lire le fichier chiffré et pour créer le nouveau fichier.

  Cas de figure le plus courant : dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur un dossier ayant une règle de chiffrement et cliquez sur **Nouveau** > **Nouveau document texte**. Cliquez avec le bouton droit de la souris sur un dossier n'ayant pas de règle de chiffrement et cliquez sur **Nouveau** > **Nouveau document texte**. Le second fichier va également être chiffré.

Les fichiers sont non chiffrés

- Plusieurs copies d'un fichier sont créés

  Si les copies d'un fichier chiffré sont créées dans le même dossier que celui du fichier original, ces copies ne sont pas chiffrées. Les copies créées ayant différents noms de fichier (par exemple doc.txt vs. doc - Copy.txt), la correspondance de nom de fichier échoue et ceux-ci ne sont pas chiffrés par le chiffrement persistant.

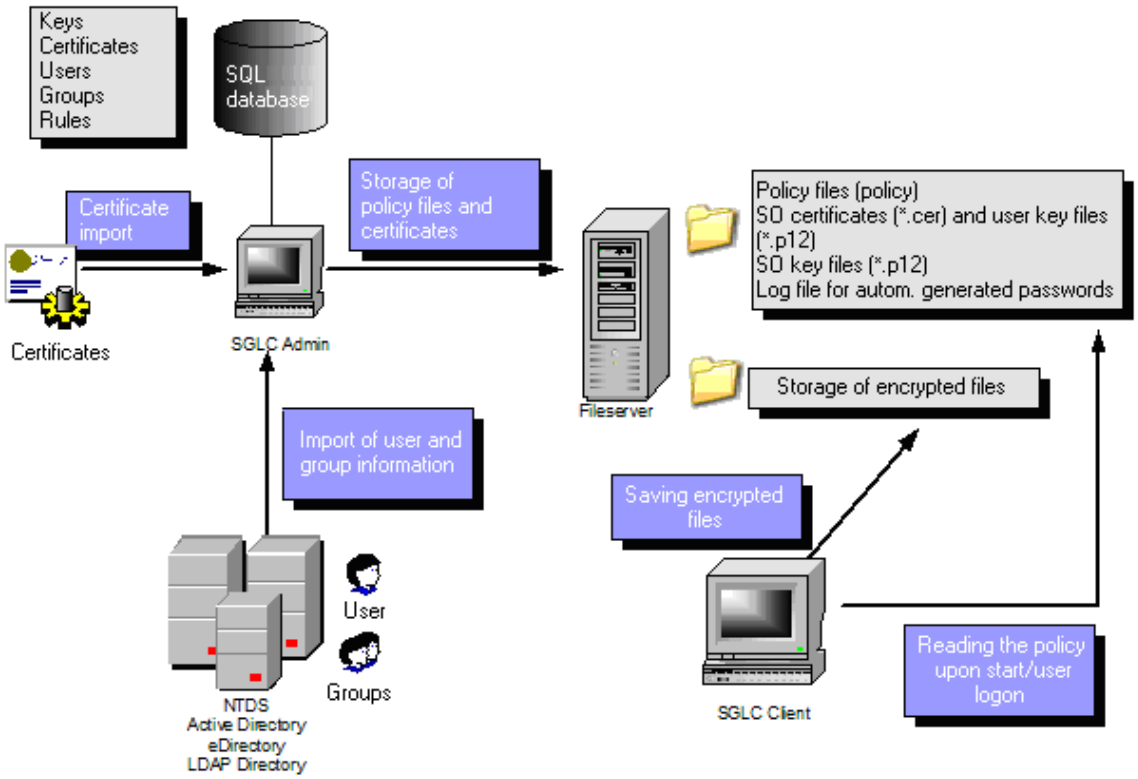
1.3.8 API Client et balises de chiffrement pour les produits de prévention de fuites de données

Si un produit de prévention des fuites de données (DLP ou Data Leakage Prevention) identifie des données nécessitant une opération de chiffrement, il utilise l'API de conpal LAN Crypt Client pour chiffrer ces fichiers. Dans conpal LAN Crypt Administration, vous pouvez définir différentes balises de chiffrement qui indiqueront la clé conpal LAN Crypt à utiliser.

L'API Client utiliser des balises de chiffrement prédéfinies afin d'appliquer des clés spéciales selon le contenu. Par exemple, la balise de chiffrement <CONFIDENTIEL> est utilisée pour chiffrer tous les fichiers que votre produit DLP considère comme étant confidentiels.

1.4 Architecture

conpal LAN Crypt consiste en deux composants : conpal LAN Crypt Administration et conpal LAN Crypt Client. Ces deux composants sont généralement installés sur un poste de travail ordinaire sous Windows XP, Windows Vista ou Windows 7. conpal LAN Crypt Administration permet aux responsables de la sécurité de définir et distribuer des profils de chiffrement. Cette illustration indique comment les différents composants interagissent et comment conpal LAN Crypt est intégré dans un réseau d'entreprise.



1.4.1 conpal LAN Crypt Administration

Les composants d'administration disposent des outils nécessaires pour l'administration centralisée de conpal LAN Crypt, qui peuvent être utilisés par un ou plusieurs responsables de la sécurité. Ces composants sont généralement installés sur un ou plusieurs ordinateurs, sous Windows XP, Windows Vista ou Windows 7. Ils peuvent également être installés sur un système Windows 2003 Server si vous souhaitez procéder à des tâches d'administration centrale avec Windows Terminal Server ou Citrix MetaFrame. Cette configuration est particulièrement adaptée aux grands réseaux, notamment lorsque les sites sont dispersés. Dans ce cas, SGLC Administration est accessible à l'aide du protocole RDP (Remote Desktop) ou ICA (Independent Computing Architecture).

Dans la mesure où le niveau maximum de sécurité et de confidentialité des données ne peut être garanti que si SGLC Administration et l'administration système fonctionnent de façon indépendante, SGLC dispose de fonctionnalités distinctes d'administration des utilisateurs et des groupes. Pour faciliter les tâches quotidiennes, les utilisateurs et les groupes gérés par conpal LAN Crypt peuvent être importés à partir des services d'annuaire Active Directory ou de tout autre annuaire de type LDAP.

conpal LAN Crypt Administration nécessite une base de données SQL pour stocker les données de configuration et gérer les utilisateurs et les groupes SGLC. Cette base de données peut être installée de façon locale sur le système d'administration si MSDE (Microsoft Express Edition) est utilisé. Pour les grandes installations, qui ont recours à plusieurs responsables de la sécurité, nous recommandons d'utiliser un système de base de données central avec une structure similaire à Microsoft SQL ou Oracle Server.

Les responsables de la sécurité ont pour fonction de définir la stratégie de sécurité de leur entreprise. Ils spécifient les stratégies et suivent leur mise en œuvre, leurs modifications et le respect de ces dernières. Les petites entreprises ne disposent généralement que d'un seul responsable de la sécurité. Par contre, les entreprises de plus grande taille disposent généralement de plusieurs responsables de la sécurité répartis dans différents services et appartenant à une hiérarchie. conpal LAN Crypt permet de représenter et tenir compte des différents niveaux hiérarchiques induits par cette situation. Le rôle responsable principal de la sécurité est au sommet de la structure décisionnelle : ce rôle, qui peut être occupé par plusieurs personnes, doit être défini avant la génération de la base de données de conpal LAN Crypt. Ces responsables définissent les stratégies de référence et décident si le principe des "deux personnes" (deux personnes indispensables pour l'authentification) doit s'appliquer aux décisions relatives à la sécurité. Tout responsable de la sécurité dispose d'autorisations de gestion qui permettent de cadrer ses droits fondamentaux. Leur domaine de responsabilité peut également être restreint à des groupes d'utilisateurs au moyen de listes de contrôle d'accès (ACL, Access Control List).
conpal LAN Crypt a recours aux clés de chiffrement par clé pour gérer les droits d'accès des utilisateurs. Ces clés sont chiffrées et stockées dans la base de données SQL et, comme tout autre contenu de base de données, sont protégées contre les modifications par des valeurs MAC et de hachage. Les tâches d'administration sont organisées de telle façon que le responsable de la sécurité peut connaître le nom d'une clé, mais pas sa valeur. Ainsi, ils peuvent manipuler des objets clé et créer des règles de chiffrement. La souplesse des procédures de contrôle des autorisations permet de couvrir la plupart des scénarios. Par exemple, un chef de section peut définir des clés et assigner des dossiers. Lors de l'étape suivante, le responsable de la sécurité génère de façon centrale le profil de chiffrement. Ainsi, les clés restent contrôlées de façon centralisée.

conpal LAN Crypt permet de détecter deux types de clé générés de façon automatique : les clés utilisateur et de groupe. Les clés utilisateur sont générées pour des individus et peuvent être reprises par des règles de chiffrement, telles que des règles de chiffrement des répertoires racine ou des dossiers locaux ou temporaires. Tout utilisateur ne dispose que d'une et une seule clé. Si les données protégées par une clé utilisateur doivent être restaurées de façon urgente, le

responsable de la sécurité doit assigner cette clé à un autre utilisateur. Ce type de restauration nécessite une autorisation administrative spéciale et peut être lié au "principe des deux personnes" (approbation par une deuxième personne) de façon à prévenir tout risque d'utilisation malveillante. Un concept similaire s'applique aux groupes d'utilisateurs : la clé de groupe.

Les fichiers de stratégie contiennent l'ensemble des règles, droits d'accès et clés nécessaires à un chiffrement transparent. Pour qu'un utilisateur puisse chiffrer ou déchiffrer des données à l'aide du logiciel conpal LAN Crypt installé sur le poste de travail client, il doit pouvoir accéder aux informations de chiffrement du fichier de stratégie. Dans ce cas, les fichiers de stratégie sont stockés sur un serveur de fichiers ou dans un dossier partagé du contrôleur de domaine (Netlogon).

Remarque : Il n'est pas nécessaire d'installer les composants conpal LAN Crypt sur les serveurs de fichiers ou les contrôleurs de domaine.

Le fichier de stratégie est protégé contre les accès non autorisés par un certificat. Seul le titulaire du certificat a accès à la clé privée de ce dernier et peut par conséquent utiliser le certificat pour accéder aux informations de chiffrement nécessaires. Dans le cas des certificats autosignés, ces derniers sont également stockés sur un serveur de fichiers et l'utilisateur doit disposer de droits d'accès en lecture pour utiliser ces certificats. conpal LAN Crypt prend également en charge l'utilisation des certificats stockés sur des cartes à puce, des clés cryptographiques USB ou toute autre carte matérielle adaptée.

Remarque : Vous pouvez utiliser conpal LAN Crypt sans nécessairement recourir à des cartes à puce ou des clés cryptographiques pour stocker les certificats.

Les chemins vers les fichiers de stratégie (du point de vue de l'utilisateur) et d'autres paramètres conpal LAN Crypt sont identifiés par des mécanismes présents dans le système d'exploitation.

Un groupe de confiance conpal LAN Crypt se compose de différents utilisateurs disposant du même profil de chiffrement. Les fichiers de stratégie de chaque utilisateur sont générés dans Administration. Tous les utilisateurs de conpal LAN Crypt qui disposent du même profil dans leur fichier de stratégie appartiennent à un groupe d'autorisation. Ils n'ont pas à se préoccuper du chiffrement ni de l'échange de la clé. Ils doivent simplement pouvoir accéder au fichier de stratégie pour que leurs données soient chiffrées ou déchiffrées en toute transparence, à l'ouverture ou à la fermeture.

1.4.2 conpal LAN Crypt Client

conpal LAN Crypt Client est installé sur les systèmes Windows (PC, postes de travail, ordinateurs portables, serveur Terminal Server) à chiffrer. Outre le pilote de filtre requis pour le chiffrement et le déchiffrement, le composant client dispose de plusieurs autres composants en option :

- Extensions propres à l'Explorateur Windows pour le chiffrement explicite initial.

- Une application utilisateur pour charger et supprimer les règles de chiffrement, et activer ou désactiver le chiffrement.
- Une application utilisateur pour afficher tous les paramètres et les règles qui sont actifs sur le client.
  Ceci est par exemple important pour les cas de support.
- Une application utilisateur pour le chiffrement initial.
- Prise en charge des clés cryptographiques, de façon à pouvoir utiliser les certificats liés à des clés cryptographiques pour accéder aux informations de chiffrement.

Le composant client commence par charger le profil créé par le responsable de la sécurité. Il déchiffre ensuite ce profil et en dérive les règles de chiffrement à appliquer à l'utilisateur qui est connecté. Ces règles sont ensuite appliquées par le pilote de filtre installé. Pour qu'un utilisateur puisse accéder à son profil de chiffrement, le certificat qui lui est assigné doit être présent sur son ordinateur ou doit pouvoir être chargé à partir d'un serveur de fichiers ou d'un dossier Netlogon partagé. Ces certificats doivent être fournis au préalable par un responsable de la sécurité, puis importés par l'utilisateur qui les demande. conpal LAN Crypt dispose également d'une option permettant d'importer les certificats de façon automatique lors du premier chargement d'un profil utilisateur.

Dans ce cas, l'utilisateur doit entrer un code confidentiel avant de procéder à l'importation du certificat. Le code confidentiel est fourni par l'administrateur de sécurité. Une vérification du certificat est effectuée à chaque chargement du profil de chiffrement. Si le certificat est valide, l'utilisateur peut se connecter à conpal LAN Crypt. En l'absence de tout certificat valide, l'utilisateur ne peut pas accéder aux données chiffrées. Lorsque le certificat est stocké sur une clé cryptographique matérielle prise en charge par le client SGLC, l'utilisateur ne doit exécuter aucune action supplémentaire une fois la clé cryptographique débloquée : le chiffrement et le déchiffrement s'effectuent automatiquement.

2 Mise en route

2.1 Certificats

conpal LAN Crypt utilise des certificats et des paires de clés publiques/privées pour sécuriser les informations de chiffrement stockées dans les fichiers de stratégie. Seul le détenteur d'un certificat peut accéder à la clé privée appartenant au certificat et donc l'utiliser pour accéder aux informations de chiffrement.

Types et origines des certificats pouvant être utilisés :

- Une société possède soit une infrastructure à clé publique (PKI) ou fait appel à un centre de confiance (Trust Center) pour créer les certificats de ses utilisateurs. Dans ce cas, il est possible d'utiliser des certificats existants.
- Sinon, le composant conpal LAN Crypt Administration peut générer des certificats autosignés. Ces certificats peuvent être utilisés uniquement avec conpal LAN Crypt ! Les certificats doivent également disposer d'une extension critique pour indiquer aux applications qu'ils ne doivent pas être utilisés. Il s'agit de certificats simples (comparables aux certificats de classe 1) et conformes à la norme X.509.
  Dans conpal LAN Crypt, vous pouvez configurer si une extension critique est ajoutée ou non à un certificat nouvellement généré.

Remarque : Dans certaines situations, des applications ignorent les extensions critiques des certificats conpal LAN Crypt. Ceci risque d'entraîner des problèmes pour les certificats autosignés. Dans ce cas, vous devez désactiver de façon explicite toutes les zones d'utilisation des certificats conpal LAN Crypt à l'aide du composant logiciel enfichable MMC de certificat pour empêcher ces certificats d'être utilisés par d'autres applications.

Les certificats sont assignés aux utilisateurs au sein du composant conpal Administration.

Informations importantes à propos de l'utilisation des certificats :

- conpal LAN Crypt utilise uniquement l'API Microsoft Crypto pour la fonctionnalité de certificat.
- conpal LAN Crypt accepte tous les fournisseurs de services cryptographiques (CSP) respectant certaines normes (par exemple, une longueur de clé RSA d'au moins 1024 bits). Il s'agit notamment de Microsoft Enhanced CSP.

Remarque : Il n'est pas possible d'utiliser Microsoft Standard CSP (Microsoft Base CSP).

Pour toute question relative à la compatibilité des autres CSP, veuillez contacter le service de support.

2.1.1 Niveaux de sécurité

Comme conpal LAN Crypt vise à fournir le niveau de sécurité le plus élevé possible, il est nécessaire de faire appel à des CSP forts tels que Microsoft Strong Cryptographic Service Provider. Ces CSP autorisent l'utilisation de clés d'une longueur maximale de 16384 bits et fournissent des algorithmes de chiffrement forts (comme 3DES).

Vous devrez également activer l'option suivante pendant l'importation d'un certificat à l'aide de l'*assistant d'importation de certificats* :

Activer la protection renforcée par clé privée

Vous serez invité(e) à saisir le mot de passe chaque fois que la clé privée sera utilisée par une application.
Après avoir cliqué sur **Terminer** dans l'*assistant d'importation de certificats*, la boîte de dialogue *Importer une clé d'échange privée* s'affiche. Cliquez sur **Définir le niveau de sécurité** pour reconfigurer le niveau de sécurité :

- Élevé :
  Si vous sélectionnez *Élevé*, vous devrez saisir un mot de passe pour confirmer que vous utilisez une clé privée. Entrez un nouveau mot de passe dans la boîte de dialogue suivante.

- Moyen
  Si vous sélectionnez *Moyen*, le système affiche une invite vous demandant de confirmer l'utilisation d'une clé privée. Cliquez pour cela sur **OK**.

Niveau de sécurité le plus élevé avec des clés d'échange privées automatiquement importées (.p12, .pfx)

conpal LAN Crypt vous permet d'importer des certificats automatiquement. Pour utiliser le niveau de sécurité élevé ou moyen avec les clés privées appartenant à ces certificats, configurez l'option Protection forte de la clé privée de la Configuration de conpal® LAN Crypt sur oui.

Si cette option n'est pas activée, le niveau de sécurité "faible" est automatiquement appliqué aux certificats importés.

Vous pouvez ainsi garantir que les certificats avec le niveau de sécurité élevé sont obligatoires et peuvent être mis en œuvre au sein de la stratégie de sécurité de l'entreprise :

Remarque : Si le niveau de sécurité le plus élevé est activé, les utilisateurs de conpal LAN Crypt doivent saisir une fois le mot de passe de la clé privée, au moment de l'ouverture de session Windows , puis ensuite, à chaque chargement d'une règle de chiffrement.
Carte à puce :
Lorsque les certificats sont stockés sur une carte à puce, le mot de passe ne devra être saisi qu'une seule fois. Tant que la carte à puce reste dans le lecteur de carte, il n'est pas nécessaire de ressaisir le mot de passe.

Remarque : Nous vous recommandons de configurer cette option sur "Élevé" avant la première utilisation de conpal LAN Crypt Administration. Sinon, le certificat initial du responsable de la sécurité principal ne sera pas utilisé avec le niveau de sécurité "Élevé" au moment de sa création par conpal LAN Crypt, ce qui n'est pas le cas, par exemple, lorsqu'il est importé d'une carte à puce.

Remarque : Par défaut, Windows met en mémoire cache les codes PIN pendant 24 heures. Le recours à des certificats logiciels peut poser des problèmes de sécurité lorsque vous vous connectez à conpal LAN Crypt Administration et que vous devez fournir une autorisation supplémentaire. Nous vous recommandons vivement de désactiver cette fonction.
Pour ce faire, renseignez ces valeurs :
`"PrivKeyCacheMaxItems"=dword:00000000`
`"PrivKeyCachePurgeIntervalSeconds"=dword:00000000`
dans la clé
`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Policies\`
`Microsoft\`
`Cryptography`

Si vous procédez ainsi, les codes PIN ne seront pas mis dans la mémoire cache.

Conditions préalables à l'utilisation de certificats avec conpal LAN Crypt

- Le certificat doit inclure une clé publique.
- La clé privée du certificat assigné doit être disponible avant l'accès par l'utilisateur au profil de chiffrement.
- conpal LAN Crypt donne uniquement la liste des certificats stockés dans *Configuration utilisateur* dans les magasins Certificats personnels, Autres personnes et Objet utilisateur Active Directory et dans *Ordinateurs locaux* du magasin Certificats personnels . conpal LAN Crypt ignore les certificats stockés dans d'autres emplacements !
  Vous pouvez utiliser le composant logiciel enfichable qu'est la console de gestion des certificats pour importer et organiser les certificats.
- Seule la clé publique sert à "associer" un certificat aux informations de chiffrement de conpal LAN Crypt. Vous n'avez pas besoin de connaître la clé privée. La clé privée reste la propriété du détenteur du certificat qui est la seule personne à pouvoir accéder aux informations de chiffrement.

Nous vous recommandons d'avoir les certificats à portée de main avant de commencer à installer conpal LAN Crypt. Les certificats apparaissent ensuite dans la boîte de dialogue *Certificats* immédiatement après l'installation de conpal LAN Crypt et peuvent être utilisés instantanément.

Remarque : conpal LAN Crypt n'administre pas les certificats. Toutefois, vous pouvez le faire en utilisant l'infrastructure PKI de votre entreprise ou les centres de confiance.

2.1.2 Vérification du certificat

conpal LAN Crypt effectue une vérification étendue des certificats. Cela signifie que les certificats ne peuvent plus être acceptés tant que la chaîne complète de certificats (évaluation d'une **R** évocation de **C** ertificats **L**) n'a pas été contrôlée.

La vérification étendue porte sur les certificats suivants :

- Les certificats fournis à la création d'un responsable principal de la sécurité. Seuls les certificats ayant passé tous les tests sont affichés.
- Les certificats créés après l'utilisation d'une clé de récupération pour assigner un nouveau certificat à un responsable de la sécurité. Seuls les certificats ayant passé tous les tests sont affichés.
- Les certificats utilisés par les responsables de la sécurité pour se connecter à la base de données conpal LAN Crypt. Si les certificats ne peuvent pas être vérifiés, l'accès sera refusé.
- Les certificats utilisés pour les autorisations supplémentaires.

Les conditions préalables à une vérification étendue des certificats sont les suivantes :

- Le certificat utilisé doit inclure une CRL.
  Certains infrastructures PKI vous permettent de définir une CRL dans le certificat lui-même. Si une CRL a été définie, la liste est évaluée. À cet effet, vous pouvez avoir besoin d'utiliser le réseau pour télécharger une CRL à partir de l'émetteur. S'il est impossible de vérifier un certificat, le profil de chiffrement ne sera pas chargé.
- Une CRL a été chargée dans le magasin de certificats local.

Remarque : Une connexion réseau doit être établie avant d'évaluer la CRL. Si cette connexion ne peut être établie, l'accès sera refusé même si le certificat en lui-même est valide.

2.1.3 Lecteurs de carte à puce

Comme le recours aux certificats est pris en charge par les fournisseurs de services cryptographiques (CSP), les cartes à puce sont reconnues automatiquement lors de l'utilisation d'une CSP. Vous pouvez donc gérer l'accès aux informations de chiffrement en utilisant les certificats des cartes à puce.

Pour utiliser les certificats sur les cartes à puce, assurez-vous que le lecteur de carte et un fournisseur de services cryptographiques adapté sont correctement installés.

2.2 Installation

Remarque : Vous pouvez installer conpal LAN Crypt uniquement si vous disposez de privilèges d'administrateur Windows.

1. Rendez-vous dans le répertoire d'installation de votre package d'installation décompressé et cliquez deux fois sur le fichier .msi.
   Un assistant d'installation vous guide dans l'installation de conpal LAN Crypt, qui est une procédure très simple. Cliquez sur **Suivant**.

2. La boîte de dialogue *Contrat de licence* s'affiche.
   Sélectionnez **J'accepte les termes du contrat de licence** dans le boîte de dialogue Contrat de licence. Si vous n'acceptez pas les termes, vous ne pourrez pas installer sur conpal LAN Crypt ! Cliquez sur **Suivant**.

3. La boîte de dialogue *Dossier de destination* s'affiche.
   Sélectionnez où vous voulez installer conpal LAN Crypt.
   Cliquez sur **Suivant**.

4. La boîte de dialogue *Sélectionner le type d'installation* s'affiche.
   Vous pouvez sélectionnez quels composants conpal LAN Crypt doivent être installés.
   Sélectionnez **Personnalisée**, puis cliquez sur **Suivant**.

Les composants suivants peuvent être installés :

- Administration
  Installe conpal LAN Crypt Administration.

- **API de script**
  Installe l'API de script conpal LAN Crypt requise pour administrer le produit à l'aide de scripts.

5. Sélectionnez les composants à installer et cliquez sur **Suivant**.

6. Après avoir vérifié vos paramètres, cliquez sur **Suivant** dans la boîte de dialogue de préparation de l'installation.
   Le processus d'installation commence.

7. Une fois l'installation terminée avec succès, une boîte de dialogue s'affiche. Cliquez sur le bouton **Terminer** de cette dernière pour valider la fin de la procédure.

Remarque : Pour valider tous les paramètres, redémarrez l'ordinateur ! Ceci permet de charger tous les pilotes.

2.3 Installation automatique

L'installation automatique signifie que vous pouvez installer conpal LAN Crypt automatiquement sur un grand nombre d'ordinateurs.
Le répertoire d'`Installation` contient le fichier `sglcadm.msi` nécessaire à une installation automatique.

2.3.1 Composants à installer

La liste ci-dessous indique les composants devant être installés et la manière de les renseigner pour une installation automatique.

Les mots-clés (en gras, police Courier) représentent la manière de spécifier les composants dans ADDLOCAL= lorsque vous procédez à une installation automatique. Respectez les majuscules et minuscules pendant la saisie des noms des composants.

conpal LAN Crypt Administration - **`Administration`**

API de script - **`ScriptingAPI`**

Remarque : Si vous ne spécifiez pas de composant, une installation complète sera réalisée.

2.3.2 Syntaxe de la ligne de commande

Pour procéder à une installation automatique, vous devez exécuter `msiexec` avec des paramètres spécifiques.

Paramètres obligatoires :
`/I`
Indique le package d'installation à installer.

`/QN`
Installation sans interaction de l'utilisateur (installation automatique)

Nom du fichier `.msi` : `sglcadm.msi`

Syntaxe :
```
msiexec /i <chemin>\sglcadm.msi /qn
```

Paramètre en option :
`/chemin Lxv< + nom de fichier>`
Consigne toute la procédure d'installation dans un journal à l'emplacement indiqué sous `<chemin + nom de fichier>`.

Exemple :
```
msiexec /i C:\Install\sglcadm_en.msi /qn
```

Vous obtenez ainsi une installation complète de conpal LAN Crypt. Le programme est installé dans le répertoire d'installation par défaut (`<lecteur système>:\Program Files\Sophos`). Le fichier `.msi` est placé dans le répertoire `Install` du lecteur C.

2.4 Mise à niveau

Si vous effectuez une mise à niveau à partir de versions antérieures de conpal LAN Crypt Administration, les étapes suivantes sont nécessaires :

- Installation de la nouvelle version
- Mise à niveau de la base de données existante
- Exécution de l'assistant de mise à niveau
- Saisie des nouvelles informations d'identification du serveur en cas de mise à niveau à partir d'une version antérieure à la version 3.61.

Remarque : la première connexion après la mise à niveau doit être exécutée par un responsable principal de la sécurité.

2.4.1 Installation de la nouvelle version

La nouvelle version doit être installée comme décrit ci-après.

Remarque : assurez-vous que toutes les instances de conpal LAN Crypt Administration sont fermées avant d'installer la nouvelle version.

2.4.2 Mise à niveau de la structure existante de la base de données conpal LAN Crypt

Grâce à l'outil de ligne de commande `CreateTables.exe`, vous pouvez effectuer la mise à niveau de la structure des tables présentes dans votre base de données conpal LAN Crypt. L'outil est disponible dans le répertoire \Install de votre package d'installation.

Remarque : la connexion à la base de données doit être effectuée avec des privilèges qui permettent la création et la modification du schéma de la base de données.

Syntaxe de la ligne de commande :

```
CreateTables <ODBCName[.OwnerName]> <SQL dialect > <Action>
```

`CreateTables.exe` met à disposition les paramètres suivants afin de vous permettre de créer des tables dans d'autres configurations :

Nom ODBC :
Nom utilisé pour la source de données ODBC.

Nom du propriétaire
Pour que la base de données puisse être adressée correctement, le propriétaire de la base de données doit être indiqué pour les bases de données Oracle. Le nom du propriétaire doit être indiqué en LETTRES CAPITALES.

Langage SQL :
```
m ... Microsoft SQL Server
o ... Oracle 9 or higher
```

Actions :
```
u ... Update of the database structure
```

Exemple 1 :
```
CreateTables SGLCSQLServer m u
```

Exemple 2 :
```
CreateTables SGLCSQLServer.SGLC o u
```

2.4.3 Assistant de mise à niveau

Une fois la base de données mise à niveau, un assistant de mise à niveau vous guide tout au long des étapes nécessaires pour terminer cette mise à niveau. L'assistant se lance après la première connexion à l'administration mise à niveau.

Remarque : seul un responsable principal de la sécurité peut procéder à la première connexion après la mise à niveau de l'administration. Si vous ne possédez pas les droits appropriés, un message s'affiche.
Les étapes de la mise à niveau peuvent varier en fonction de la version que vous avez mise à jour.

Exécutez les étapes suivantes de l'assistant :

- Saisie d'un nom d'emplacement.
- Vérification et, si nécessaire, correction de l'intégrité de la base de données.
  Les informations sur les erreurs corrigées s'afficheront.
- Création d'une nouvelle clé de récupération

Une fois l'assistant terminé, vous pouvez utiliser l'administration.

2.4.4 Codes d'accès de connexion au serveur pour les versions antérieures à la version 3.61

Après la mise à niveau, les informations d'identification de connexion doivent être de nouveau saisies sous *Paramètres centraux* sur la page *Serveur*. Si vous utilisez un **Service d'annuaire Microsoft**, procédez comme suit :

- Saisissez le `nom du domaine` sous *Nom du domaine ou du serveur*.
- Saisissez le *Nom d'utilisateur* sous la forme `nom d'utilisateur@nom du domaine`.

2.5 Désinstallation

Remarque : vous pouvez désinstaller conpal LAN Crypt uniquement si vous disposez de privilèges d'administrateur Windows.

1. Sélectionnez **Démarrer**, **Panneau de configuration**, **Ajout/Suppression de programmes**.
2. Sélectionnez **conpal LAN Crypt Administration** dans la liste des programmes installés.
3. Cliquez sur **Supprimer** pour désinstaller conpal LAN Crypt Administration.
4. Si vous souhaitez vraiment désinstaller conpal LAN Crypt Administration, cliquez sur **OK** dans le message d'avertissement qui apparaît.
5. Redémarrez votre ordinateur pour terminer le processus de désinstallation.

Remarque : lorsque vous désinstallez conpal LAN Crypt, le contenu de la base de données de conpal LAN Crypt est préservé. Si nécessaire, la base de données doit être supprimée séparément à l'aide des outils proposés par le système d'exploitation ou des outils d'administration de la base de données.
En outre, tous les paramètres spécifiques aux utilisateurs restent dans le système (clés de registre, paramètres de stratégie de groupe, etc.).

3 Administration

conpal LAN Crypt Administration s'intègre de manière transparente dans la console de gestion de Microsoft (MMC) et offre au responsable de la sécurité une interface utilisateur sécurisée dotée de la fonctionnalité MMC caractéristique.
La console Administration a été mise au point pour permettre aux utilisateurs de bénéficier des outils de réplication Windows existants. Cela permet non seulement d'obtenir un niveau de performance élevé mais aussi de réduire les coûts totaux de possession puisque les clients disposant d'un grand nombre de postes de travail veulent généralement un seul système pour les administrer.

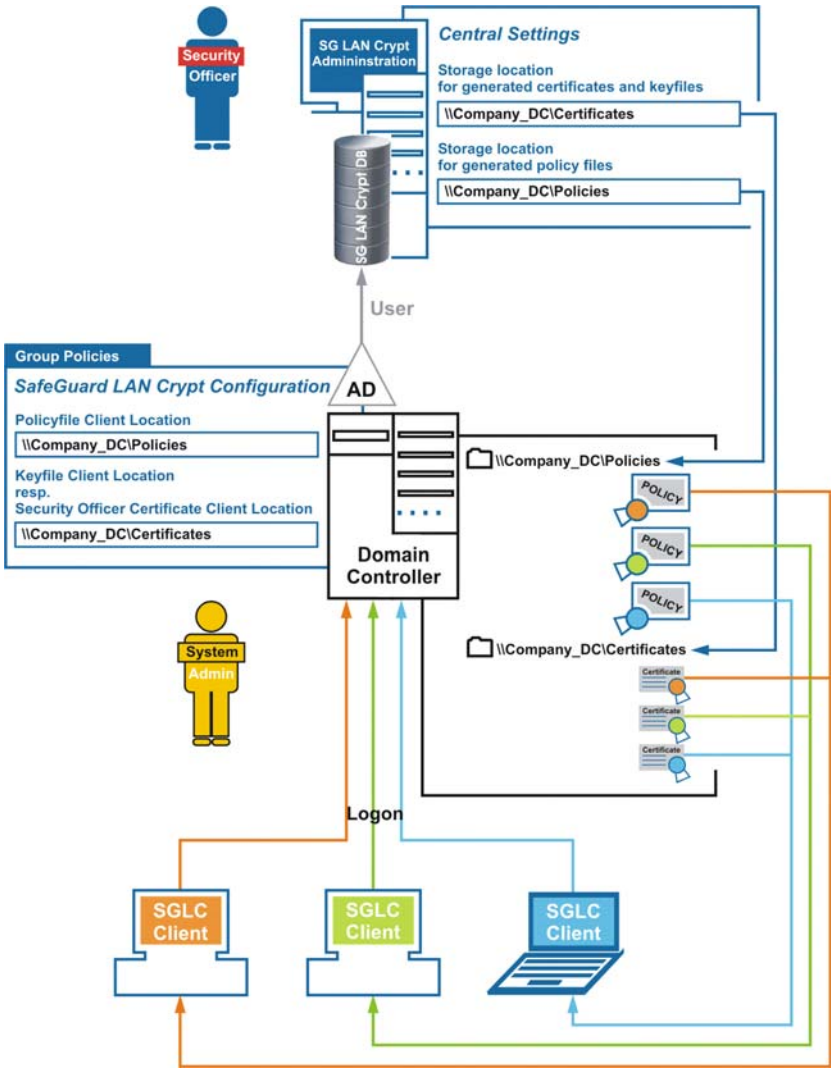
La console conpal LAN Crypt Administration est en règle générale installée sur une machine séparée, à partir de laquelle il est possible d'accéder aux services d'annuaires nécessaires et à la base de données conpal LAN Crypt.

conpal LAN Crypt utilise le concept de responsable de la sécurité. Au départ, il y a un **responsable principal de la sécurité** qui installe la console Administration. Pendant l'installation, le responsable principal de la sécurité doit indiquer où devront être enregistrés les certificats et les fichiers de clés (c'est-à-dire la partie publique du certificat du responsable principal de la sécurité et les fichiers .p12 contenant les certificats des utilisateurs importés sur les machines clientes) générés pour les utilisateurs. Après l'installation, vous devez indiquer où doivent être enregistrés les fichiers de stratégie générés pour les utilisateurs. Les fichiers de stratégie contenant les règles de chiffrement sont générés pour chaque utilisateur.

Par la suite, les certificats, les fichiers .p12 et les fichiers de stratégie sont automatiquement importés par les clients à partir de l'emplacement de stockage désigné.

Les clients doivent donc pouvoir accéder à ces répertoires. Le **responsable principal de la sécurité** et l'**administrateur système** doivent ensemble définir ces répertoires (généralement les dossiers réseau partagés).

Les clients peuvent utiliser les stratégies de groupe lorsqu'ils se connectent à un contrôleur de domaine pour savoir comment accéder à ces fichiers. L'administrateur système spécifie les emplacements de stockage dans la console conpal LAN Crypt Configuration. conpal LAN Crypt est configuré dans l'objet de stratégie de groupe valide pour les utilisateurs.



Les clients conpal LAN Crypt n'ont pas besoin de se connecter à la base de données de conpal LAN Crypt.
Les informations permettant de trouver les certificats, les fichiers .p12 et les fichiers de stratégie sont accessibles dans les stratégies de groupe. Ces fichiers sont ensuite automatiquement transférés aux clients.

Un mot de passe est nécessaire à l'utilisateur pour importer un certificat. Dans le cas de certificats générés par conpal LAN Crypt, le fichier p12pwlog.csv contient les mots de passe et peut servir, par exemple, à créer un courrier PIN.

3.1 Étapes de la procédure

- Préparations :
  - Facultatif : installer le système de base de données fourni
  - Ajouter une source de données (ODBC)
  - Créer des tables de base de données (CreateTables.exe)
- **Administrateur système** : Définir les paramètres dans la console conpal LAN Crypt Configuration.
- Créer le responsable principal de la sécurité initial

  Définir les emplacements de stockage
  - pour les certificats et les fichiers de clés générés par conpal LAN Crypt

Remarque : les certificats des utilisateurs (fichiers p12) et la partie publique du certificat du responsable de la sécurité sont importés par les clients à partir de ce répertoire. Un répertoire défini avec l'administrateur du système est normalement déjà disponible (partage réseau).

  - pour les certificats SO générés par conpal LAN Crypt
  - pour le fichier journal des mots de passe qui contient les mots de passe générés automatiquement pour les fichiers de clés
- Définir les paramètres centraux (noyau)

  Vous définissez ici les emplacements de stockage des fichiers de stratégie générés pour les utilisateurs. Pour ce faire, travaillez avec votre **administrateur système**.

Remarque : si vous utilisez une base de données Oracle et y accédez à partir des consoles Administration sur les différents postes, vous devrez également indiquer les paramètres des pages de codes (see *Onglet Base de données* on page 58).

- Créer des responsables principaux de la sécurité supplémentaires
- Définir les droits des responsables de la sécurité
- Importer les objets (unités organisationnelles, groupes, utilisateurs) à partir du service d'annuaire (par exemple, Active Directory)
- Assigner des responsables de la sécurité aux unités organisationnelles (OU, organizational unit)et définir leurs droits
- Créer des clés
- Créer des règles de chiffrement
- Générer ou assigner des certificats

- Générer des fichiers de stratégie

3.2 Étapes de préparation de l'administration de conpal LAN Crypt

Après l'installation, vous devez suivre la procédure décrite ci-après avant de commencer à administrer conpal LAN Crypt :

- Facultatif : installer le système de gestion de base de données
  Cette opération est nécessaire uniquement si votre système de base de données ne comprend pas une base de données que vous souhaitez utiliser pour administrer conpal LAN Crypt. Pour parer à cette éventualité, conpal LAN Crypt possède sa propre base de données que vous pourrez utiliser librement pour les tâches d'administration. Il s'agit de Microsoft SQL Server 2008 R2 Express Edition.
  Par ailleurs, conpal LAN Crypt accepte les systèmes de base de données suivants :
  - Microsoft SQL Server 2005
  - Microsoft SQL Server 2005 Express
  - Microsoft SQL Server 2008 R2
  - Microsoft SQL Server 2008 R2 Express
  - Oracle*9i*
  - Oracle*10g*
  - Oracle11

Remarque : si vous utilisez une base de données Oracle, vous devez installer le client Oracle avant d'utiliser conpal LAN Crypt Administration. Si vous sélectionnez la variante "runtime" du client Oracle, vous devez également installer le pilote ODBC d'Oracle.
conpal LAN Crypt ne prend pas en charge Microsoft ODBC pour Oracle.
Veillez à ne pas utiliser les mots-clés réservés de l'éditeur lorsque vous générez des objets de base de données.

- Indication d'une source de données (ODBC)
  Si vous souhaitez utiliser votre propre système de base de données, vous devez connaître les données d'accès à cette base pour pouvoir indiquer la source des données.

- Création de tables de base de données
  Après avoir indiqué la source de données, vous devez créer les tables conpal LAN Crypt dans la base de données à l'aide de l'outil fourni avec votre logiciel (CreateTables.exe).

3.2.1 Installation du système de base de données fourni

La description suivante fait référence à Microsoft SQL Server 2008 R2 Express Edition. Dans cet exemple de description, les valeurs par défaut de cette version ont été utilisées dans la mesure du possible.

Pour installer le système de base de données, procédez comme suit :

1. Dans le répertoire d'installation de votre package d'installation décompressé, cliquez deux fois sur le fichier SQLEXPR32_x86_ENU.exe.

Remarque : si vous utilisez un système d'exploitation en 64 bits, téléchargez la version 64 bits de Microsoft SQL Server 2008 R2 Express Edition depuis www.microsoft.com.

2. Acceptez le contrat de licence et cliquez sur **Suivant**.

3. Les fichiers d'installation sont extraits et l'assistant d'installation démarre.

4. Suivez les instructions de l'assistant d'installation et acceptez toutes les valeurs par défaut.

Valeurs par défaut : Les descriptions suivantes des étapes de préparation font références à ces valeurs par défaut. Si vous procédez à des modifications (méthode d'authentification, instance de base de données), vous devez les prendre en compte au moment d'indiquer la source de données et de créer les tables de base de données.

Authentification de la base de données : Par défaut, Express Edition utilise l'authentification Windows.
Condition préalable requise à l'utilisation de l'authentification Windows, l'utilisateur qui se connecte à la base de données doit posséder les droits d'administrateur Windows.

Base de données principale : Par défaut, la base de données principale existante est utilisée au moment de spécifier la source de données. En général, nous recommandons de ne PAS utiliser la base de données principale car cela peut entraîner des problèmes lors de la mise à niveau d'Express Edition ou de la version de SQL Server.

Vous pouvez créer une base de données distincte pour conpal LAN Crypt et la spécifier au moment d'ajouter la source de données. Pour Microsoft SQL Server 2008 R2 Express Edition, vous pouvez créer une base de données en utilisant la commande suivante sur la ligne de commande :

osql -E -S .\SQLEXPRESS -Q “CREATE DATABASE <nom_de_la_base_de_données>“
Une base de données avec le nom spécifié utilisant la spécification Windows est créée.
Avec le paramètre -U, par exemple, vous pouvez indiquer un nom d'utilisateur pour l'authentification. Pour voir tous les paramètres, saisissez osql -?.

Vous pouvez aussi télécharger Microsoft SQL Server 2008 R2 Management Studio Express gratuitement et l'utiliser pour créer une base de données distincte.

À l'étape suivante, une source de données doit être spécifiée afin que conpal LAN Crypt puisse utiliser le système de base de données.

3.2.2 Ajout d'une source de données (ODBC)

Remarque : la source de données doit être ajoutée avec l'administrateur de source de données ODBC 32 bits, lequel est également disponible sur les systèmes 64 bits. Si vous utilisez un système 64 bits, démarrez l'administrateur de source de données ODBC en cliquant sur Démarrer\Tous les programmes\Sophos\conpal LAN Crypt \ODBC Data Source Administrator (x86). Ceci permet de s'assurer que la version appropriée est lancée.

Désignez une source de données afin que conpal LAN Crypt puisse utiliser la base de données via le système de gestion de données. Pour ce faire, utilisez l'administrateur de source de données ODBC.

ODBC (Open Database Connectivity) permet l'accès aux données à partir d'un large éventail de systèmes de gestion de bases de données. Par exemple, si vous avez un programme servant à accéder à une base de données SQL, ODBC vous permet d'utiliser ce même programme pour accéder aux données d'une autre base. Pour ce faire, vous devez ajouter des "pilotes" au système. ODBC vous assiste dans l'ajout et la configuration de ces pilotes.

Pour ajouter une source de données :

1. Sélectionnez Démarrer\Paramètres\Panneau de configuration\Outils d'administration\Sources de données (OBDC).
   L'administrateur de source de données OBDC s'ouvre.

2. Sélectionnez l'onglet **Sources de données système** et cliquez sur **Ajouter....**
   Une liste s'affiche. Vous pouvez y ajouter des sources de données, chacune possédant son nom de source de données système. Ces sources de données sont enregistrées en local sur un ordinateur mais ne sont assignées à aucun utilisateur en particulier : tout utilisateur possédant les droits appropriés peut utiliser un nom de source de données système.

3. Sélectionnez **SQL Server** comme pilote pour la création de la source de données et cliquez sur **Terminer**.

Remarque : si SQL Server Native Client est disponible dans la liste, sélectionnez cette entrée.

4. Une boîte de dialogue apparaît maintenant dans laquelle vous pouvez saisir le nom **SGLCSQLServer** en référence à la source de données.
   Configurez le nom de référence de la source de données dans la configuration de conpal LAN Crypt. L'option par défaut est **SGLCSQLServer**. Si vous souhaitez utiliser un nom différent, configurez-le.

Remarque : le nom de la source ODBC est sensible à la casse. Saisissez ici les noms exactement de la même façon qu'ils ont été spécifiés dans la configuration de conpal LAN Crypt.
Vous devez saisir les noms dans la configuration avant d'exécuter pour la première fois la console conpal LAN Crypt Administration.

5. Dans le champ *Serveur*, sélectionnez le serveur qui servira à établir la connexion, puis cliquez sur **Suivant**.

6. Acceptez les paramètres par défaut de la boîte de dialogue suivante. Si vous cochez l'option **Avec l'authentification Windows NT par l'ID de connexion réseau**, vous choisissez d'utiliser les données utilisateur Windows pour vous connecter à la base de données. Vous n'avez pas besoin d'entrer un mot de passe.
   Cliquez sur **Suivant**.

7. Acceptez les paramètres par défaut de la boîte de dialogue suivante.
   Par la suite, la base de données principale existante est utilisée.
   En revanche, si vous avez généré votre propre base de données, sélectionnez-la ici.

8. Acceptez les paramètres par défaut de la boîte de dialogue suivante puis cliquez sur **Terminer**.

3.2.3 Création de tables dans la base de données conpal

Grâce à l'outil de ligne de commande `CreateTables.exe` vous pouvez créer les tables requises dans
votre base de données conpal LAN Crypt. L'outil est disponible dans le répertoire d'installation de votre package d'installation décompressé.

Remarque : la connexion à la base de données doit être effectuée avec des privilèges qui permettent la création et la modification du schéma de la base de données.

Pour créer la table dans votre base de données, procédez comme suit :

1.) Saisissez ce qui suit sur la ligne de commande : `CreateTables SGLCSQLServer m c`.

Si vous avez utilisé les valeurs par défaut lors de l'installation, la configuration du système de base de données est maintenant terminée. Vous pouvez maintenant démarrer conpal LAN Crypt Administration.

3.2.3.1 Syntaxe de ligne de commande CreateTables

```
CreateTables <ODBCName[.OwnerName]> <SQL dialect > <Action>
```

Vous pouvez créer des tables dans des configurations différentes grâce aux paramètres suivants fournis par `CreateTables.exe` :

ODBCname :
Nom utilisé pour la source de données ODBC.

OwnerName
Pour que la base de données puisse être adressée correctement, le propriétaire de la base de données doit être indiqué pour les bases de données Oracle. Le nom du propriétaire doit être indiqué en LETTRES CAPITALES.

SQL Dialect :
```
m ... Microsoft SQL Server
o ... Oracle 9 or higher
```

Actions :
```
c ... Create all tables
```

Exemple 1 :
```
CreateTables SGLCSQLServer m c
```

Exemple 2 :
```
CreateTables SGLCSQLServer.SGLC o c
```

3.3 Responsables principaux de la sécurité

conpal LAN Crypt utilise le concept de responsable de la sécurité. La configuration initiale comprend un responsable principal de la sécurité qui peut ensuite déléguer des tâches en créant des responsables de la sécurité supplémentaires et en leur assignant des droits spécifiques d'administration de conpal LAN Crypt. Le premier responsable principal de la sécurité peut même créer des responsables principaux de la sécurité supplémentaires.

Les listes d'accès ACL servent à définir les droits assignés aux responsables de la sécurité créés par un responsable principal de la sécurité. Il est ensuite possible d'assigner chaque responsable de la sécurité à différentes unités organisationnelles (OU) de l'administration centrale. Leurs droits s'appliquent alors exclusivement à l'OU à laquelle ils sont assignés. Les droits sont hérités en aval dans la hiérarchie organisationnelle jusqu'à ce que d'autres droits soient assignés.

Après avoir configuré le système de base de données et la source de données, la prochaine étape consiste à créer un **responsable principal de la sécurité** initial au moment du premier lancement de la console conpal LAN Crypt Administration.
Un responsable principal de la sécurité détient toujours tous les droits existants.

Remarque : au moment de la création du responsable principal de la sécurité initial, vous devez également définir l'emplacement de stockage des certificats et des fichiers de clés générés par conpal LAN Crypt. La partie publique du certificat du responsable de la sécurité, demandée par les clients, est également stockée ici. Les certificats des utilisateurs (fichiers .p12) seront importés ultérieurement à partir de ce répertoire. Le répertoire que vous avez défini avec l'**administrateur système** est normalement déjà disponible (partage réseau).

Vous pouvez modifier ultérieurement tous les paramètres définis au moment de la création du responsable principal de la sécurité initial dans le menu *Paramètres centraux* de la console conpal LAN Crypt Administration.

3.3.1 Responsable principal de la sécurité initial

Après le premier lancement de la fonction Administration (Démarrer, Programmes, Sophos, conpal, LAN Crypt/SGLC Administration) et votre connexion à la base de données, l'assistant de création du responsable principal de la sécurité initial apparaît à l'écran. Il se compose de quatre étapes :

Entrez les données du responsable principal de la sécurité initial. Le nom que vous entrez sera considéré comme le Common Name si vous utilisez les certificats générés par conpal LAN Crypt.
Les champs de l'adresse de messagerie et des commentaires sont facultatifs. Cliquez sur **Suivant**.

Remarque : l'adresse de messagerie est ajoutée au fichier journal des certificats générés par conpal LAN Crypt. Elle peut servir, par exemple, à créer à un courrier de codes PIN transmis par messagerie électronique.

Dans la deuxième boîte de dialogue de l'assistant, désignez les emplacements de stockage pour :

- les certificats et les fichiers de clés générés (.p12) ;
- les certificats générés par le responsable de la sécurité ;
- le fichier journal des mots de passe générés automatiquement pour les fichiers de clés.

Emplacement de stockage pour les certificats et les fichiers de clés générés

Le cas échéant, conpal LAN Crypt peut également générer des certificats autosignés. Ces certificats (fichiers .p12) sont générés lors de l'assignation de certificats aux utilisateurs. Vous désignez ici l'emplacement où ces fichiers seront enregistrés.

C'est également l'endroit où est enregistrée la partie publique du certificat du responsable de la sécurité (.cer) qui sert à sécuriser la base de données d'administration.

Les fichiers de clés (.p12) et la partie publique du certificat du responsable de la sécurité doivent être mis à la disposition des utilisateurs.

Dans conpal LAN Crypt Configuration, désignez le dossier dans lequel conpal LAN Crypt doit rechercher un fichier .p12 pour l'utilisateur si la clé privée du fichier de stratégie n'est pas présente. La même procédure s'applique à la partie publique du certificat du responsable de la sécurité.

Si conpal LAN Crypt trouve un fichier .cer approprié contenant la partie publique du certificat du responsable de la sécurité, il l'importe automatiquement.

Remarque : avant de pouvoir exploiter cette fonctionnalité, vous devez définir les chemins adaptés dans conpal LAN Crypt Configuration.

Vous pouvez aussi distribuer manuellement les fichiers de clés des utilisateurs et la partie publique du certificat de l'administrateur. Dans ce cas, assurez-vous que les clients importent les deux.

Remarque : les clients doivent importer la partie publique du certificat du responsable de la sécurité qui a généré les fichiers de stratégie.
Si vous modifiez le chemin sous lequel sont enregistrés les fichiers .cer des responsables de la sécurité et les fichiers .p12 des utilisateurs après avoir créé les responsables de la sécurité, vous devez copier leurs fichiers .cer dans le nouvel emplacement. Sinon, il sera impossible de trouver les parties publiques des certificats des responsables de la sécurité. Les fichiers .p12 des utilisateurs doivent également être générés sous le nouveau chemin.

Emplacement pour les certificats générés des responsables de la sécurité

conpal LAN Crypt stocke les certificats des responsables de la sécurité dans des fichiers .p12, par exemple sous forme de sauvegarde. Vous pouvez désigner ici dans quel dossier ils seront enregistrés.

Remarque : ils contiennent des données sensibles ; il est donc essentiel que vous les protégiez contre les accès non autorisés !

Fichier journal des mots de passe

Vous désignez ici l'emplacement de stockage et le nom du fichier journal des fichiers de clés PKCS#12 générés. Ce fichier contient les mots de passe des fichiers de clés PKCS#12 générés et peut servir par exemple à créer un courrier contenant les codes PIN.

Remarque : vous devez protéger ce fichier et ne jamais l'enregistrer dans le même dossier que les fichiers POL.
Avec conpal LAN Crypt, vous pouvez facilement protéger le fichier journal des mots de passe. Pour ce faire, installez l'administration et le client sur le même ordinateur. Après avoir créé le responsable principal de la sécurité initial, créez une règle de chiffrement qui chiffre le fichier journal des mots de passe, générez un profil pour le MSO initial et chargez le profil. La clé de chiffrement utilisée doit exclusivement être mise à disposition des Responsables principaux de la sécurité et des Responsables de la sécurité disposant des droits de création de certificats. L'exécution de l'assistant de chiffrement initial entraîne le chiffrement du fichier journal des mots de passe. Pour s'assurer que le mot de passe du MSO initial n'a pas été compromis lorsque le fichier n'était pas chiffré, créez un nouveau certificat et assignez-le au MSO initial.

Remarque : si l'utilisateur procédant à l'assignation de certificats ne détient pas le droit de modifier le fichier journal des mots de passe, conpal LAN Crypt ne sera pas en mesure de créer les certificats.

Cliquez sur **Suivant**.

Validité du certificat

Dans cette troisième boîte de dialogue de l'assistant, configurez la période de validité des certificats générés par conpal LAN Crypt et assignez un certificat existant, ou un certificat généré par conpal LAN Crypt, au responsable de la sécurité.

Si vous utilisez un certificat généré par conpal LAN Crypt, il est valide pendant la période spécifiée.
Tous les certificats générés ensuite auront cette période de validité.

Certificat du responsable de la sécurité initial

Vous devez sélectionner le certificat de chiffrement à utiliser pour sécuriser les données du responsable de la sécurité. Vous pouvez également sélectionner un certificat de signature que le responsable de la sécurité doit utiliser pour s'identifier auprès du module conpal LAN Crypt Administration. Si vous ne spécifiez aucun certificat de signature, le certificat de chiffrement sera également utilisé à des fins d'authentification.

Cliquez sur le bouton **Parcourir...** pour sélectionner un certificat existant ou pour que conpal LAN Crypt en génère un nouveau.

Remarque : pour utiliser un certificat existant, celui-ci doit être disponible. Si vous utilisez un certificat logiciel, il doit être chargé dans le magasin de certificats. Si le certificat est enregistré sur une clé cryptographique, celle-ci doit être reliée au système. Pour importer un certificat, cliquez sur **Importer le certificat**.

Dans la boîte de dialogue suivante, cliquez sur **Nouveau certificat**. Sélectionnez le nouveau certificat dans la liste et cliquez sur **OK**.

Cliquez sur **Suivant**.

Dans la quatrième boîte de dialogue de l'assistant, vous pouvez saisir une région et son préfixe. Lorsque conpal LAN Crypt génère la clé, il ajoute ce préfixe au début du nom de la clé. Il utilise toujours le préfixe de la région assignée au responsable de la sécurité qui a généré la clé. Ce préfixe indique clairement pour quelle unité d'administration cette clé est utilisée. Dans Paramètres centraux, vous pouvez créer des régions supplémentaires, puis les assigner à des responsables de la sécurité différents. Cette procédure est particulièrement utile dans les environnements distribués.

Vous devez désigner un emplacement. Dans les bases de données distribuées, l'emplacement sert à assigner clairement les journaux d'événements au sein de la journalisation de la base conpal LAN Crypt.

Vous devez désigner l'emplacement même si vous n'utilisez pas une base de données distribuée. Ainsi, les entrées seront assignées clairement lorsque la base de données sera distribuée ultérieurement.

Lorsque vous cliquez sur **Terminer** conpal LAN Crypt crée le responsable principal de la sécurité et affiche la boîte de dialogue de connexion à conpal LAN Crypt Administration.

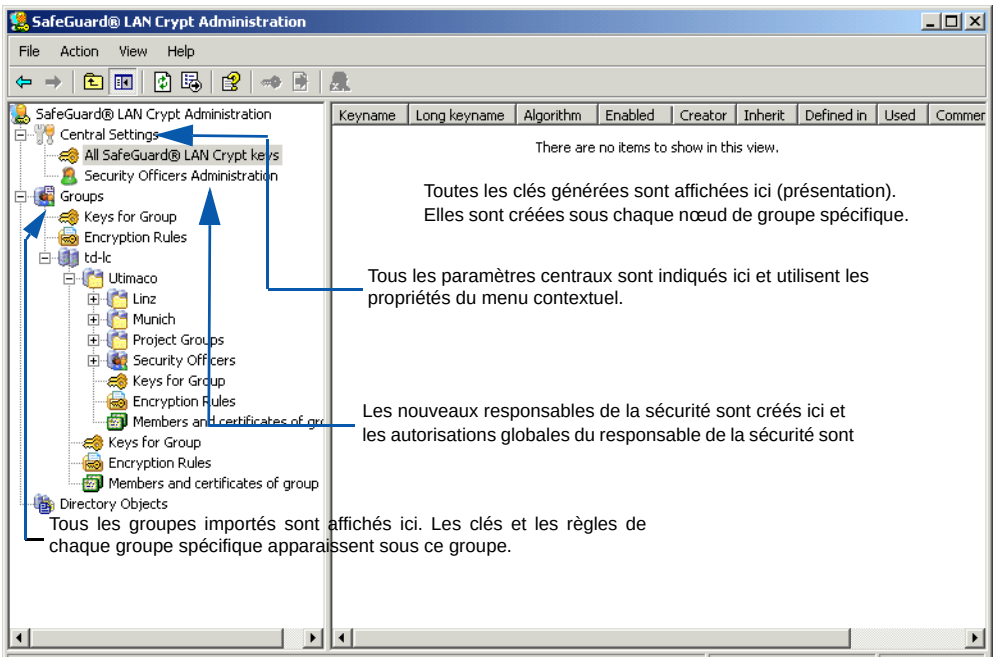
Par la suite, tous les responsables de la sécurité détenant le droit de se connecter à la base de données de conpal LAN Crypt Administration seront affichés dans cette boîte de dialogue.

Sélectionnez le responsable principal de la sécurité qui vient d'être créé et cliquez sur **OK**. conpal LAN Crypt Administration s'ouvre.

Remarque : une fois connecté, une boîte de dialogue apparaît et vous informe qu'une clé de récupération n'a pas encore été générée. Si vous ne possédez pas de clé de récupération, vous courez le risque de perdre vos données administratives et toutes les données chiffrées en cas d'urgence (par exemple, si vous perdez un certificat).
Cette boîte de dialogue s'affiche à chaque connexion d'un responsable principal de la sécurité tant qu'une clé de récupération n'a pas été générée. Si vous cochez l'option **Ne plus m'avertir**, cette boîte de dialogue ne s'affichera plus, même si aucune clé de récupération n'a été générée.

3.4 Administration : aperçu

Lorsque conpal LAN Crypt est installé, le fichier **SGLAdmin.msc** est enregistré dans le dossier d'installation de conpal LAN Crypt. Cliquez sur cette entrée via le menu de démarrage de Windows (Démarrer/Tous les programmes/...) pour ouvrir une fenêtre dans la console de gestion qui affiche uniquement les composants logiciels enfichables nécessaires à conpal LAN Crypt Administration.



Vous pouvez également ajouter le composant logiciel enfichable conpal LAN Crypt Administration à l'affichage normal de la console de gestion (Fichier\Ajouter/Supprimer un composant logiciel enfichable - conpal LAN Crypt Administration). Cet ajout du composant logiciel enfichable ne vous dispense pas du mot de passe pour la base de données conpal LAN Crypt.

Qui est connecté :
La barre d'état affiche quel responsable de la sécurité est actuellement connecté. Vous pouvez également voir s'il s'agit d'un responsable principal de la sécurité ou non.

Barre d'outils de la console Administration

De nombreuses fonctions conpal LAN Crypt apparaissent dans la barre d'outils de la console Administration. Les fonctions et le nombre d'icônes présentes dans la barre d'outils dépendent de l'onglet sélectionné.

Vous pouvez également sélectionner toutes les fonctions qui apparaissent sous forme d'icônes dans le menu contextuel correspondant.

Cliquez avec le bouton droit de la souris sur la page **conpal LAN Crypt Administration** pour afficher les propriétés du nœud et les modifier si nécessaire. Vous trouverez une description de ces propriétés dans les sections suivantes.

3.4.1 Confirmations

Dans la console conpal LAN Crypt Administration, indiquez les actions requises à confirmer avant exécution. Pour ce faire, cliquez sur **Propriétés** dans le menu contextuel du nœud racine *conpal LAN Crypt Administration*. Une boîte de dialogue affiche ces options.

Si vous sélectionnez une action, vous devrez confirmer sa sélection avant qu'elle soit exécutée. L'action ne sera pas exécutée tant que vous ne l'aurez pas confirmée.

- Confirmer la création d'une référence de groupe
  L'ajout d'une référence de groupe dans un groupe différent doit être confirmée.
  Sélectionnez le groupe > clic droit de la souris > Copier > sélectionnez un groupe différent > clic droit de la souris > Coller > Confirmation.

Remarque : toutes les opérations consistant à copier, couper et coller sont accessibles par le menu contextuel, par une action de glisser-déposer ou de glisser-déposer tout en maintenant la touche CTRL enfoncée.

- **Confirmer la création d'une référence de groupe**
  La création d'une référence pour un groupe existant doit être confirmée.
- **Confirmer le déplacement du groupe dans un autre groupe**
  Le déplacement d'un groupe dans un groupe différent doit être confirmée.
- **Confirmer la suppression du groupe de la base de données**
  La suppression d'un groupe doit être confirmée.
- **Confirmer la suppression d'un raccourci du groupe**
  La suppression d'une référence de groupe doit être confirmée.
- **Confirmer la suppression de tous les raccourcis du groupe**
  S'il existe une référence à un groupe dans un autre groupe (par exemple; si dans groupe1 et groupe2 figure un lien vers groupe3), la suppression de cette référence doit être confirmée. (sélectionnez groupe3 > clic droit de la souris > sélectionnez **Supprimer les liens**).
- **Confirmer la suppression des clés du groupe**
  La suppression des clés utilisées dans une règle de chiffrement et désactivées par la suite doit être confirmée. Les clés utilisées sont indiquées dans le composant Administration et résident dans la base de données, y compris si elles ont été supprimées d'un groupe. Les clés qui n'ont pas encore été utilisées seront également supprimées de la base de données si supprimées d'un groupe.
- **Confirmer l'ajout de la clé au groupe**
  Les clés utilisées dans une règle de chiffrement et qui ont été supprimées de tous les groupes

figurent dans la base de données et apparaissent dans *Paramètres centraux > Toutes les clés conpal LAN Crypt*. Elles peuvent ensuite être réassignées à un groupe au moyen d'un glisser-déposer. Cette action doit être confirmée.

- **Confirmer la création de la référence pour la clé dans le groupe**
  L'insertion d'un lien dans une clé d'un groupe (par exemple, en la faisant glisser et en la déposant d'un groupe dans un autre) doit être confirmée. Les clés sont toujours copiées ou un lien menant vers elles est inséré. Il est impossible de couper les clés.

- **Confirmer la suppression de la référence pour la clé dans le groupe**
  La suppression d'un lien menant vers une clé d'un groupe doit être confirmée.

Identité du responsable de la sécurité connecté

Cette boîte de dialogue affiche quel responsable de la sécurité est actuellement connecté. Le nom du responsable de la sécurité est affiché en bas de la fenêtre.
La barre d'état de conpal LAN Crypt Administration affiche quel responsable de la sécurité est actuellement connecté.

3.4.2 Paramètres d'utilisateurs

L'onglet **Paramètres d'utilisateurs** conditionne l'affichage des informations dans le module conpal LAN Crypt Administration.

Activez

- *Ajouter le nom de domaine à chaque nom de groupe*, pour afficher la relation entre les groupes conpal LAN Crypt et les domaines dans le module conpal LAN Crypt Administration. Cette option est particulièrement utile si conpal LAN Crypt doit être utilisé dans plusieurs domaines.

- *Afficher les"Utilisateurs et certificats sélectionnés"* pour afficher tous les utilisateurs (et leurs certificats) qui ont été importés dans conpal LAN Crypt sous le nœud *Paramètres centraux*. L'affichage des utilisateurs et des certificats peut prendre plusieurs minutes pour les installations importantes. Vous devez ensuite redémarrer conpal LAN Crypt Administration de façon à appliquer les modifications apportées à l'option *Afficher les "Utilisateurs et certificats sélectionnés"*.

- *Afficher les parents des utilisateurs* pour afficher le groupe parent d'un utilisateur en particulier sous le nœud *Membres et certificats du groupe*. Ceci permet de déterminer si la base de données conpal LAN Crypt contient des utilisateurs qui ne sont assignés à aucun groupe. Vous devez ensuite redémarrer conpal LAN Crypt Administration de façon à appliquer les modifications apportées à l'option *Afficher le parent utilisateur*.

- *Désactiver la mise en cache des listes utilisateur*
  Afin d'améliorer les performances, conpal LAN Crypt crée généralement des listes d'utilisateurs à l'arrière-plan et poursuit leur création lorsqu'un utilisateur passe à un autre

nœud dans le module Administration. Les résultats de ces listes sont placés en mémoire tampon, de façon à réduire les appels à la base de données lors de la consultation de la liste. Cette fonction permet de gagner beaucoup de temps, notamment pour les listes volumineuses. Cependant, dans les environnements comportant plusieurs administrateurs conpal LAN Crypt en parallèle (Terminal Server), ceci risque de nécessiter davantage de mémoire. Pour contourner ce problème, activez cette option. Ainsi, les listes ne sont plus placées en mémoire tampon et la création de la liste se termine lorsque l'utilisateur quitte le noeud ou passe à un autre.
Nous recommandons de n'utiliser cette option que si la mémoire disponible devient insuffisante.
Les modifications apportées à la base de donnés au cours de la même session ne sont pas reportées de façon automatique dans une liste.
Vous pouvez mettre les modifications à jour à tout moment en appuyant sur F5.

Remarque : les modifications apportées aux paramètres mentionnés ci-dessus ne sont pas stockées dans la base de données. Il s'agit de paramètres personnels qui sont enregistrés pour chaque utilisateur dans le composant logiciel enfichable MMC (Microsoft Management Console).

3.5 Paramètres centraux

Dans l'onglet *Paramètres centraux*, définissez de manière centrale les différentes propriétés de conpal LAN Crypt Administration.

À cet effet, cliquez sur **Propriétés** dans le menu contextuel du nœud *Paramètres centraux*. Vous pouvez aussi opérer cette sélection en cliquant sur l'icône "Propriétés" dans la barre d'outils de conpal LAN Crypt Administration. Ces propriétés sont accessibles à partir des différents onglets et peuvent être modifiées, si nécessaire.

Remarque : seul le responsable principal de la sécurité peut afficher la page Autorisation supplémentaire et les onglets Clé de récupération et Régions.
Seuls les responsables de la sécurité détenant le droit global de modifier la configuration peuvent afficher les onglets Serveur et Configuration. Le droit global permettant de modifier la configuration s'applique également à la modification des chemins dans l'onglet Répertoires.
Seuls les responsables principaux de la sécurité peuvent procéder à des changements dans les onglets *Algorithme*, Certificats et Résolution des règles.

3.5.1 Onglet Algorithmes

conpal LAN Crypt propose les algorithmes de chiffrement suivants :

- AES-128

- **AES-256**
- **3DES**
- **DES** (déconseillé)
- **IDEA**
- **XOR** (déconseillé)

Sélectionnez les algorithmes que vous souhaitez utiliser. Lorsque vous générerez ultérieurement des clés différentes, vous pourrez utiliser les algorithmes que vous avez sélectionnés ici.

Remarque : en cas de modification ultérieure de ces paramètres (par exemple, si DES est supprimé de la liste des algorithmes disponibles), cela n'aura aucun effet sur les clés précédemment générées ou les données chiffrées associées à ces clés.
En cas de répercussion sur un algorithme, ce dernier sera tout simplement indisponible lorsque vous générerez une nouvelle clé.

Algorithme par défaut

Vous sélectionnez ici l'algorithme à utiliser par défaut pour générer automatiquement les clés des utilisateurs et des groupes.

3.5.2 Onglet Clés

Clés

Des problèmes liés aux noms de clés internes dupliqués peuvent se produire lorsque plusieurs installations conpal LAN Crypt sont réunies, par exemple lors de la fusion de deux entreprises ou services.
Par conséquent, chaque clé est identifiée par son propre identifiant global unique (GUID). Le GUID est généralement généré de façon aléatoire par conpal LAN Crypt et ne peut plus être modifié par la suite.

Cependant, si des fichiers qui ont été chiffrés avec conpal LAN Crypt doivent être échangés avec une autre société, vous devez appliquer une méthode permettant de générer une clé commune. C'est la seule façon de s'assurer qu'un fichier chiffré avec, par exemple, la clé CRYPTOCLE de la société A peut également être déchiffrée par la société B. Pour ce faire, la société B doit également générer une clé appelée CRYPTOCLE qui reprend les mêmes paramètres que la clé de la société A. Ceci inclut également le GUID de la clé.

Pour remédier à cette situation, conpal LAN Crypt dispose d'une option qui permet d'entrer manuellement le GUID lors de la génération d'une clé. Pour cela, activez simplement l'option **Autoriser les responsables de la sécurité à définir la GUID des nouvelles clés** (**GUID aléatoire par défaut**).

Valeur de la clé

Si vous activez l'option spécifiant que **seuls les responsables de la sécurité disposant du droit "Générer un profil" sont habilités à générer les clés** (**les clés sans valeur *ne sont pas* autorisées**), vous pouvez vous assurer que seuls les responsables disposant des droits *Créer une clé* et *Générer un profil* peuvent générer des clés (nom et valeur).

conpal LAN Crypt vous autorise à générer des clés sans valeur. Vous pouvez utiliser ces clés sans restrictions dans la console Administration. Leurs valeurs sont générées lorsque vous créez les fichiers de stratégie pour les utilisateurs. Toutefois, cela peut s'avérer problématique si vous utilisez une base de données distribuée. Par exemple : Si les fichiers de stratégie qui contiennent des clés sans valeur (créées manuellement sans valeur <GROUPKEY>) sont générés dans une fenêtre de temps de réplication sur des sites différents. Si des fichiers de stratégie sont générés sur chaque site, une valeur différente sera générée pour la clé. Il en résulterait une clé avec deux valeurs différentes.

Si vous cochez l'option spécifiant que **seuls les responsables de la sécurité disposant du droit "Générer un profil" sont habilités à générer les clés** (**les clés sans valeur *ne sont pas* autorisées**), (les clés sans valeur ne sont pas autorisées), seuls les responsables de la sécurité disposant des droits *Générer une clé* et *Générer un profil* peuvent générer des clés. Ils ne peuvent plus générer de clés sans valeur. Si le responsable de la sécurité ne désigne pas une valeur à la création de la clé, la valeur est générée automatiquement lorsque la clé est enregistrée.

Pour les clés de groupe dont les valeurs sont générées à la création de fichiers de stratégie, leurs valeurs sont également générées automatiquement lorsqu'elles servent à créer une règle de chiffrement.

Si cette option est activée, les responsables de la sécurité qui ne détiennent pas le droit *Créer des profils* ne seront pas en mesure de générer des clés.

Ils ne pourront pas non plus utiliser des clés de groupe (<GROUPKEY>) dans les règles de chiffrement.

Remarque : l'option spécifiant que **seuls les responsables de la sécurité disposant du droit "Générer un profil" peuvent générer des clés** (**les clés sans valeur *ne sont pas* autorisées**) n'a pas d'incidence sur le mode d'utilisation des clés spécifiques aux utilisateurs (<USERKEY>) dans les règles de chiffrement !

3.5.3 Onglet Certificats

Vous indiquez ici la longueur (1024, 2048, 4096 bits) et la validité des clés pour les nouveaux certificats générés par conpal LAN Crypt.

Sous Nom convivial des nouveaux certificats, vous pouvez spécifier un nom pour les certificats créés par conpal LAN Crypt. Tous les certificats portent ce nom et peuvent donc facilement être identifiés comme certificats conpal LAN Crypt.

Si vous activez l'option **Ajouter les extensions critiques aux nouveaux certificats**, une extension critique qui indique à d'autres applications qu'elles ne doivent pas utiliser ces certificats, est ajoutée aux certificats nouvellement générés.

Vous pouvez également renseigner une période d'alerte, en jours, pendant laquelle le système affichera un avertissement (si les règles sont annulées ou en surlignant en jaune les certificats de la liste).

3.5.4 Onglet Résolution des règles

Ignorer les utilisateurs sans certificat valide lors de la résolution

(Dans cette section, "annuler" signifie "ignorer" lorsqu'on parle de règles). Sélectionnez cette option si vous voulez que le système ignore les utilisateurs sans certificats assignés au moment de la création des fichiers de stratégie. Aucun fichier de stratégie ne sera donc généré pour ces utilisateurs.

Remarque : en cas de création d'un utilisateur, d'activation de cette option et de certificat non encore assigné à l'utilisateur, le système n'affichera pas d'alerte s'il est incapable de créer des fichiers de stratégie pour cet utilisateur pendant la définition (l'application) des règles de chiffrement.

Sélectionner l'ordre dans lequel les règles doivent être classées sur le client :

Remarque : ce paramètre est seulement appliqué aux clients de la version 3.90 ou versions supérieures.

Vous pouvez ici choisir parmi trois différentes méthodes de tri. La méthode de tri 3, celle par défaut, est utilisée par les versions du client au-dessous de la version 3.90 :

- **Méthode de tri 1**
  1. Règles d'ignorance
  2. Règles d'exclusion
  3. Règles de chiffrement

- **Méthode de tri 2**
  1. Règles d'ignorance
  2. Règles d'exclusion
  3. Règles de chiffrement spécifiées comme chemins absolus sans caractères génériques
  4. Règles de chiffrement spécifiées comme chemins absolus avec caractères génériques n'incluant pas les sous-dossiers
  5. Règles de chiffrement spécifiées comme chemins absolus avec caractères génériques incluant les sous-dossiers
  6. Toutes les autres règles de chiffrement

  Un chemin absolu est un chemin UNC (commençant par une double barre oblique inverse) ou <lettre de lecteur>:\

Par exemple : \\serveur\partage*.* ou c:\chiffrer*.*.

- **Méthode de tri 3 (par défaut)**
  La méthode de tri 3 ne fait pas de distinction entre les règles d'ignorance, d'exclusion et de chiffrement.
  Les règles sont triées dans l'ordre suivant :
  1. Tous les chemins absolus sans caractères génériques
  2. Tous les chemins absolus avec caractères génériques n'incluant pas les sous-dossiers
  3. Tous les chemins absolus avec caractères génériques incluant les sous-dossiers
  4. Toutes les autres règles

  Un chemin absolu est un chemin UNC (commençant par une double barre oblique inverse) ou <lettre de lecteur>:\
  Par exemple : \\serveur\partage*.* ou c:\chiffrer*.*.

Dans l'une des sections ci-dessus (par exemple : Méthode de tri 3 - Toutes les autres règles), les règles sont ordonnées en fonction de la précision de la définition du chemin.

L'ordre et le suivant :
1. Chemins UNC
2. Chemins commençant par <lettre du lecteur>: La barre oblique inverse après la lettre de lecteur n'est ici pas considérée.
2. Tous les autres chemins
En outre :
- Les chemins comportant davantage de barres obliques inverses apparaissent avant ceux en comportant moins
- Les chemins sans caractères joker apparaissent avant les chemins avec les caractères joker *. et *.*

Remarque : les modifications apportées à cette option option ne prennent effet sur les clients que lorsque les nouveaux profils sont générés et distribués.

Sélectionner le format de chiffrement qui doit être utilisé par le client conpal LAN Crypt.

Configurez ici le mode de chiffrement des fichiers utilisé par les clients. conpal LAN Crypt prend en charge les modes de chiffrement suivants :

- Format CBC (version 3.50 ou supérieure)
  Ce format est utilisé par les versions client 3.50 et versions supérieures. Ces clients peuvent lire des fichiers chiffrés en mode OFB (ancien format). Le mode de chiffrement des nouveaux fichiers est CBC.

- Format XTS-AES (version 3.90 ou supérieure)
  Ce format peut être utilisé par les versions 3.90 et versions supérieures du client. Ces clients peuvent lire des fichiers chiffrés en mode OFB et CBC. Le mode de chiffrement des nouveaux fichiers est XTS-AES. Ce mode est uniquement utilisé pour les clés AES. Si un fichier est chiffré avec une clé utilisant un autre algorithme, c'est le mode de chiffrement CBC qui sera utilisé.

Pour les versions du client au-dessous de la version 3.90, seule la configuration suivante s'applique :
Format CBC pour le chiffrement avec utilisation facultative de l'ancien format ou "ancien format de chiffrement". Tous les autres paramètres sont ignorés par ces clients. Ils utilisent le format CBC ou l'ancien format par défaut.

Utiliser ce format de fichier de chiffrement jusqu'à une date définie

Lors d'un processus de mise à niveau, un mode de chiffrement ancien peut être configuré. Cet ancien de mode de chiffrement est actif jusqu'à une date définie. En commençant par cette date, tous les clients doivent être migrés pour prendre en charge le mode de chiffrement des fichiers configurés. Sinon, les nouveaux clients créent des fichiers chiffrés à l'aide du mode configuré, mais ces fichiers ne peuvent pas être lus par de plus anciens clients.

En fonction du paramétrage pour que le format de chiffrement soit utilisé, les formats suivants peuvent être sélectionnés ici :

- **Ancien format** (**versions 2.x, 3.0x, 3.1x**)
- **Format CBC** (**version 3.50 ou supérieure**)
  est uniquement disponible si XTS-AES est configuré au format des fichiers de chiffrement.

CBC nécessite une version client 3.90 ou supérieure. Les plus anciens clients évaluent seulement le paramètre **Utiliser ce format de fichier de chiffrement jusqu'à une date définie**, si l'**Ancien format** est sélectionné.

Vous devez spécifier jusqu'à quelle date l'ancien format doit être appliqué pour chiffrer les fichiers. Après cette date, ou si cette option est dessélectionnée, les fichiers sont écrits à l'aide du nouveau format de chiffrement. Toute modification apportée à cette option ne prend effet sur les clients que lorsque les nouveaux profils sont générés et distribués.

Après que tous les clients ont été mis à jour, nous vous recommandons d'exécuter le chiffrement initial avec l'outil de chiffrement initial. Vous vous assurez ainsi que seul le format de chiffrement conpal LAN Crypt est utilisé.

Ce changement est pris en compte à la prochaine application des règles de chiffrement.

3.5.5 Onglet Serveur

Pour importer des groupes et des utilisateurs à partir d'un serveur, conpal LAN Crypt exige les données de connexion à ce serveur. Vous devez entrer ces informations dans l'onglet Serveur. Cliquez sur **Ajouter** pour ouvrir une autre boîte de dialogue contenant trois onglets : *Détails*, *Préférences* et *Certificats*

Détails du serveur : connexion par mot de passe

1. Entrez le *Nom du domaine ou du serveur*, le *Nom d'utilisateur* et le *Mot de passe* correspondant.

Pour éviter les doublons, saisissez également un autre nom servant d'*Alias* pour le serveur au cas où plusieurs noms peuvent accéder au même serveur.

Remarque : si vous utilisez un **Service d'annuaire Microsoft**, procédez comme suit :

- Saisissez le `nom du domaine` sous *Nom du domaine ou du serveur*.
- Saisissez le *nom d'utilisateur* sous la forme `nom d'utilisateur@domaine`.

Remarque : le nom d'utilisateur doit être saisi dans la syntaxe LDAP (nom canonique) afin d'importer des objets depuis un service d'annuaire non lié à Microsoft.
Exemple : `cn=admin,O=techops`

2. Spécifiez l'API à utiliser.
   Sélectionnez <Microsoft> ou <autre> dans la liste déroulante. Le paramètre fictif <autre> vaut pour toutes les API non liées à Microsoft.
3. Spécifiez la méthode d'authentification LDAP à utiliser pour accéder au serveur. conpal LAN Crypt propose les méthodes suivantes :
   - Mot de passe (LDAP)
   - Mot de passe (LDAP avec SSL)
4. Cliquez sur **OK**.

▶ Le serveur apparaît dans la table sous l'onglet *Serveur*.

Message d'erreur après échec de connexion
Si conpal LAN Crypt ne peut pas se connecter au serveur, un message d'erreur s'affiche dans conpal LAN Crypt Administration.

Détails du serveur : connexion anonyme

1. Entrez le *Nom de serveur*. Pour éviter les doublons, saisissez également un autre nom servant d'*Alias* pour le serveur au cas où plusieurs noms peuvent accéder au même serveur.
2. Spécifiez l'API à utiliser.
   Sélectionnez <Microsoft> ou <autre> dans la liste déroulante. Le paramètre fictif <autre> vaut pour toutes les API non liées à Microsoft.
3. Spécifiez la méthode d'authentification LDAP à utiliser pour accéder au serveur. conpal LAN Crypt propose les méthodes suivantes pour la connexion anonyme :
   - Anonyme (LDAP)
   - Anonyme (LDAP avec SSL)
4. Cliquez sur OK.

▶ Le serveur apparaît dans la table sous l'onglet *Serveur*.

Message d'erreur après échec de connexion
Si conpal LAN Crypt ne peut pas se connecter au serveur, un message d'erreur s'affiche dans conpal LAN Crypt Administration.

Paramètres

Identification d'un objet

conpal LAN Crypt utilise un identifiant GUID (Global Unique ID) précis et invariable pour identifier les objets importés dans Active Directory. Cet identifiant GUID sert également à synchroniser la base de données et le service d'annuaire étant donné que les noms des différents objets uniques peuvent changer, afin de garantir la mise en miroir dans la base de données des mises à jour dans Active Directory et qu'aucun objet nouveau ne soit créé dans la base de données en raison d'un nouveau nom dans Active Directory.

Cependant, d'autres services d'annuaire n'utilisent pas ce type d'identifiant. Dans ce cas, conpal LAN Crypt offre un autre moyen d'identifier les objets sans ambiguïté. Vous pouvez configurer conpal LAN Crypt de sorte que certains attributs LDAP servent à une identification unique des objets. Vous configurez ces attributs dans conpal LAN Crypt Administration.

Les paramètres `<par défaut>` et `<autre>` sont toujours disponibles. Généralement, le paramètre `<par défaut>` est suffisant pour le serveur concerné. Les attributs évalués par le paramètre `<par défaut>` sont toujours affichés en dessous de `<par défaut>`. Cela vous permet de visualiser les attributs évalués dans la configuration par défaut. Vous pouvez également assigner un attribut spécifique si tous ces attributs sont déjà présents dans le service d'annuaire concerné. Choisissez `<autre>` pour désigner un attribut différent de ceux déjà affichés.

Remarque : lorsque vous choisissez un attribut, assurez-vous qu'il contient toutes les données nécessaires à une identification de l'objet sans ambiguïté.

- **Objet GUID**

  Vous désignez ici l'attribut utilisé pour l'identification.
  Si vous laissez le paramètre sur `<par défaut>`, les deux attributs, `GUID` et `objectGUID` sont évalués.
  Si vous voulez utiliser un autre attribut LDAP pour identifier les objets, sélectionnez `<autre>` sous *Objet GUID* et saisissez le nom de l'attribut LDAP dans le champ de saisie qui se trouve à côté. Cet attribut doit contenir les données qui permettront une identification de l'objet sans ambiguïté.

- **L'attribut GUID a une valeur binaire**

  Cette option concerne uniquement le mode d'affichage de l'objet GUID dans la boîte de dialogue*Propriétés* correspondante. Pour obtenir un affichage correct, cochez cette option si l'attribut GUID que vous utilisez a une valeur binaire.

En cas de doute, cochez cette option.

Attributs des utilisateurs

- **Attribut pour le nom d'utilisateur**
  Ce paramètre concerne uniquement le mode d'affichage des utilisateurs dans la console conpal LAN Crypt Administration. Les utilisateurs sont affichés dans la boîte de dialogue *Propriétés* d'un groupe et dans le composant logiciel enfichable *Utilisateur et certificats*. Vous pouvez sélectionner un des attributs existants ou saisir un attribut LDAP en sélectionnant <autre>.
  `<par défaut>` évalue (`CN` et `SN`).

- **Attribut du nom de connexion**
  Mention spéciale associée à l'attribut du nom de connexion. conpal LAN Crypt nomme les fichiers de stratégie en fonction du nom de connexion de l'utilisateur. L'utilisateur peut uniquement se connecter si son nom de connexion et le nom du fichier de stratégie sont identiques.
  Vous désignez ici l'attribut LDAP qui est utilisé pour définir le nom de connexion de l'utilisateur.
  `<par défaut>` évalue `SAMAccountName`, `userPrincipalName` et `UID`. Si deux ou trois de ces attributs sont déjà présents dans le service d'annuaire, vous pouvez sélectionner celui qui définit le nom de connexion de l'utilisateur.
  Choisissez `<autre>` pour désigner un autre attribut de service d'annuaire qui contient le nom de connexion.

Remarque : si le nom dans l'attribut contient le caractère @, conpal LAN Crypt coupe le nom à ce niveau. Cela peut s'avérer problématique, notamment si des adresses de messagerie sont utilisées.

- **Attribut d'adresse de messagerie**
  Cet attribut est ajouté pour les certificats autogénérés.

- **Attribut de commentaire**
  Tout comme pour l'adresse électronique, cet attribut permet d'identifier les objets utilisateur. Ceci est particulièrement utile lorsque le nom d'utilisateur et le nom de connexion ne peuvent pas être utilisés par l'assistant pour identifier des objets lorsque des certificats sont assignés. À ce stade, vous pouvez entrer le nom de l'attribut que l'assistant doit utiliser pour identifier le bon utilisateur lorsque des certificats sont assignés.

Remarque : si des attributs vides sont importés lors de la synchronisation (par exemple en raison du fait qu'un attribut a été supprimé dans l'AD), les commentaires conpal LAN Crypt ne sont pas affectés. Les entrées existantes sont conservées. Les nouveaux contenus d'attributs remplacent

les commentaires existants.
Si vous sélectionnez <par défaut>, les commentaires ne sont pas importés.

Certificats

Dans l'onglet *Certificats*, indiquez si les certificats assignés à l'utilisateur dans l'annuaire LDAP doivent être transférés au moment de l'importation de l'utilisateur dans la base de données conpal LAN Crypt.
Vous n'avez alors plus besoin d'assigner des certificats à ces utilisateurs dans conpal LAN Crypt Administration. Dans cet onglet, vous pouvez également spécifier un attribut contenant le certificat de l'utilisateur.

Remarque : les certificats assignés de cette manière ne sont pas vérifiés (date d'expiration, sur une CRL, etc.).

Activez l'option

- **Assigner automatiquement les certificats à l'importation**

si vous voulez que les certificats de l'annuaire LDAP soient automatiquement importés et assignés à l'utilisateur lorsqu'ils sont importés dans la base de données conpal LAN Crypt.

`<par défaut>` évalue `userCertificate` et `UserCertificate; binaire`.
Cliquez sur `<autre>` pour choisir un autre attribut contenant le certificat.

Lorsque vous cliquez sur **OK**, conpal LAN Crypt transfère les données de connexion à la liste des serveurs.
Vous pouvez aussi modifier ou supprimer ces détails dans la liste.

3.5.6 Onglet Répertoires

Remarque : les paramètres définis dans cet onglet sont toujours enregistrés dans le dossier de configuration en cours du responsable de la sécurité. Si aucun dossier de configuration n'a été créé, le système utilise le dossier <DEFAULT CONFIGURATION>.

Emplacement de stockage pour les fichiers de stratégie créés

Vous devez indiquer où doivent être enregistrés les fichiers de stratégie générés pour les utilisateurs.

Saisissez l'emplacement de stockage (généralement une unité de réseau partagée avec l'utilisateur) dans le champ de saisie. Le nom de dossier que vous saisissez doit déjà exister.

Remarque : vérifiez que l'utilisateur peut accéder à ce dossier car les fichiers de stratégie (POL) créés sont chargés ou copiés à partir de ce dossier lorsque l'utilisateur se connecte.

Remarque : vous devez également indiquer l'emplacement de stockage des fichiers de stratégie du point de vue du client. Ce paramètre est accessible dans conpal LAN Crypt Configuration.

Remarque : vous devez également indiquer l'emplacement de stockage des fichiers de stratégie du point de vue du client. Ce paramètre est accessible dans conpal LAN Crypt Configuration.

Options des fichiers de stratégie - spécification du format de fichier de stratégie

Si vous utilisez différentes versions du client conpal, assurez-vous que tous vos clients conpal peuvent lire les fichiers de stratégie générés. conpal LAN Crypt prend en charge plusieurs formats de fichier de stratégie :

- Créer les anciens fichiers de stratégie (.pol)
  Versions du client conpal LAN Crypt antérieures à la version 3.12.1
- Créer les anciens fichiers de stratégie (par défaut)
  Versions du client conpal LAN Crypt antérieures à la version 3.90
- Créer les nouveaux fichiers de stratégie (.xml.bz2)
  Version 3.90 ou versions supérieures du client conpal LAN Crypt

Sélectionner le format couvrant tous vos clients.

Créer les fichiers de stratégie supplémentaires selon le nom Novell

Si vous activez cette option, conpal LAN Crypt génère deux fichiers de stratégie pour chaque utilisateur. Un fichier comporte le nom de connexion Novell et l'autre le nom d'utilisateur Windows. Ces fichiers ont des contenus identiques.

L'utilisation du nom de connexion Novell doit aussi être indiqué dans la configuration ou les Paramètres de client LAN Crypt avant que vous puissiez l'utiliser pour vous connecter.

Remarque : ce paramètre affecte le mode de suppression des profils dans la console conpal LAN Crypt Administration. La procédure de suppression des profils est similaire à celle de leur création. Si le nom de connexion Novell doit être utilisé ici (deux fichiers de stratégie créés), les deux profils seront effacés si ce paramètre n'est pas modifié. La suppression consiste ici à générer des fichiers de stratégie vides. Si le paramètre est changé à l'exécution, il est possible que, bien que deux fichiers de stratégie aient été créés, seul celui portant le nom d'utilisateur Windows soit supprimé. Cela s'explique par le fait que le paramètre a été désactivée, seul le fichier de stratégie portant le nom d'utilisateur Windows est donc supprimé. Le fichier de stratégie Novell reste dans l'emplacement de stockage défini et en théorie peut être utilisé pour la connexion. Le système réagira de manière similaire si l'option **Compresser les fichiers de stratégie** a été activée. Dans ce cas, jusqu'à quatre fichiers de stratégie sont générés pour chaque utilisateur.
Si besoin, n'oubliez pas d'effectuer la coordination avec l'administrateur du système.

Emplacement de stockage pour les certificats et les fichiers de clés créés (*.p12)

Le cas échéant, conpal LAN Crypt peut également générer des certificats autosignés. Ces certificats (fichiers .p12) sont générés lors de l'assignation de certificats aux utilisateurs.

L'emplacement dans lequel ces fichiers doivent être enregistrés est à spécifier dans l'onglet Répertoires.

C'est également l'endroit où est enregistrée la partie publique du certificat du responsable de la sécurité (.cer) qui sert à sécuriser la base de données d'administration.

Les fichiers de clés (.p12) et la partie publique du certificat du responsable de la sécurité doivent être mis à la disposition des utilisateurs.

Dans conpal LAN Crypt Configuration, désignez le dossier dans lequel conpal LAN Crypt doit rechercher un fichier .p12 pour l'utilisateur si la clé privée du fichier de stratégie n'est pas présente. La même procédure s'applique à la partie publique du certificat du responsable de la sécurité.

Afin que conpal LAN Crypt reconnaisse automatiquement les fichiers de clés de l'utilisateur, les noms des fichiers doivent correspondre au nom de connexion de l'utilisateur (`"Nomconnexion.p12"`).

Lorsque conpal LAN Crypt trouve le fichier correspondant, il affiche une boîte de dialogue avec les codes PIN. Vous devez envoyer à l'utilisateur un courrier d'information sur son code PIN (contenu dans le fichier journal des mots de passe). Le certificat et la clé associée sont automatiquement importés après la saisie du code par l'utilisateur.

Si conpal LAN Crypt trouve un fichier .cer contenant la partie publique du certificat du responsable de la sécurité, il l'importe automatiquement.

Remarque : avant de pouvoir exploiter cette fonctionnalité, vous devez définir les chemins adaptés dans conpal LAN Crypt Configuration.

Vous pouvez aussi distribuer manuellement les fichiers de clés des utilisateurs et la partie publique du certificat de l'administrateur. Dans ce cas, assurez-vous que les clients importent les deux.

Remarque : les clients doivent importer la partie publique du certificat du responsable de la sécurité qui a généré les fichiers de stratégie.
Si vous modifiez le chemin sous lequel sont enregistrés les fichiers .cer des responsables de la sécurité et les fichiers .p12 des utilisateurs après avoir créé les responsables de la sécurité, vous devez copier leurs fichiers .cer dans le nouvel emplacement. Sinon, il sera impossible de trouver les parties publiques des certificats des responsables de la sécurité.

Mot de passe par défaut pour les fichiers de clés des utilisateurs

Dans conpal LAN Crypt, vous pouvez définir un mot de passe uniforme pour tous les fichiers de clés des utilisateurs.

À cet effet, copiez un fichier contenant le mot de passe souhaité (32 caractères au maximum) dans le répertoire qui contient le fichier journal des mots de passe (see *Fichier journal des mots de passe des fichiers de clés* on page 51).

Le fichier contenant le mot de passe doit porter le même nom que le fichier journal correspondant pour les mots de passe (nom par défaut : p12pwlog.csv) mais son extension doit être .pwd (comme pour le nom par défaut du fichier journal des mots de passe : p12pwlog.pwd). Si le système trouve ce type de fichier, tous les fichiers de clés créés pour les utilisateurs auront ce mot de passe.

Dans ce fichier, si vous entrez `*logonname*` comme mot-clé, à la place du mot de passe par défaut, le nom de connexion en vigueur est utilisé comme mot de passe.

Remarque : un mot de passe aléatoire est TOUJOURS attribué aux fichiers .p12 des responsables de la sécurité en raison de leur niveau de sécurité élevé.

Emplacement pour les certificats des responsables de la sécurité (*.p12)

conpal LAN Crypt stocke les certificats des responsables de la sécurité dans des fichiers .p12, par exemple sous forme de sauvegarde. Vous pouvez désigner ici dans quel dossier ils seront enregistrés.

Remarque : ils contiennent des données sensibles ; il est donc essentiel que vous les protégiez contre les accès non autorisés !

Fichier journal des mots de passe des fichiers de clés

Vous désignez ici l'emplacement de stockage et le nom du fichier journal des fichiers de clés PKCS#12 créés (nom par défaut : p12pwlog.csv). Ce fichier contient les mots de passe des fichiers de clés PKCS#12 générés et peut servir par exemple à créer un courrier contenant les codes PIN.

Le fichier .csv contient les informations suivantes (les mots-clés entre parenthèses correspondent aux en-têtes des colonnes du fichier.csv) :

- Date de création (`CreateDate`)
- Heure de création (`CreateTime`)
- Date d'expiration (`ExpirationDate`)
- Heure exacte d'expiration de la validité (`ExpirationTime`)
- Nom d'utilisateur (`Name`)
- Nom de connexion (`Logonname`)
- Adresse de messagerie (`EMail`)
- Mode de création (`Mode`). Les valeurs possibles sont les suivantes :
  Le certificat `<GUI>` a été généré dans la boîte de dialogue *Propriétés* de l'utilisateur.

Le certificat `<SO>` d'un responsable de la sécurité. Il a été généré lorsque le responsable de la sécurité a été créé.
Le certificat `<WIZARD>` a été généré à l'aide de l'assistant d'assignation de certificats.

- Nom du fichier (`FileName`)
- Mot de passe (`Password`)

Remarque : vous devez protéger ce fichier et ne jamais l'enregistrer dans le même dossier que les fichiers POL.

Remarque : si l'utilisateur procédant à l'assignation de certificats ne détient pas le droit de modifier le fichier journal des mots de passe, conpal LAN Crypt ne sera pas en mesure de créer les certificats.

3.5.7 Onglet Régions

conpal LAN Crypt vous permet de définir des régions pour faciliter et simplifier l'administration des clés. Chaque région est assignée à un responsable de la sécurité spécifique qui en est responsable. Lorsque ce responsable de la sécurité crée des clés, le système ajoute automatiquement le préfixe de cette région au début du nom des clés. Vous pouvez donc toujours savoir pour quelle unité administrative cette clé a été créée. Cette procédure est particulièrement utile dans les environnements distribués.

Entrez le nom et le préfixe des régions dans les champs de saisie correspondants. Cliquez sur **Ajouter** pour ajouter une nouvelle région à la liste des régions existantes. Vous pouvez sélectionner les régions affichées lorsque vous créez un responsable de la sécurité.

Pour modifier ou supprimer une région existante, sélectionnez la région concernée puis cliquez sur **Edition** ou **Supprimer**.

Remarque : vous pouvez supprimer une région seulement si elle n'est pas assignée à un responsable de la sécurité.

3.5.8 Onglet Configurations

Cet onglet vous permet de créer des dossiers de configuration particuliers à chaque région, puis de les assigner à un responsable de la sécurité.

Les dossiers de configuration contiennent toutes les données à saisir dans l'onglet *Répertoires* :

- l'emplacement de stockage pour les fichiers de stratégie créés ;
- l'emplacement de stockage pour les certificats et les fichiers de clés créés ;
- l'emplacement de stockage pour les certificats des responsables de la sécurité créés ;

- l'emplacement de stockage et le nom du fichier journal des mots de passe
- les options des fichiers de stratégie

Les dossiers de configuration sont toujours assignés à une région existante. Normalement, un responsable de la sécurité assigné à une région peut utiliser uniquement les dossiers de configuration générés pour cette région. Le dossier <DEFAULT CONFIGURATION> constitue l'exception puisqu'il peut être utilisé dans chaque région.

En choisissant une configuration particulière pour une OU (région), vous vous assurez que les chemins corrects seront définis pour un ou plusieurs responsables de la sécurité et que tous les responsables de la sécurité utiliseront les mêmes chemins pour enregistrer les fichiers créés.

Toutes les modifications apportées à l'onglet *Répertoires* sont toujours enregistrées dans le dossier de configuration actuellement assigné.

Remarque : le droit global Modifier la configuration indique si un responsable de la sécurité a le droit de modifier sa propre configuration. S'il ne détient pas ce droit, il peut seulement utiliser les chemins sélectionnés.
Si un responsable de la sécurité modifie un dossier de configuration existant, il modifie la configuration de tous les responsables de la sécurité assignés à cette configuration.

Création d'un dossier de configuration

Pour créer un dossier de configuration, procédez ainsi.

1. Sélectionnez une région existante pour laquelle vous voulez créer le dossier de configuration ou choisissez <Pas de région> pour créer un dossier de configuration auquel vous assignerez des responsables de la sécurité assignés à aucune région.
2. Dans *Nouveau nom*, saisissez le nom du nouveau dossier de configuration.
3. Sélectionnez un dossier de configuration existant dans la liste.
   Le système copie ce dossier de configuration et l'enregistre avec le nouveau nom. Cliquez sur **Copier**.
4. Pour modifier le dossier de configuration, sélectionnez-le et cliquez sur **Edition**.
5. Une boîte de dialogue s'affiche, identique à l'onglet *Répertoires* dans *Propriétés*. Saisissez les noms de chemins adéquats et définissez les options de fichier de stratégie. Cliquez sur OK.
6. Le système affiche ensuite le nouveau dossier de configuration dans la liste, dans la région concernée, et vous pouvez l'utiliser pour créer plus de responsables de la sécurité. Pour modifier la configuration (et la région) d'un dossier de configuration existant, sélectionnez l'onglet *Propriétés* du responsable de la sécurité concerné.
7. Vous pouvez créer autant de dossiers de configuration supplémentaires que nécessaire.

3.5.9 Onglet Autorisation supplémentaire

conpal LAN Crypt vous permet de définir les opérations exigeant l'autorisation supplémentaire d'au moins un responsable de la sécurité. Une autorisation supplémentaire peut être demandée pour les opérations suivantes :

Opération	Autorisations nécessaires
Modifier les paramètres d'autorisation supplémentaire	Réalisable uniquement par un responsable principal de la sécurité.
Modifier la clé de restauration	Réalisable uniquement par un responsable principal de la sécurité.
Les opérations suivantes peuvent être effectuées uniquement par les responsables qui détiennent le droit global d'autoriser les opérations et ont le droit d'exécuter l'action. **IMPORTANT :** Dans certains cas, il n'est pas suffisant de détenir le droit global d'autorisation supplémentaire. En effet, le responsable de la sécurité accordant l'autorisation supplémentaire doit posséder le droit correspondant pour cet objet spécifique.	
Modifier les paramètres globaux	Requiert le droit global **Modifier la configuration**. Le système vous invite à confirmer que vous souhaitez modifier les onglets *Algorithmes*, *Certificat*, *Régions*, *Répertoires*, *Clés*, *Logiciel antivirus*, *Résolution des règles*, *Serveur*, Configuration et Autres paramètres. Seuls les responsables principaux de la sécurité peuvent autoriser les changements dans les onglets *Algorithmes*, *Certificats*, *Clés*, *Résolution des règles*, Régions et Autres paramètres !
Créer un responsable de la sécurité	Requiert le droit global **Créer un responsable de la sécurité**
Modifier listes d'accès	Requiert le droit global **Modifier les droits globaux** et les droits spécifiques au groupe ou responsable de la sécurité correspondant.
Modifier les autorisations	Requiert le droit global **Modifier les ACL.**
Assigner le certificat	Requiert le droit global **Assigner le certificat** et les droits spécifiques au groupe correspondant.

Opération	Autorisations nécessaires
Utiliser les clés spécifiques à un utilisateur ou un groupe	Requiert le droit global Utiliser clés spécifiques. La spécification de l'autorisation supplémentaire pour l'utilisation de clés spécifiques n'affecte pas l'utilisation des paramètres fictifs <userkey> ou <groupkey>. Cela ne fait que restreindre la gestion (affichage/utilisation/ modification) d'une clé spécifique.
Administrer des groupes	Requiert le droit global **Modifier les groupes** et les droits spécifiques au groupe correspondant.
Administrer des utilisateurs	Requiert le droit global **Modifier les utilisateurs** et les droits spécifiques au groupe correspondant.
Gérer la journalisation	Requiert le droit global **Lire journal** et **Gérer la journalisation**
Créer des règles	Cette opération nécessite le droit global **Générer une règle** ainsi que les droits propres au groupe correspondant.
Créer ou déplacer des clés	Cette opération nécessite le droit global **Créer une clé** ainsi que les droits propres au groupe correspondant.
Créer des profils	Cette opération nécessite le droit global **Générer le profils** ainsi que les droits propres au groupe correspondant.
Afficher la valeur de la clé	Requiert le droit global Lire la clé. Une autorisation supplémentaire est requise lors de la sélection de l'option Afficher la valeur de la clé dans la boîte de dialogue des propriétés de clé.

Si l'une de ces opérations requiert une autorisation supplémentaire, vous devez préciser combien de responsables de la sécurité sont nécessaires pour effectuer cette opération.

Pour ce faire, sélectionnez l'opération. Cliquez deux fois sur l'opération sélectionnée. Une boîte de dialogue s'ouvre et vous pouvez y spécifier le nombre de responsable de la sécurité nécessaire. Lorsque vous cliquez sur **OK**, conpal LAN Crypt met à jour les données dans l'onglet Autorisation supplémentaire.

Un message s'affiche si le système reconnaît que le nombre requis de responsables de la sécurité n'est pas disponible.

Remarque : le système est incapable de trouver précisément le nombre de responsables de la sécurité actuellement disponibles. Le nombre que vous demandez peut ne pas être disponible même si le message ne s'affiche pas. Par exemple, les droits d'un responsable de la sécurité peuvent avoir été modifiés ultérieurement ou un responsable de la sécurité a peut-être été supprimé.

Remarque : s'il est porté à votre connaissance que les responsables de la sécurité nécessaires ne sont pas disponibles et que vous avez mentionné qu'au moins un responsable de la sécurité

supplémentaire est requis au moment où vous avez défini le nombre de responsables de la sécurité nécessaires (confirmation de ce paramètre après avoir cliqué sur **OK** et fermé la boîte de dialogue), ce paramètre sera néanmoins validé pour raison technique.
Cela conduit à une situation où les actions exigeant une autorisation supplémentaire ne sont plus menées à bien du fait que les responsables de la sécurité nécessaires ne sont pas disponibles. Si ce paramètre est spécifié pour l'option **Modifier les paramètres d'autorisation supplémentaire**, les paramètres de cette boîte de dialogue ne peuvent plus être modifiés.
Le paramètre peut seulement être modifié par la génération d'une clé de récupération (voir *Annulation de l'autorisation supplémentaire*)

Une situation similaire peut se produire au moment de supprimer des responsables de la sécurité. En effet, le système ne vérifie pas si le nombre requis de responsables de la sécurité pour l'autorisation supplémentaire est toujours correct après la suppression d'un responsable. conpal LAN Crypt s'assure uniquement qu'un responsable principal de la sécurité existe dans le système.

Remarque : si vous n'utilisez pas de jetons pour une autorisation supplémentaire, nous vous conseillons de paramétrer Protection forte de la clé privée sur Oui.

Octroi de l'autorisation supplémentaire

Si une autorisation supplémentaire a été demandée pour une opération, l'assistant d'autorisation supplémentaire est lancé dès que cette opération est sélectionnée. L'assistant demande l'autorisation d'au moins un responsable principal de la sécurité supplémentaire. Vous pouvez sélectionner le responsable principal de la sécurité adéquat dans la boîte de dialogue.
Si conpal LAN Crypt utilise le certificat de ce responsable de la sécurité pour parvenir à l'authentifier, l'opération demandée peut être effectuée.
Si plusieurs responsables de la sécurité possèdent le même certificat, ce dernier ne peut être utilisé qu'une seule fois dans une procédure d'autorisation. Tous les autres responsables de la sécurité possédant ce certificat seront supprimés de la liste.

Remarque : la boîte de dialogue dans laquelle vous sélectionnez un responsable de la sécurité comporte une option vous permettant de restreindre l'affichage aux responsables de la sécurité d'une région précise. Les responsables de la sécurité qui ne sont assignés à aucune région en particulier sont toujours affichés dans la liste.

Annulation de l'autorisation supplémentaire

Une autorisation supplémentaire pour une action est généralement valide pour la durée entière de la session conpal LAN Crypt Administration. Cliquez sur le bouton **Annuler autorisation** dans la barre d'outils de conpal LAN Crypt Administration pour supprimer l'information concernée de sorte qu'une autorisation supplémentaire soit nécessaire à la prochaine réalisation de l'opération au cours de la session.

Suppression d'une autorisation supplémentaire

Si la configuration aboutit à la présence d'un nombre insuffisant de responsables de la sécurité pour accorder l'autorisation supplémentaire nécessaire à une opération, vous pouvez utiliser la clé de récupération pour remettre à zéro le nombre de responsables de la sécurité nécessaires pour modifier les paramètres d'autorisation supplémentaire.

Pour ce faire, cliquez sur **Assigner le certificat** dans la fenêtre de connexion. Un assistant est lancé afin de remettre à zéro le nombre de responsables de la sécurité supplémentaires requis. Voir ci-dessous pour de plus amples informations. Pour plus de détails, voir ci-dessous.

3.5.10 Onglet Clés de récupération

conpal LAN Crypt vous permet de créer une clé de récupération. Cette clé vous permet d'assigner un nouveau certificat à un responsable de la sécurité lorsqu'il se connecte à la base de données conpal LAN Crypt (cliquez sur le bouton Assigner certificats), si le certificat est détérioré ou inutilisable. À l'aide de la clé de récupération, vous pouvez aussi remettre à zéro le nombre de responsables de la sécurité supplémentaires nécessaires pour changer les paramètres de l'autorisation supplémentaire sur 0.

Vous pouvez diviser une clé de récupération en plusieurs parties et préciser combien de parties sont nécessaires à l'assignation d'un nouveau certificat. Les différentes parties de la clé de récupération peuvent être réparties entre différents responsables de la sécurité. Les détenteurs des différentes parties doivent être présents pendant l'utilisation de la clé et faire appel à un assistant pour présenter les parties de la clé. Vous pouvez entrer manuellement (les parties de) la clé de récupération ou la charger à partir d'un fichier.

Pour générer une clé de récupération, cliquez sur le bouton **Générer une clé de récupération** de l'onglet *Clés de récupération*. Vous lancez ainsi l'assistant pour la clé de récupération.

Utilisez les listes déroulantes pour sélectionner le nombre de parties que la clé contiendra et le nombre de parties nécessaires pour la clé de récupération. Dans notre exemple, la clé aura trois parties, dont deux sont nécessaires pour assigner un nouveau certificat de responsable de la sécurité à la connexion. Cliquez sur **Suivant**.

Pour chaque partie de la clé, l'assistant affiche une boîte de dialogue dans laquelle vous précisez si la clé partielle doit être enregistrée dans un fichier ou affichée à l'écran afin que vous puissiez la noter. L'assistant se ferme automatiquement à la fin du traitement de toutes les parties.

Dans l'onglet Clé de récupération, à côté de la clé par défaut, vous pouvez voir le nombre de parties que contient la clé (dans notre exemple 3) et le nombre de parties nécessaires pendant l'utilisation (dans notre exemple 2).

Remarque : pendant que vous créez et répartissez les parties de la clé de récupération, n'oubliez pas qu'elles contiennent des données extrêmement sensibles. Il est essentiel que vous protégiez la clé de récupération contre les accès non autorisés.

Remarque : vous utiliserez toujours la clé de récupération la plus récente.
En effet, les clés de récupération précédentes ne sont plus valides et ne peuvent plus être utilisées pour assigner un certificat.

Utilisation de la clé de récupération.

Si vous ne pouvez plus accéder à la base de données (en raison de l'expiration d'un certificat), cliquez sur **Assigner le certificat** dans la fenêtre de connexion pour lancer *Assistant de récupération de clés*.

Si une boîte de dialogue vous informe qu'il est impossible d'utiliser le certificat, vous pourrez lancer l'assistant après avoir sélectionné un responsable de la sécurité.

Suivez les instructions affichées à l'écran.

L'assistant affiche une boîte de dialogue dans laquelle vous pouvez remettre à zéro le nombre de responsables de la sécurité nécessaires à la modification des paramètres pour une autorisation supplémentaire.

Vous écartez ainsi l'éventualité d'une situation où une autorisation supplémentaire deviendrait impossible en raison de l'absence de responsables de la sécurité capables de l'accorder.

Si vous activez cette option, un seul responsable de la sécurité peut modifier ultérieurement les paramètres d'autorisation supplémentaire.

3.5.11 Onglet Base de données

Remarque : ce paramètre est requis uniquement si vous utilisez une base de données Oracle à laquelle vous accédez par les consoles Administration des différents postes. Seul un responsable principal de la sécurité peut effectuer ce paramétrage.

Le support NLS (National Language Support) d'Oracle convertit le texte pour l'utilisateur afin qu'il soit toujours affiché de la même manière, quel que soit le jeu de caractères utilisé, et même si le codage numérique des caractères est différent en raison de jeux de caractères différents (par exemple : WE8MSWIN1252: ü=FC00, AL16UTF16: ü=7C00).

Si le texte est ajouté à la base de données et extrait à l'aide d'un jeu de caractères différent, cela pourrait donner lieu à un calcul erroné de la somme de contrôle (MAC) car si les caractères étaient par exemple convertis en binaire, ces données binaires poseraient des problèmes pour MAC.

Pour éviter ces erreurs, vérifiez que le même code de page/jeu de caractères est utilisé sur tous les postes pouvant accéder à la base de données via le client Oracle.

Dans l'onglet *Base de données*, vous pouvez désigner le jeu de caractères qui sera utilisé par tous les postes accédant à la base de données. Lorsque vous lancez la console conpal LAN Crypt

Administration, vérifiez que la configuration du client Oracle correspond à celle de la base de données. Si ce n'est pas le cas, un message d'avertissement s'affichera et la console Administration ne pourra pas être lancée.

Dans le champ d'édition, entrez le jeu de caractères à utiliser pour que les clients Oracle puissent se connecter à la base de données. Pour un client Oracle, ce paramètre est accessible dans la base de registre sous la valeur `NLS_Lang` (`Language.Territory.CharacterSet`, exemple : `FRENCH_FRANCE.`**`WE8MSWIN1252`**).

Le jeu de caractères du poste en cours est affiché sous *INFO* : dans l'onglet *Base de données*. Tous les autres clients pouvant accéder à la base de données doivent normalement utiliser ce jeu de caractères.

Remarque : nous vous recommandons d'utiliser un seul jeu de caractères ! Si vous faites appel à plusieurs jeux de caractères, des erreurs peuvent se produire pendant le calcul de la somme de contrôle (MAC).
En règle générale, il est toutefois possible d'utiliser plusieurs jeux de caractères. Néanmoins, vous devriez utiliser plusieurs jeux de caractères uniquement si les jeux concernés sont en grande partie identiques avec très peu de caractères différents. Vous devriez identifier ces caractères et ne pas les utiliser pour des entrées dans la base de données.

Désactivation de la vérification

conpal LAN Crypt vous permet de désactiver la vérification du jeu de caractères. Si vous ne renseignez pas le champ d'édition, aucune vérification ne sera effectuée et vous pourrez toujours vous connecter à la console Administration. Nous vous rappelons que cela peut être source d'erreurs au moment du calcul de la somme de contrôle (MAC).

Pour prévenir l'apparition d'erreurs consécutives à la désignation d'un jeu de caractères (erreurs de frappe par exemple) qui peut aller jusqu'à une situation où le responsable principal de la sécurité, responsable de la configuration, ne peut plus se connecter à la console Administration, conpal LAN Crypt contrôle les données saisies validées en appuyant sur **Appliquer** ou sur **OK**. Si le jeu de caractères désigné ne correspond pas à celui utilisé par le poste, un message s'affiche et le jeu de caractères valide est ajouté au champ d'édition. L'onglet *Base de données* reste à l'écran pour contrôler que les données ont été saisies. Si nécessaire, modifiez les paramètres et appuyez de nouveau sur **Appliquer** ou **OK**.

3.5.12 Onglet Antivirus

Pour que les utilitaires antivirus puissent analyser les fichiers chiffrés avec conpal LAN Crypt, vous devez les mentionner ici. L'antivirus concerné se verra alors accorder l'accès à toutes les clés conpal LAN Crypt et pourra reconnaître les signatures de virus dans les fichiers chiffrés. Cela est impossible sans les clés conpal LAN Crypt.

Pour ajouter un utilitaire antivirus, cliquez sur **Ajouter**. Entrez les données suivantes dans la boîte de dialogue qui apparaît :

- le nom de l'antivirus (ce nom s'affiche dans l'onglet *Logiciel antivirus* sous *Produit*) ;
- le nom de l'exécutable du logiciel effectuant l'analyse.

Activez l'option **Utiliser la vérification du code d'authentification**.

Remarque : nous vous recommandons vivement l'utilisation d'un utilitaire antivirus à code d'authentification de sorte à définir ici l'utilitaire et à activer la vérification du code d'authentification. Seule cette vérification assure que l'exécutable est celui qu'il faut et que seules des applications de confiance accèdent aux clés conpal LAN Crypt.

Cliquez sur **OK** pour que l'antivirus apparaisse dans la liste. Vous pouvez ensuite ajouter d'autres utilitaires antivirus.

3.5.13 Onglet Client API

conpal LAN Crypt fournit un Client API permettant aux applications de contrôler la fonctionnalité de chiffrement des fichiers à l'aide d'une simple ligne de commande ou d'une API de style COM. Retrouvez plus de renseignements dans la documentation Client API dans le dossier \DOC de votre package d'installation décompressé.

Remarque : l'API doit être sélectionnée au cours de l'installation de conpal LAN Crypt Client. Si vous souhaitez utiliser le Client API sur vos clients, assurez-vous qu'il est installé correctement.

Sur l'onglet *Client API*, indiquez les paramètres du Client API.

- Sélectionnez **Activer le client API** pour mettre l'API à disposition sur le client. Les applications peuvent désormais contrôler la fonctionnalité du fichier via l'API de style COM.
- Sélectionnez **Activer l'accès API pour l'outil de ligne de commande de chiffrement des fichiers conpal** pour permettre le contrôle de la fonctionnalité de chiffrement de fichiers à l'aide d'un simple outil de ligne de commandes.
- **API de style COM uniquement** : par défaut, les règles de chiffrement définies dans conpal LAN Crypt Administration ont la priorité sur les tâches de chiffrement effectuées via le Client API. Si vous voulez que les "règles API" soient prioritaires, veuillez sélectionner l'option **Les règles API ont priorité sur les règles de chiffrement dans les profils**.
  Remarque : dans conpal LAN Crypt, les **Règles Ignorer** et les **Règles d'exclusion** ont la priorité la plus élevée et ne peuvent pas être remplacées par les règles API. Les mêmes fichiers/répertoires sont automatiquement exclus du chiffrement (see *Files/directories excluded from encryption* on page 7).

L'accès API étant restreint aux applications autorisées, vous devez indiquer les applications autorisées à l'utiliser. Pour cela :

1. cliquez sur Ajouter sur l'onglet Client API.
2. Saisissez le nom de l'application.
3. Indiquez l'exécutable qui va accéder à l'API.
4. Si vous voulez utiliser des fichiers exécutables signés Authenticode pour accéder à l'API, sélectionnez l'option Le fichier exécutable doit être signé Authenticode.
5. Si vous voulez également utiliser des fichiers exécutables signés par des fournisseurs de confiance, sélectionnez l'option **Le fichier exécutable doit être signé Authenticode par un fournisseur de confiance**. Vous serez ainsi assuré que les fichiers exécutables acceptés sont uniquement ceux qui sont signés à l'aide du certificat enregistré en tant que *Certificat de signature* d'un fournisseur sur l'onglet *Fournisseurs de confiance*.
   Remarque : les fournisseurs de confiance doivent être enregistrés sur l'onglet *Fournisseurs de confiance* dans les *Préférences conpal LAN Crypt*.
6. Ajoutez éventuellement un commentaire.

Après avoir cliqué sur **OK**, l'application apparaît dans la liste. Vous pouvez ensuite ajouter d'autres applications.

3.5.14 Onglet Fournisseurs de confiance

Sur l'onglet Fournisseurs de confiance, vous pouvez enregistrer les fournisseurs autorisés à signer un fichier exécutable avec Authenticode pour accéder au Client API.

Pour ajouter un fournisseur de confiance :

1. cliquez sur Ajouter sur l'onglet Fournisseurs de confiance.
2. Saisissez le nom du fournisseur.
3. Saisissez le certificat de signature du fournisseur.
   Si elle est sélectionnée sur l'onglet Client API, l'API acceptera uniquement les fichiers exécutables signés Authenticode à l'aide de ce certificat.
4. Ajoutez éventuellement un commentaire.

Après avoir cliqué sur **OK**, le fournisseur apparaît dans la liste. Vous pouvez ensuite ajouter d'autres fournisseurs.

3.5.15 Onglet Autres paramètres

Options du responsable de la sécurité

conpal LAN Crypt peut être configuré pour automatiquement créer une ACL avec le droit de consultation pour le groupe racine d'un responsable de la sécurité nouvellement créé. Le responsable de la sécurité doit avoir l'autorisation globale Administrer les groupes ou Administrer les utilisateurs.Il peut ainsi accéder (consulter et/ou modifier) tous les groupes dont il est responsable.

Si vous sélectionnez l'option Définir les autorisations du groupe pour les responsables de la sécurité autorisés à administrer les groupes ou les utilisateurs, les ACL du groupe racine sont créés automatiquement.

Options du fournisseur de services cryptographiques

Si l'option **Utiliser l'enveloppement de clé (paramètres par défaut)** est sélectionnée, les données du responsable de la sécurité et les données du profil de l'utilisateur seront chiffrées à l'aide d'une clé de session aléatoire avec l'algorithme sélectionné (3DES par défaut). Cette clé de session est ensuite chiffrée au format RSA avec la clé publique issue du certificat.

Si vous utilisez des cartes à puce, assurez-vous que celles que vous souhaitez utiliser reconnaissent l'algorithme que vous avez sélectionné.

Si vous dessélectionnez cette option, les données seront chiffrées au format RSA sans clé de session. Notez que cette option n'est peut-être pas prise en charge par les cartes à puce.

3.6 Affichage de toutes les clés conpal LAN Crypt

La sélection du nœud *Toutes les clés conpal LAN Crypt* permet d'afficher un aperçu de toutes les clés gérées par conpal LAN Crypt. Vous pouvez afficher ici les informations suivantes :

- le nom de clé long ;
- l'algorithme correspondant à la clé ;
- une indication si la clé est active ;
- la personne qui a créé la clé (générateur) ;
- une indication si la clé doit être héritée ;
- une indication du groupe pour lequel la clé a été générée ;
- une indication si la clé est en cours d'utilisation ;
- le champ de commentaires.

Cliquez sur un titre de colonne pour trier le contenu de la table en ordre croissant ou décroissant, pour mettre en avant les informations voulues.

3.6.1 Recherche de clés

Vous pouvez non seulement trier les informations relatives aux clés, mais encore rechercher une clé donnée. Pour ce faire, cliquez avec le bouton droit de la souris sur l'onglet **Toutes les clés conpal LAN Crypt**, puis sélectionnez **Rechercher** une **clé** dans le menu contextuel.

Remarque : la fonction **Rechercher une clé** est également disponible dans l'onglet de clé de groupe de chacun des groupes.
Pour ajouter une clé dans un groupe, vous avez aussi besoin du droit *Copier la clé* pour le groupe dans lequel se trouve la clé ainsi que du droit *Créer la clé* pour le groupe dans lequel la clé doit être ajoutée.

Cette opération active un assistant qui permet de rechercher la clé voulue. Au cours de l'étape 1, vous pouvez indiquer si vous souhaitez rechercher la clé en fonction de son GUID ou de son nom.

Exemple :

{[56]% renvoie toutes les clés dont le GUID commence par 5 ou 6.

Cliquez ensuite sur **Suivant** pour rechercher les clés voulues dans la base de données. Si la clé est trouvée, l'étape 2 affiche le nom de la clé, son GUID et le groupe ayant servi à la générer.

Si vous avez appelé la fonction **Rechercher une clé** à partir d'un nœud de clé de groupe, activez l'option **Affecter la clé au groupe actuel** pour créer un lien vers la clé trouvée. Vous pouvez ensuite utiliser une clé dans le groupe qui est actuellement sélectionné, même si elle a été générée dans un autre groupe. Si vous activez cette option, cliquez sur **Suivante**, puis cliquez sur **Fermer** lors de l'étape 3, pour afficher une icône de clé spéciale dans le nœud de clé de groupe correspondant au groupe actuel. Vous pouvez désormais utiliser cette clé dans les règles de chiffrement.

Remarque : si vous sélectionnez l'option **Affecter la clé au groupe actuel**, cette dernière n'a d'effet que si vous avez appelé la fonction **Rechercher une clé** à partir de l'onglet **Clé de groupe** d'un groupe, et non pas à partir de l'onglet **Toutes les clés conpal LAN Crypt**.
Des clés spécifiques peuvent également être sélectionnées. Toutefois, elles ne seront pas affectées au groupe actuel. Si votre sélection contient une clé spécifique, le message correspondant sera affiché sur la dernière page de l'assistant.

3.7 Affichage des utilisateurs et certificats sélectionnés

Le nœud *Utilisateurs et certificats sélectionnés* n'est disponible que si l'option *Afficher les "Utilisateurs et certificats sélectionnés"* est active dans la section des paramètres utilisateur de *conpal LAN Crypt Administration* (see *Paramètres d'utilisateurs* on page 38).

Si vous cliquez sur *Afficher "Tous les utilisateurs et certificats"*, un avertissement indique que ce processus peut prendre plusieurs minutes. Cet avertissement s'applique particulièrement aux grandes sociétés, où le nombre d'utilisateurs et de certificats peut être très élevé.

Remarque : si le système est défini pour mettre en mémoire cache les listes d'utilisateurs, vous devez actualiser l'affichage via l'icône de la barre d'outils ou en appuyant sur F5 pour pouvoir saisir de nouveaux critères de recherche.

Sélectionnez l'option *Afficher les utilisateurs correspondants* pour activer les champs de saisie en vue de définir vos critères de recherche :

Les informations suivantes sur l'utilisateur sont récupérées dans la base de données de conpal LAN Crypt :

- le nom de connexion.
- le nom d'utilisateur ;
- l'assignation entre l'utilisateur et le certificat ;
- le demandeur du certificat ;
- le numéro de série du certificat ;
- la date de début de validité du certificat ;
- la date de fin de validité du certificat ;
- le nom du groupe parent.

Vous pouvez définir des critères de recherche d'après ces attributs. conpal LAN Crypt recherche les chaînes de caractères définies dans les attributs de l'utilisateur récupérés.

Dans la première liste déroulante, vous pouvez sélectionner le ou les attributs sur lesquels doit porter le processus de recherche.

En outre, vous pouvez définir si l'attribut sélectionné doit correspondre à la chaîne de caractères saisie (*faut être*) ou si seuls doivent être affichés les utilisateurs pour lesquels l'attribut sélectionné ne correspond pas à la chaîne de caractères saisie (*ne faut pas être*).

Dans la liste déroulante située sur la droite, saisissez la chaîne de caractères que conpal LAN Crypt recherche dans l'attribut défini.

Utilisez les caractères génériques SQL suivants pour saisir la chaîne de caractères :

%	n'importe quelle séquence de caractères

_	caractère unique (par exemple, a__ recherchera tous les noms contenant trois caractères et commençant par a)
[]	caractère unique d'une liste (par exemple, [a-cg]% recherchera tous les noms commençant par a, b, c ou g)
[^]	caractère unique non inclus dans une liste (par exemple, [^a]% recherchera tous les noms ne commençant pas par a)

Vous pouvez indiquer jusqu'à trois conditions dans le processus de recherche.

Si vous entrez plusieurs conditions, définissez la façon dont ces conditions sont à associer (AND/OR).

Cliquez avec le bouton droit de la souris sur *Afficher les "Utilisateurs et certificats sélectionnés"* pour exploiter toutes les fonctions du composant logiciel enfichable de certificat disponibles pour chaque groupe (see *Assignation de certificats* on page 118).

À ce stade, l'assistant d'assignation de certificats est uniquement disponible pour les responsables principaux de la sécurité. Si un responsable de la sécurité dispose d'autorisations adéquates, il peut utiliser le menu *Propriétés* pour assigner un certificat à un utilisateur donné.

Cependant, si le responsable de la sécurité ne dispose pas d'autorisations pour cet utilisateur, l'icône correspondante s'affiche.

3.8 Création d'un responsable de la sécurité

Les responsables principaux de la sécurité et les responsables de la sécurité autorisés peuvent créer des responsables de la sécurité supplémentaires. Ces responsables de la sécurité peuvent ensuite être assignés à des OU séparées. Ils reçoivent initialement des droits globaux qui définissent précisément leurs tâches. Dès que les responsables de la sécurité ont été assignés à une OU (un objet dans conpal LAN Crypt Administration), les ACL peuvent servir à restreindre leurs droits en fonction de cet objet particulier.

Remarque : si les droits globaux d'un responsable de la sécurité ne lui permettent pas d'effectuer une action précise, il sera impossible d'avoir recours à une ACL pour lui accorder le droit correspondant à cette action.

1. Pour créer un nouveau responsable de la sécurité (SO), sélectionnez l'onglet *Paramètres centraux/Administration des responsables de la sécurité*. Pour ouvrir la boîte de dialogue initiale de création d'un responsable de la sécurité , cliquez sur **Ajouter nouveau RS...** dans le menu contextuel de ce nœud ou cliquez sur **Ajout nouveau RS...** dans le menu Action.

2. Dans cette boîte de dialogue, entrez un **Nom** et si nécessaire une adresse de messagerie et un commentaire. Puis cliquez sur **Suivant**.

Remarque : l'adresse de messagerie est ajoutée au fichier journal des certificats générés par conpal LAN Crypt. Elle peut servir, par exemple, à créer à un courrier de codes PIN transmis par messagerie électronique.

3. Indiquez maintenant si le nouveau responsable de la sécurité détiendra ou non des droits de responsable principal de la sécurité. Un responsable principal de la sécurité détient tous les droits globaux existants. Cliquez sur le bouton **Parcourir...** pour sélectionner un certificat existant ou demander à conpal LAN Crypt d'en générer un pour vous.
   Assignation de certificats à l'aide d'une source LDAP
   conpal LAN Crypt permet d'affecter des certificats à partir de Microsoft Active Directory ou de toutes autres sources LDAP.
   Pour ce faire, sélectionnez **LDAP** dans la liste déroulante de la boîte de dialogue *Sélectionner un certificat*.

   Dans le champ d'édition affiché, vous pouvez entrer l'URL de la source LDAP. Après avoir cliqué sur **Actualiser**, le contenu de la source LDAP s'affiche.
   Les textes entre crochets (par exemple, Sub_OU_1]) correspond aux unités organisationnelles (OU) dans la source LDAP. Pour afficher les certificats d'une unité organisationnelle, cliquez deux fois dessus.
   Cliquez deux fois sur [..] pour remonter d'un niveau hiérarchique.
   Sélectionnez un certificat et cliquez sur **OK**. Le certificat est maintenant assigné au responsable de la sécurité.

Remarque : si le serveur LDAP n'autorise aucune connexion anonyme, vous devez entrer les données de connexion au serveur dans l'onglet **Serveur** des **Paramètres centraux**.

Remarque : si vous utilisez conpal LAN Crypt pour générer un certificat de chiffrement, le responsable de la sécurité doit importer la clé privée sur la station de travail à partir du fichier .p12 généré.
Si le certificat de chiffrement a été assigné à partir d'un annuaire LDAP, la clé privée correspondante doit être présente sur la station de travail du responsable de la sécurité. Le certificat de chiffrement est utilisé pour l'accès cryptographique à la clé de base de données symétrique.

4. D'autre part, vous pouvez cliquer sur le second bouton Parcourir pour sélectionner un certificat de signature existant ou demander à conpal LAN Crypt d'en générer un autre pour vous.

Remarque : si vous utilisez conpal LAN Crypt pour générer un certificat de signature, le responsable de la sécurité doit importer la clé privée sur la station de travail à partir du fichier .p12 généré.
Si la signature certificate a été assignée à partir d'un annuaire LDAP, la clé privée correspondante doit être présente sur la station de travail du responsable de la sécurité. Le certificat de signature

est utilisé pour la signature dans les profils généraux et pour l'authentification pendant la connexion API étendue.

5. Si vous avez défini des régions pour vos responsables de la sécurité, vous pouvez maintenant sélectionner une région.

6. Si vous avez créé des *dossiers de configuration* individuels pour ces régions, vous pouvez maintenant sélectionner un dossier.

Remarque : le système affiche uniquement les configurations générées pour la région sélectionnée.

7. Cliquez sur **Suivant**.

8. Dans la dernière boîte de dialogue de l'assistant, vous pouvez sélectionner les actions que pourra exécuter le responsable de la sécurité.
   Tous les droits globaux nécessaires aux actions sélectionnées seront définis automatiquement. Ces droits sont affichés dans les propriétés du responsable de la sécurité (cliquez deux fois sur un responsable de la sécurité pour les afficher) dans l'onglet *Autorisations globales*. Vous pouvez modifier les droits globaux sur cette page.
   Cette boîte de dialogue vous permet d'autoriser un responsable de la sécurité à effectuer une action précise en lui accordant automatiquement tous les droits nécessaires à cette action.

   Si un nouveau responsable de la sécurité obtient ainsi l'autorisation globale Administrer les groupes ou Administrer les utilisateurs , conpal LAN Crypt crée automatiquement une ACL avec les droits de consultation pour le groupe racine de ce responsable de la sécurité, à condition que l'option Définir les autorisations du groupe pour les responsables de la sécurité autorisés à administrer les groupes ou les utilisateurs soit activée. Le responsable de la sécurité peut ainsi accéder (consulter et/ou modifier) tous les groupes dont il est responsable.

Vous pouvez activer l'option Définir les autorisations du groupe pour les responsables de la sécurité autorisés à administrer les groupes ou les utilisateurs dans l'onglet *Autres paramètres* des **Paramètres centraux**.

9. Cliquez sur **Terminer**.

Le nouveau responsable de la sécurité s'affiche dans conpal LAN Crypt Administration.

3.8.1 Octroi/modification des autorisations globales

Le responsable de la sécurité doit détenir des droits globaux. Si vous sélectionnez le nœud Administration des responsables de la sécurité, tous les responsables de la sécurité existants s'afficheront dans le volet d'affichage à droite. Cliquez deux fois sur un responsable de la sécurité pour ouvrir les onglets contenant les propriétés qui lui sont dévolues.

L'onglet *Autorisations globales* sert à accorder au responsable de la sécurité les "droits de base" nécessaires à l'administration de conpal LAN Crypt. Au moment de la création de ces droits, si le responsable de la sécurité avait déjà obtenu le droit d'effectuer certaines actions, ces droits nécessaires seront déjà activés.

Remarque : un responsable principal de la sécurité détient toujours tous les autorisations globales existantes.

Les autorisations globales suivants peuvent être alloués à un responsable de la sécurité :

Remarque : Cliquez sur **Accepter** pour sélectionner simultanément toutes les autorisations globales. Cliquez à nouveau pour annuler la sélection de toutes les autorisations globales.

Autorisations	Description
Créer un responsable de la sécurité	Le responsable de la sécurité est autorisé à créer des responsables de la sécurité supplémentaires.
Créer des profils	Le responsable de la sécurité dispose de l'autorisation globale de lancer le programme de résolution de profils et de générer des fichiers de stratégie pour les utilisateurs individuels. Cette autorisation est nécessaire pour paramétrer l'autorisation Créer des profils d'un groupe donné pour un responsable de la sécurité. La création de profils permet au responsable de la sécurité de créer des profils pour les utilisateurs où le responsable de la sécurité dispose du droit Créer des profils pour le groupe parent de l'utilisateur. *(see Groupe parent d'un utilisateur on page 90).* Cette autorisation est une condition préalable requise pour l'assignation de valeurs aux clés. Un utilisateur qui a seulement l'autorisation Créer des clés peut uniquement générer des clés sans valeurs !

Autorisations	Description
Créer des profils pour tous les membres	Cette autorisation requiert que l'autorisation Créer des profils soit paramétrée. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Créer des profils pour tous les membres pour un groupe donné. Créer des profils pour tous les membres permet à un responsable de la sécurité de créer des profils pour tous les utilisateurs où ce responsable à l'autorisation Créer des profils sur le groupe parent ou l'autorisation Créer des profils pour tous les membres sur l'un des groupes auquel l'utilisateur est membre. Remarque : étant donné que l'autorisation globale Créer des profils est une condition préalable requise pour Créer des profils pour tous les membres, les conditions suivantes s'appliquent : Si vous désactivez l'autorisation Créer des profils, l'autorisation Créer des profils pour tous les membres est désactivée automatiquement. Si vous activez l'autorisation Créer des profils pour tous les membres, l'autorisation Créer des profils est automatiquement activée.
Créer des clés	Le responsable de la sécurité peut générer des clés dans les groupes individuels. Un utilisateur ayant l'autorisation *Créer des clés* peut uniquement générer des clés sans valeur ! Au sein de la console Administration, les clés sans valeur peuvent être assignées aux règles de chiffrement. La valeur elle-même est générée au moment de la création des fichiers de stratégie. Pour générer manuellement des clés avec valeurs, le responsable de la sécurité doit avoir l'autorisation *Créer des profils*.
Copier des clés	Le responsable de la sécurité a le droit de copier des clés.
Supprimer des clés	Le responsable de la sécurité peut supprimer des clés dans les groupes individuels.
Lire clé	Le responsable de la sécurité peut voir les données des différentes clés d'un groupe.
Créer des certificats	Le responsable de la sécurité peut générer des certificats pour les utilisateurs.

Autorisations	Description
Assigner des certificats	Le responsable de la sécurité a le droit d'assigner des certificats aux utilisateurs. Le responsable de la sécurité peut lancer l'assistant pour assigner les certificats. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Assigner des certificats d'un groupe donné pour un responsable de la sécurité. L'assignation de certificats permet au responsable de la sécurité d'assigner des certificats aux utilisateurs lorsque le responsable de la sécurité dispose du droit Assigner des certificats pour le groupe parent de l'utilisateur (see *Groupe parent d'un utilisateur* on page 90).
Assigner des certificats à tous les membres	Cette autorisation requiert que l'autorisation Assigner des certificats soit paramétrée. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Assigner des certificats à tous les membres d'un groupe donné. L'assignation de certificats à tous les membres permet à un responsable de la sécurité d'assigner des certificats à tous les utilisateurs où le responsable de la sécurité dispose du droit Assigner des certificats pour le groupe parent de l'utilisateur ou Assigner des certificats à tous les membres pour l'un des groupes auquel l'utilisateur est membre. Remarque : étant donné que l'autorisation globale d'Assigner des certificats est une condition préalable requise pour Assigner des certificats à tous les membres les conditions suivantes s'appliquent : Si vous désactivez l'autorisation Assigner des certificats, l'autorisation Assigner des certificats à tous les membres est automatiquement désactivée. Si vous activez l'autorisation Assigner des certificats pour tous les membres, l'autorisation Assigner des certificats est automatiquement activée.
Administrer des groupes	Le responsable de la sécurité peut effectuer des modifications dans les groupes. Ajout de sous-groupes, déplacement, synchronisation ou suppression de groupes.

Autorisations	Description
Connexion à la base de données	Le responsable de la sécurité peut se connecter à la base de données conpal LAN Crypt. Le paramètre par défaut est activé pour cette autorisation. Cette autorisation permet à un responsable de la sécurité de modifier facilement la base de données (par exemple, en cas de départ d'un membre du personnel dans une entreprise). Ce droit n'est pas accordé aux personnes qui sont habilitées à agir uniquement si une autre personne les y autorise. Cela garantit que ces personnes pourront uniquement autoriser des actions nécessitant une confirmation et n'auront aucun moyen de procéder à des modifications dans conpal LAN Crypt.
Autoriser les opérations	Le responsable de la sécurité peut participer à des actions nécessitant une confirmation.
Administrer des utilisateurs	Le responsable de la sécurité peut ajouter ou retirer un utilisateur au sein d'un groupe et synchroniser les groupes.
Copier des utilisateurs	Le responsable de la sécurité est autorisé à ajouter (copier) des utilisateurs dans les groupes. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Copier des utilisateurs d'un groupe donné pour un responsable de la sécurité. Pour ajouter un utilisateur à un groupe, le responsable de la sécurité doit avoir l'autorisation Copier des utilisateurs sur le groupe parent de l'utilisateur.
Créer des règles	Le responsable de la sécurité est autorisé à générer des règles de chiffrement pour les utilisateurs.
Modifier les autorisations globales	Le responsable de la sécurité peut modifier les droits globaux octroyés à un autre responsable de la sécurité.
Modifier les ACL	Le responsable de la sécurité peut modifier l'ACL d'un groupe.
Utiliser clés spécifiques	Le responsable de la sécurité peut utiliser des clés spécifiques dans les règles de chiffrement et peut afficher des clés spécifiques dans *Toutes les clés conpal® LAN Crypt.*
Modifier la configuration	Le responsable de la sécurité peut modifier la configuration (chemins). Cette autorisation est nécessaire pour afficher l'onglet Configurations dans les Paramètres centraux et pour que le responsable de la sécurité puisse effectuer des changements dans l'onglet Répertoires s'il est connecté à la base de données.
Lire les entrées du journal	Le responsable de la sécurité peut consulter les paramètres de journalisation ainsi que les événements.

Autorisations	Description
Gérer la journalisation	Le responsable de la sécurité peut modifier les paramètres de journalisation. Il peut archiver, supprimer et vérifier les entrées.
Importer des objets répertoire	Le responsable de la sécurité peut importer des OU, des groupes et des utilisateurs à partir d'un service d'annuaire et les ajouter à la base de données conpal LAN Crypt. Avant de pouvoir importer des objets de l'annuaire, le responsable de la sécurité a aussi besoin des autorisations *Administrer les groupes* et *Administrer les utilisateurs*. Elles sont activées automatiquement lorsque l'autorisation *Importation des objets du répertoire* est sélectionnée. Si un responsable de la sécurité ne possède pas cette autorisation, le nœud *Objets du répertoire*, qui sert à importer les OU, groupes et utilisateurs, n'est pas visible dans la console Administration.

Veuillez noter les points suivants relatifs à l'octroi d'autorisations globales :

- Un responsable de la sécurité ne détient pas d'autorisation globale tant qu'il ne lui a pas été accordé spécifiquement !
- Un responsable de la sécurité peut modifier uniquement les autorisations qu'il possède personnellement.
- Un responsable de la sécurité ne peut pas modifier une ACL décrivant ses propres autorisations.
- Certains droits sont accordés uniquement si vous possédez un autre droit. La sélection de ce type d'autorisation entraîne l'activation automatique de l'autre autorisation.
- conpal LAN Crypt peut être configuré pour automatiquement créer une ACL avec le droit de consultation pour le groupe racine d'un responsable de la sécurité nouvellement créé. Le responsable de la sécurité doit avoir l'autorisation globale Administrer les groupes ou Administrer les utilisateurs.Il peut ainsi accéder (consulter et/ou modifier) tous les groupes dont il est responsable.
  Ce comportement doit être activé sur l'onglet *Autres paramètres* dans les **Paramètres centraux**.
- Si un responsable de la sécurité est changé et reçoit l'autorisation globale Administrer les groupes ou Administrer les utilisateurs et ne possède pas d'ACL pour le groupe racine, il sera créé. L'ACL a le droit de consultation du groupe. Les ACL existantes ne sont pas changées.

Sélectionnez les autorisations globales que vous voulez accorder au responsable de la sécurité, puis cliquez sur **Appliquer**.

3.8.2 Autorisations de modification des paramètres d'un responsable de la sécurité

Il est possible de transférer les droits de modification des paramètres d'un responsable de la sécurité à d'autres responsables de la sécurité.
Un responsable principal de la sécurité peut à tout moment modifier ces paramètres. Le droit doit avoir été accordé spécifiquement à un responsable de la sécurité.

Les autorisations globales d'un responsable de la sécurité donné déterminent quels sont les autorisations qu'il peut modifier pour les autres responsables de la sécurité.

Vous pouvez définir quels droits sont associés à cet objet (c'est-à-dire le responsable de la sécurité) pour les autres responsables de la sécurité dans l'onglet Sécurité. Le bandeau supérieur de la boîte de dialogue affiche les responsables de la sécurité ayant le droit de modifier les paramètres associés à ce responsable de la sécurité.

1. Cliquez sur **Ajouter** pour lancer l'assistant d'ajout d'un responsable de la sécurité. Sur la première page de l'assistant, sélectionnez le responsable de la sécurité recherché dans la liste des responsables de la sécurité existants.

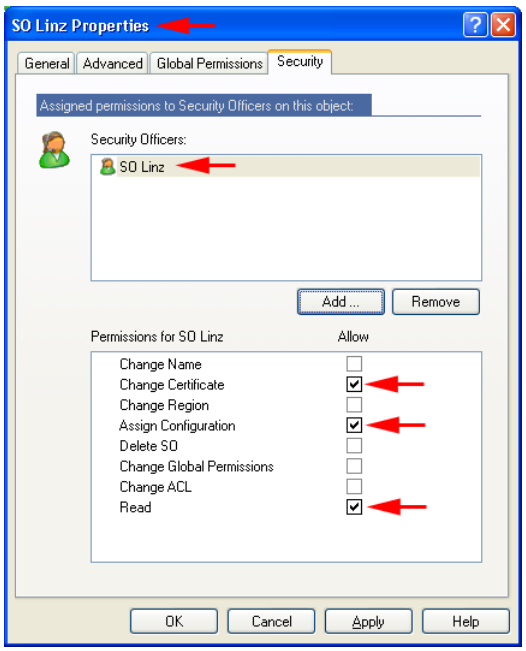
2. Cliquez sur **Suivant** pour afficher la page dans laquelle vous donnez au responsable de la sécurité en cours le droit de modifier cet objet (il s'agit du responsable de la sécurité dont les paramètres sont en cours de traitement).

Remarque : Cliquez sur **Autoriser** pour sélectionner simultanément toutes les autorisations. Cliquez à nouveau pour annuler la sélection de toutes les autorisations globales. La configuration des autorisations globales indique qu'il est impossible d'accorder les droits désactivés au responsable de la sécurité.

Autorisations	Description
Modifier le nom	Permet de modifier le nom du responsable de la sécurité auquel est assigné le détenteur de l'autorisation.
Modifier le certificat	Permet de modifier le certificat du responsable de la sécurité auquel est assigné le détenteur du droit.
Modifier la région	Permet de modifier le préfixe de la région du responsable de la sécurité auquel est assigné le détenteur du droit.
Assigner la configuration	Permet de modifier la configuration du responsable de la sécurité auquel est assigné le détenteur du droit.
Supprimer un responsable de la sécurité	Permet de supprimer le responsable de la sécurité auquel est assigné le détenteur de l'autorisation.
Modifier les autorisations globales	Permet de modifier les autorisations globales du responsable de la sécurité auquel est assigné le détenteur de l'autorisation.

Autorisations	Description
Modifier une ACL	Permet de modifier les autorisations globales de l'ACL à laquelle est assigné le détenteur du droit.
Lire	Affiche le responsable de la sécurité auquel est assigné le détenteur de l'autorisation dans *Paramètres centraux\Administration des responsables de la sécurité*. C'est la condition préalable à tous les droits permettant la gestion de ce responsable de la sécurité. L'activation est automatique si un droit de ce type est sélectionné.

Vous pouvez également accorder les autorisations **Modifier le certificat**, **Allouer la configuration** et **Lire** au responsable de la sécurité dont les propriétés sont définies ici. Avant de pouvoir effectuer ces opérations, ce responsable de la sécurité doit être présent dans la liste des responsables de la sécurité détenant des droits pour cet objet (dans ce cas, ce responsable de la sécurité).



Lire
Affiche le responsable de la sécurité désigné dans *Paramètres centraux\Administration des responsables de la sécurité*. Le responsable de la sécurité peut voir les autorisations qui lui ont été accordés.

Modifier le certificat
La condition préalable est la détention du droit "Lire". Autorise le responsable de la sécurité à modifier son propre certificat.

Assigner la configuration
Autorise le responsable de la sécurité à s'assigner une configuration différente.

Remarque : il est impossible d'accorder des autorisations dont la case à cocher est grisée car le responsable de la sécurité sélectionné ne détient pas les autorisations globales nécessaires pour le faire.

3. Accordez au responsable de la sécurité les droits appropriés en sélectionnant les cases à cocher et en cliquant sur **Terminer**.
   Le système affiche maintenant le responsable de la sécurité dans le volet supérieur de la page Sécurité. Un volet en bas de la page affiche l'ACL avec les droits du responsable de la sécurité sélectionné.

3.8.3 Tous les droits pour les groupes/OU d'un responsable de la sécurité donné

Pour consulter les droits d'un responsable de la sécurité donné pour tous les groupes/OU pour lesquels il dispose de l'intégralité des droits, choisissez Administration des responsables de la sécurité et cliquez deux fois sur le responsable de la sécurité correspondant.

Dans la boîte de dialogue des propriétés du responsable de la sécurité, sélectionnez l'onglet Groupes. Cet onglet contient deux vues de listes :

- La vue de liste supérieure vous montre tous les groupes/OU pour lesquels ce responsable de la sécurité a des droits.
- La seconde vue de liste montre les droits correspondants du responsable de la sécurité pour le groupe/OU sélectionné.

Vous pouvez ainsi facilement avoir un aperçu de tous les droits dont dispose un responsable de la sécurité donné pour tous les différents groupes dans votre structure organisationnelle.

Vous ne pouvez pas changer les droits d'un responsable de la sécurité dans cette vue. Le changement des droits est seulement possible dans la boîte de dialogue des propriétés d'un groupe.

Remarque : seuls les groupes pour lesquels un responsable de la sécurité a des droits (autorise ou refuse) s'affichent. Les groupes pour lesquels un responsable de la sécurité a hérité de droits ne s'affichent pas.

3.8.4 Modification ou renouvellement des certificats de responsables de la sécurité ou responsables principaux de la sécurité

Vous trouverez ci-dessous les différentes méthodes qui permettent de modifier ou renouveler un certificat de responsable de la sécurité ou de responsable principal de la sécurité :

Variante 1 : Via Administration des responsables de la sécurité

1. Lancez conpal LAN Crypt Administration et connectez-vous en tant que responsable principal de la sécurité. Vous pouvez également vous connecter en tant que responsable de la sécurité, à condition que ce rôle dispose de droits de modifications pour le responsable concerné. Ceci peut inclure les responsables de la sécurité lorsqu'ils disposent des droits requis et que leur certificat reste valide.

2. Activez la page *Paramètres centraux*, puis accédez au nœud *Administration des responsables de la sécurité*.

3. Cliquez avec le bouton droit de la souris sur le responsable de la sécurité concerné, puis sélectionnez l'entrée *Propriétés* dans le menu contextuel.

4. Allez dans l'onglet *Étendu*.

5. Dans la section *Certificat de chiffrement*, cliquez sur le bouton *Rechercher* pour sélectionner le nouveau certificat de chiffrement du responsable de la sécurité.

6. Vous pouvez également accéder à la section *Certificat de signature (facultatif)* et cliquer sur *Rechercher* pour sélectionner un nouveau certificat de signature pour le responsable de la sécurité.

Remarque : vous pouvez uniquement modifier les certificats de signature du responsable de la sécurité avec la variante 1 et non pas la variante 2.

Variante 2 : Utilisation de la clé de restauration

1. Lancez conpal LAN Crypt Administration.

2. Dans la boîte de dialogue du responsable de la sécurité, sélectionnez le responsable principal de la sécurité requis.

3. Cliquez sur le bouton *Modifier le certificat* et suivez les instructions qui s'affichent dans l'*assistant de récupération de clés*.

La variante 1 s'applique à la plupart des cas. La variante 2 a été conçue comme méthode de substitution et ne doit être utilisée que si aucun responsable de la sécurité disposant des droits nécessaires n'est en mesure de se connecter à conpal LAN Crypt Administration.

Remarque : il existe une condition requise à la variante 2 : l'existence d'une clé de restauration. Quelle que soit la méthode utilisée, vous devez vous assurer que le profil généré par le responsable de la sécurité est généré de nouveau, avant le terme de l'ancien certificat. Si tel n'est pas le cas, les clients ne pourront plus charger le profil.
Toutefois, vous pouvez autoriser l'affectation de certificats avec une autorisation supplémentaire

uniquement. Vous devez tenir compte du fait que ce type d'assignation aura un effet lorsque les certificats du responsable de la sécurité seront modifiés.

3.9 Connexion à conpal LAN Administration

Pour se connecter à la console conpal LAN Crypt Administration, un responsable de la sécurité doit détenir le droit correspondant. Les responsables principaux de la sécurité détiennent toujours ce droit puisqu'ils reçoivent automatiquement tous les droits disponibles.

Lorsque vous lancez la console Administration (Démarrer/Tous les programmes/Sophos/ conpal LAN Crypt/Administration), la boîte de dialogue de connexion suivante s'affiche à l'écran.

Tous les responsables de la sécurité autorisés sont affichés dans la liste. Si vous activez l'option **Afficher uniquement les responsables de la sécurité d'une région**, puis sélectionnez cette région, seuls les responsables de la sécurité de cette région seront affichés.

Pour activer la connexion, le système doit accéder à la clé privée associée au certificat (clé logicielle ou clé sur clé cryptographique).
Après avoir sélectionné le responsable de la sécurité requis, cliquez sur **OK** pour ouvrir conpal LAN Crypt Administration.

Clé de restauration

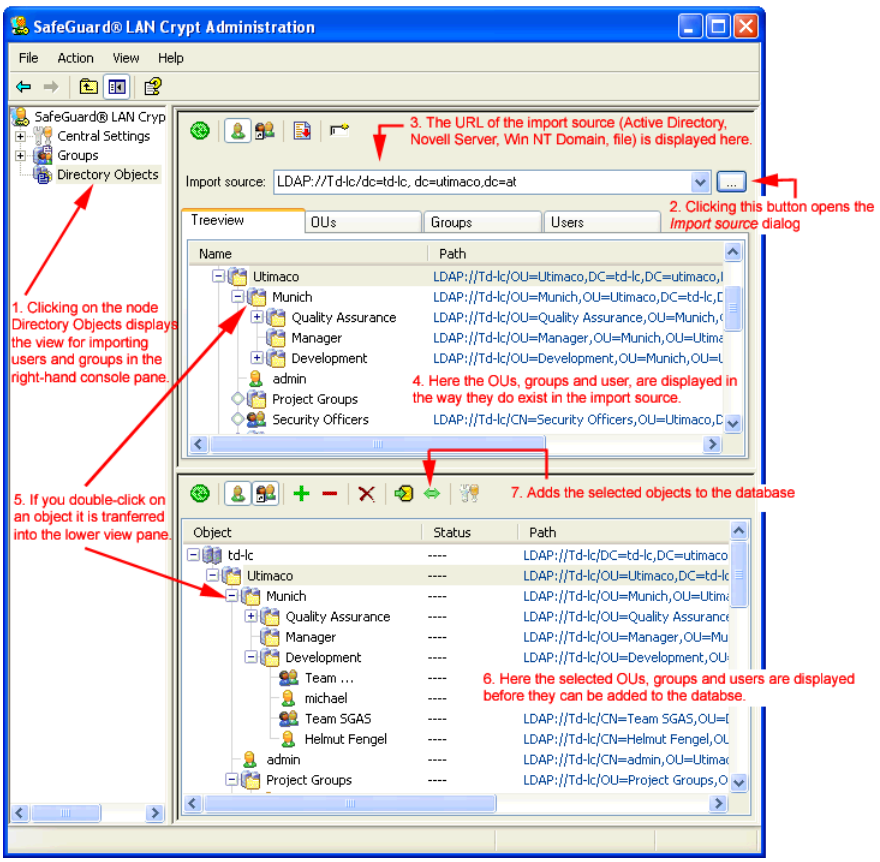
Si la clé associée au certificat du responsable de la sécurité a expiré ou a été détériorée ou égarée, entrez une clé de récupération pour renouveler le certificat.

Remarque : si un nouveau certificat est généré pendant la récupération, ce certificat et son mot de passe associé seront enregistrés sous le chemin par défaut (C:\Documents and Settings\All Users\Documents\Sophos\Admin\) et non pas le chemin configuré car à ce stade, aucune configuration propre au responsable de la sécurité n'est en place.

3.10 Importation de groupes et d'utilisateurs

conpal LAN Crypt vous permet d'importer des groupes et des utilisateurs à partir de services d'annuaire accessibles via LDAP, à partir de domaines, ou en les important à partir d'un fichier qui a été créé manuellement et qui contient les groupes et utilisateurs avec leurs dépendances spécifiques.

Cliquez sur *Objets de l'annuaire* pour afficher les fenêtres d'importation et d'assemblage des groupes à importer dans la base de données, dans le volet droit de la console.



Remarque : si un responsable de la sécurité connecté ne peut pas afficher le nœud Objets de l'annuaire, cela signifie qu'il ne possède pas l'autorisation globale "Importer objets du répertoire". Ce nœud apparaît uniquement dans la console Administration si le responsable de la sécurité est détenteur du droit mentionné.

3.10.1 Importer des groupes et utilisateurs à partir d'un fichier

Vous pouvez importer des utilisateurs et des groupes à partir d'un fichier que vous avez créé manuellement et qui contient les groupes et utilisateurs avec leurs dépendances spécifiques. Les groupes et utilisateurs importés sont créés dans le nœud *Groupes* de conpal LAN Crypt Administration.

Pour importer des utilisateurs et des groupes à partir d'un fichier, cliquez sur **Rechercher le fichier** dans la boîte de dialogue *Source d'importation*. Cliquez sur le bouton **Rechercher**. conpal LAN Crypt affiche une boîte de dialogue dans laquelle vous sélectionnez le fichier à partir duquel devront être importés les groupes et les utilisateurs (see *Sélection de la source d'importation* on page 82).

Le fichier d'importation est un fichier texte simple sans extension de fichier spéciale (nous vous suggérons d'utiliser .log comme extension par défaut). Le contenu du fichier doit répondre à certaines spécifications.

Format du fichier d'importation

Un fichier d'importation comprend plusieurs sections. Celles-ci sont séparées par un nombre arbitraire de lignes vides.

Chaque section représente un utilisateur ou un groupe.

Chaque section comporte un en-tête et un nombre fixe de lignes qui commencent chacune par un mot-clé. Les lignes doivent se terminer par un caractère de nouvelle ligne. Il est possible qu'il n'existe aucune autre nouvelle ligne entre les lignes d'une section.

L'en-tête est le nom de section entre crochets. Le nom de section sert à définir l'appartenance des utilisateurs et des groupes.

Les mots-clés définissent les données relatives aux utilisateurs et groupes tels qu'ils apparaissent dans la boîte de dialogue *Propriétés*.

Mots-clés	Description

type=
facultatif
	`USER`
	`GROUP`
	Définit si l'objet importé représente un utilisateur (USER) ou un groupe (GROUP).

name= facultatif	Définit le nom de connexion de l'utilisateur. Il est affiché sous *Nom de connexion* dans la console conpal LAN Crypt Administration.
display= facultatif	Vous permet de définir un nom d'utilisateur différent du nom de connexion. Il est affiché sous *Nom d'utilisateur* dans la console conpal LAN Crypt Administration. En l'absence de nom, le nom de connexion saisi sous `name=` est affiché sous *Nom d'utilisateur* dans la console conpal LAN Crypt Administration.
mail= facultatif	Vous permet de saisir l'adresse de messagerie de l'utilisateur. Elle est affichée dans l'onglet Détails des propriétés de l'utilisateur. **REMARQUE:** l'adresse de messagerie est ajoutée au fichier journal des mots de passe pour les certificats générés par conpal LAN Crypt. Elle peut servir, par exemple, à créer à un courrier de codes PIN transmis par messagerie électronique.

members=	Lorsque des groupes sont utilisés, ce mot-clé permet de définir quels utilisateurs et quels autres groupes appartiennent à un groupe précis. Pour ajouter un membre, saisissez le nom de section identifiant l'utilisateur ou le groupe (par exemple, `U_BKA,G_Sophos`). Utilisez des virgules pour séparer le nom des membres de chaque groupe.
Si vous saisissez `//` au début d'une ligne, vous pourrez entrer un commentaire sur cette ligne, à un endroit quelconque dans le fichier d'importation.	

Remarque : vous n'avez pas besoin de respecter scrupuleusement les majuscules et les minuscules lorsque vous effectuez une saisie dans le fichier d'importation.

Exemple :

```
[U_JB1]
type=USER
name=JB1
Display=Jesse Black
Mail=jb1@company.com
// mes commentaires .....

[U_PW1]
type=USER
name=PW1
Mail=jb1@company.com

[U_JG1]
type=USER
name=JG1

[U_JFU]
type=USER
name=JFU

[G_COMPANY]
type=GROUP
name=Company
members=G_QA,G_Scranton,G_PDM,G_Empty,U_JFU
// mes commentaires ..... .....

[G_QA]
type=GROUP
name=QA
members=U_JB1,U_PW1

[G_PDM]
type=GROUP
name=JG1
members=U_NGR
```

3.10.2 Icônes dans le système Administration

Met à jour l'affichage de la fenêtre activée.

Affiche les utilisateurs de groupes donnés.

Affiche également les membres de groupes et les utilisateurs dans des groupes donnés. Les membres dont l'objet n'est pas directement contenu dans le groupe sont grisés.

Déplace l'objet sélectionné dans le volet du bas. Équivaut à cliquer deux fois sur l'objet sélectionné.

Utiliser comme nouveau chemin.
Vous pouvez utiliser ce paramètre pour restreindre le mode d'affichage de l'arborescence. Si vous sélectionnez un nœud puis cliquez sur ce bouton, le système affiche uniquement l'arborescence en dessous du nœud sélectionné. En outre, le chemin est ajouté à la liste déroulante, ce qui vous permet de revenir rapidement à cet affichage.

Affiche l'arborescence.

Ferme l'arborescence.

Supprime un objet sélectionné de l'affichage.

Ajoute les objets, affichés dans le volet en bas à droite, à la base de données conpal LAN Crypt.

Synchronise les objets, affichés dans le volet en bas à droite, avec ceux déjà présents dans la base de données conpal LAN Crypt.

Ouvre la boîte de dialogue dans laquelle vous désignez les options de transfert.
Vous devez indiquer les options de transfert avant de transférer les objets à partir de la source d'importation.

3.10.3 Sélection de la source d'importation

Vous pouvez saisir l'URL du serveur à partir duquel seront importées directement les données dans le champ de saisie *Source d'importation* (par exemple, LDAP://usw-scranton/dc=usw-scranton,dc=company,dc=us pour le service d'annuaire Active Directory sur le contrôleur de domaine usw-scranton).

Cliquez sur le bouton **Rechercher** : conpal LAN Crypt affiche une boîte de dialogue dans laquelle vous importerez la source.

LDAP://

- **Domaine**

  Si l'ordinateur est membre d'un domaine Active Directory, cliquez sur ce bouton pour afficher la structure entière du domaine telle qu'elle est enregistrée sur le contrôleur de domaine.

Remarque : vous ne pouvez pas importer de groupes intégrés à partir de l'Active Directory. Nous recommandons par conséquent de répartir les utilisateurs dans des OU ou des groupes et de les importer.

- **Rechercher le conteneur :**

  Si l'ordinateur est membre d'un domaine Active Directory et si vous sélectionnez "Rechercher le conteneur :", le système affichera le bouton **Parcourir...** sur lequel vous pouvez cliquer pour afficher une autre boîte de dialogue. Vous pourrez y sélectionner un nœud particulier dans l'arborescence Active Directory.

WinNT://

- **Ordinateur**

  Affiche les groupes locaux et les utilisateurs de l'ordinateur auquel vous êtes actuellement connecté.
  Généralement, ces groupes et utilisateurs servent uniquement à réaliser des essais.

- **Domaine**

  Si l'ordinateur est membre d'un domaine Windows NT, cliquez sur ce bouton pour afficher la structure entière du domaine telle qu'elle est enregistrée sur le contrôleur de domaine.

  Remarque : si vous utilisez le protocole WinNT, le système ne fait pas la différence entre les utilisateurs renommés et les nouveaux utilisateurs durant la synchronisation. En effet, le protocole WinNT n'affecte pas de GUID uniques aux objets utilisateur.

FILE://

- **Rechercher le fichier**

  Pour importer des utilisateurs et des groupes à partir d'un fichier, cliquez sur **Rechercher le**

fichier dans la boîte de dialogue *Source d'importation*. Cliquez sur **Rechercher** pour sélectionner le fichier à partir duquel devront être importés les groupes et les utilisateurs. Le fichier d'importation doit avoir un format spécifique pour que vous puissiez importer les utilisateurs et les groupes. Pour plus d'informations sur la façon de créer le fichier importé, see *Importer des groupes et utilisateurs à partir d'un fichier* on page 78.

Après avoir sélectionné une source d'importation, cliquez sur le bouton **Transférer** pour afficher l'URL vers la source sous *Chemin*.

En cliquant sur **OK**, conpal LAN Crypt affiche les données sélectionnées dans le volet en haut à droite de la console. Vous pouvez y afficher les données sélectionnées dans une arborescence, rassemblées dans des unités organisationnelles (OU), des groupes et des utilisateurs.

Uniquement pour le serveur LDAP

Si l'ordinateur administrateur n'est pas un membre du domaine, utilisez cette procédure pour importer les groupes et les utilisateurs à partir d'un serveur :

1. Dans l'onglet *Serveur* de Paramètres centraux, entrez le nom du serveur, le nom d'utilisateur et le mot de passe.
2. Pour LDAP ou SSL, indiquez si <Microsoft> ou d'<autres> mises en œuvre sont en cours d'utilisation.
3. Dans le champ de saisie *Source d'importation*, entrez l'adresse du serveur à partir duquel les données doivent être importées.

3.10.4Préparatifs pour le transfert dans la base de données conpal LAN Crypt

Dans le volet en haut à droite sont affichés les OU, les groupes et utilisateurs tels qu'ils ont été stockés dans la source d'importation.

Parmi ces OU, groupes et utilisateurs affichés, sélectionnez ceux que vous voulez importer dans la base de données conpal LAN Crypt. Commencez par déplacer les objets sélectionnés dans le volet inférieur où vous pourrez les traiter.

Remarque : le fait d'ajouter un objet (nœud) dans le volet inférieur ne signifie pas pour autant que vous l'avez ajouté à la base de données. Vous pouvez uniquement regrouper les objets dans ce volet. Pour les transférer vers la base de données, cliquez sur **Ajouter à la base de données** ou **Synchroniser**.

3.10.4.1 Paramétrage du transfert de données

Vous pouvez optimiser les performances en définissant les paramètres de transfert. Ces derniers concernent uniquement les transferts dans le volet inférieur pour vous permettre de préparer le

transfert des données vers la base de données. Cliquez sur l'icône des paramètres de transfert pour ouvrir une boîte de dialogue proposant trois options :

- **Évaluer le statut des objets dans la base de données**

  Cette option ne s'applique que si les entrées figurent déjà dans la base de données, c'est-à-dire au moment de la synchronisation de la base de données. Si cette option est sélectionnée, vous pourrez visualiser les éléments suivants dans la vue inférieure de chaque objet :

  - si l'objet figure déjà dans la base de données (dans la colonne Statut).
  - si le responsable de la sécurité connecté a le droit de modifier un groupe (dans la colonne Ajouter groupe). Une croix rouge signale que le responsable de la sécurité ne détient pas le droit d'ajouter le groupe. Une coche verte signifie que le responsable de la sécurité a le droit d'ajouter le groupe.
  - si le responsable de la sécurité connecté a le droit d'ajouter des utilisateurs (dans la colonne Ajouter utilisateur). Une croix rouge signale que le responsable de la sécurité ne détient pas le droit d'ajouter des utilisateurs. Une coche verte signifie que le responsable de la sécurité a le droit d'ajouter des utilisateurs.

- **Calculer les affiliations**

  Si cette option est sélectionnée, le système affichera également les affiliations du groupe (les groupes et utilisateurs qui ne sont pas des membres directs des différents groupes). Pour les distinguer des membres directs, ils apparaissent sous forme d'icônes grisées.

Remarque : le système calcule les membres uniquement après leur transfert dans la base de données.

- **Trier les objets**

  Le tri par ordre alphabétique des groupes importants peut prendre beaucoup de temps. En règle générale, le tri n'est pas effectué. Si vous voulez trier les objets par ordre alphabétique, activez cette option.

Mise à jour de l'affichage

Si vous n'avez défini aucune option de transfert, vous pourrez réaliser ces actions après le transfert en cliquant sur le bouton **Mise à jour**. Cliquez sur "Mise à jour" pour ouvrir une boîte de dialogue affichant les mêmes options. La mise à jour concerne uniquement les données affichées dans le volet inférieur.

3.10.4.2 Transfert des objets vers le volet inférieur

En cliquant deux fois sur un nœud ou en sélectionnant un nœud puis en cliquant sur le bouton **Transférer**, vous activez le transfert des objets dans l'arborescence de la source d'importation dans le volet inférieur. Avant le transfert des objets, une boîte de dialogue s'affiche. Vous pouvez alors choisir le mode de transfert des différents conteneurs et objets.

- **Transférer uniquement cet objet :**
  Ajoute l'objet sélectionné sans son contenu.

- **Transférer aussi les membres directs :**
  Ajoute tous les objets présents dans le conteneur sélectionné.

- **Transfert récursif des membres :**
  Ajoute tous les objets présents dans ce conteneur ainsi que tous les objets membres et présents dans un autre conteneur. Les membres sont transférés avec leur hiérarchie complète.

Sélectionnez l'option voulue et cliquez sur **OK** pour transférer les objets vers le volet inférieur pour qu'ils soient prêts à être ajoutés à la base de données conpal LAN Crypt.

Avant leur transfert dans la base de données, vous pouvez ajouter plus de groupes dans cet affichage (provenant d'autres sources par exemple) puis effectuer en une seule fois le transfert de la totalité dans la base de données.

3.10.4.3 Ajout de données à la base de données ou synchronisation

Les objets ne seront pas ajoutés à la base de données conpal LAN Crypt tant qu'ils n'auront pas été regroupés dans le volet inférieur et que vous aurez cliqué sur le bouton **Ajouter à la base de données** ou **Synchroniser** dans cette fenêtre.

Remarque : si vous ajoutez des objets à une arborescence existante, vous devez toujours commencer par les ajouter à la base de données. Pour ce faire, cliquez sur le bouton **Ajouter à la base de données**.
La synchronisation sera utilisée seulement si la modification porte sur les relations entre les objets.

Lorsque vous cliquez sur **Ajouter à la base de données**, le système ajoute les objets puis lance la procédure de synchronisation. Celle-ci commence en affichant une fenêtre comportant trois options.

- **Synchroniser la base de données complète**
  Si vous sélectionnez cette option, le système synchronisera toutes les entrées présentes dans la base de données conpal LAN avec celles de la source d'importation. Les modifications sont affichées dans l'écran qui apparaît ensuite.

  Sélectionnez cette option si des objets ont été supprimés de Active Directory et devraient également l'être de la base de données.

Remarque : cela peut prendre longtemps si la synchronisation complète implique une arborescence complexe.

- **Synchroniser uniquement les entrées visibles**
  Correspond à la sélection dans le volet en bas à droite dans la console Administration.

- **Recalculer toutes les affiliations**

  Si vous sélectionnez cette option, le système recalcule tous les membres en fonction de leur source d'importation et les ajoute de nouveau à la base de données. Les membres sont ajoutés même s'ils ont été désactivés dans le volet en bas à droite de la console (à la suite de la désactivation de l'option **Calculer les affiliations** dans les paramètres de transfert).

- **Utiliser les relations visibles**

  Si vous sélectionnez cette option, seules les relations affichées dans le volet inférieur droit de la console seront ajoutées à la base de données. Les "Relations masquées" ne sont pas ajoutées à la base de données (et **Calculer les affiliations** est désactivée dans les paramètres de transfert).

Remarque : si cette option est utilisée pendant la synchronisation, sans que les relations des objets présents dans la base de données soient affichées dans le volet inférieur droit de la console, toutes les relations présentes dans la base de données seront supprimées.

Lorsque vous sélectionnez une option et cliquez sur **OK**, le système affiche une boîte de dialogue d'information sur la synchronisation. Vous devez confirmer les changements opérés dans cette boîte de dialogue.

- **Toutes les entrées**
  Affiche tous les changements dans une liste. Correspond au nombre total d'entrées dans les autres pages.

- **Objets supprimés**
  Affiche les objets supprimés dans la source d'importation (serveur) depuis la dernière synchronisation mais encore présents dans la base de données conpal LAN Crypt.

- **Relations nouvelles dans le répertoire**
  Affiche les objets et membres qui ont été ajoutés à la base de données conpal LAN Crypt ou les nouveaux objets et membres qui ont été créés dans la source d'importation (serveur) depuis la dernière synchronisation et n'ont pas encore été transférés dans la base de données.
- **Anciennes relations dans la base de données**
  Affiche les objets et les membres qui sont encore dans la base de données mais ne le sont plus dans la source d'importation. Par exemple des groupes peuvent avoir été supprimés ou des relations modifiées sur le serveur.

Remarque : la procédure de synchronisation évalue seulement les objets importés au moins une fois d'une source d'importation vers la base de données.
Si des objets sont supprimés dans la source d'importation, ces modifications sont uniquement implémentées dans la base de données lorsque l'option Synchroniser la base de données complète est sélectionnée.

Les groupes et les utilisateurs ajoutés manuellement dans la console Administration ne sont pas évalués pendant la synchronisation et n'apparaissent donc pas sur ces pages.

Vous pouvez annuler l'action pour chaque objet présent dans cet affichage en cliquant sur l'action (en la décochant). Seules les actions sélectionnées (cochées) seront exécutées. Cliquez sur **OK** pour achever la synchronisation des données.

Lorsque les OU (unités organisationnelles), les groupes et les utilisateurs ont été importés, les responsables de la sécurité responsables peuvent être assignés à chaque unité organisationnelle.

3.10.4.4 Ajout manuel de groupes

Pour ajouter un nouveau groupe manuellement, sélectionnez le nœud/groupe à ajouter au nouveau groupe, puis cliquez sur **Nouveau groupe** dans le menu contextuel.

Saisissez un nom pour le nouveau groupe dans le champ *Nom du groupe*, puis cliquez sur **OK**. Le système affiche maintenant le groupe dans conpal LAN Crypt Administration.

Dans la boîte de dialogue *Propriétés* du groupe, vous pouvez ajouter des utilisateurs existants ou en créer des nouveaux.

À la différence des groupes importés, vous pouvez déplacer les groupes créés manuellement à l'intérieur de leur structure hiérarchique à l'aide de glisser-déposer.

3.10.4.5 Relations entre les groupes

Pour créer des relations entre les groupes, vous pouvez copier un groupe et l'insérer dans un autre groupe. Un groupe inséré de la sorte s'affiche sous forme de raccourci dans le groupe parent. En conséquence, les membres du groupe inséré héritent de toutes les clés et de toutes les règles de chiffrement du groupe parent. La condition préalable à l'héritage des clés est que ces clés soient définies comme pouvant être héritées du groupe parent. Les droits de modification du groupe ne sont PAS hérités.

Comme ce groupe est inséré dans le nouvel emplacement sous forme de raccourci uniquement, les règles de chiffrement, les membres, les certificats et les clés ne sont pas affichés. Ces valeurs sont visibles uniquement dans le groupe "réel" dans la hiérarchie. Les clés héritées peuvent servir aussi à créer des règles de chiffrement.

Pour ajouter un groupe à un autre groupe via un raccourci :

1. Sélectionnez le groupe concerné, ouvrez son menu contextuel et sélectionnez **Copier**.
2. Sélectionnez le groupe cible dans lequel vous souhaitez insérer le groupe, puis cliquez sur **Insérer** dans le menu contextuel du groupe cible. Vous pouvez aussi créer un raccourci en appuyant sur Ctrl et en glissant et déposant le groupe sur le groupe cible.

3. Le système vous invite à confirmer l'ajout du groupe. Cliquez sur **OK** pour confirmer.

4. Le groupe est maintenant affiché comme raccourci sous l'autre groupe.

Il est désormais facile d'accorder tous les droits d'un groupe à tous les membres d'un autre groupe.

si vous voulez accorder aux membres de l'équipe 1 les mêmes droits que ceux détenus par les membres de l'équipe 2, pour un laps de temps limité (par exemple, pour que l'équipe 1 aide l'équipe 2 sur un projet), il vous suffit d'ajouter un raccourci au groupe équipe 1 dans le groupe équipe 2. Générez ensuite de nouveaux fichiers de stratégie. À la prochaine connexion d'un membre de l'équipe 1, il pourra accéder aux données de l'équipe 2. Lorsque l'équipe 1 n'aura plus besoin de droits supplémentaires, vous pourrez supprimer le raccourci du groupe équipe 2, puis générer de nouveaux fichiers de stratégie.
À la prochaine connexion d'un membre de l'équipe 1, il ne pourra plus accéder aux données de l'équipe 2.

3.10.5 Suppression de groupes

Vous pouvez supprimer des groupes individuels/unités organisationnelles (OU) ainsi que des raccourcis dans conpal LAN Crypt Administration.

Pour **supprimer un groupe**, sélectionnez **Supprimer** dans le menu contextuel de ce groupe. Toutes les relations des sous-groupes et des utilisateurs seront supprimées. Les utilisateurs proprement dits ne seront supprimés que si une OU est supprimée dans conpal LAN Crypt Administration. Dans ce cas, toutes les relations des utilisateurs pouvant exister dans d'autres OU sont également supprimées. Les clés ne sont JAMAIS supprimées. Elles restent dans la base de données conpal LAN Crypt.
Avant la suppression d'un groupe, une boîte de dialogue s'affiche et vous demande de confirmer que vous voulez supprimer le groupe.

Pour **supprimer le raccourci** d'un groupe, cliquez sur **Supprimer** dans le menu contextuel du raccourci. Seul le raccourci sera supprimé. Le groupe proprement dit ne sera pas touché.
Avant de supprimer un raccourci, une fenêtre s'affiche et vous demande de confirmer que vous voulez effectuer cette action.

Le menu contextuel du groupe parent contient l'entrée **Supprimer liens** que vous utilisez pour supprimer un raccourci. Cliquez sur **Supprimer liens** pour supprimer tous les raccourcis de ce groupe. Le groupe proprement dit ne sera pas touché.

3.10.6 Icônes de groupe

Les OU et les groupes sont représentés par des icônes différentes dans conpal LAN Crypt Administration en fonction de leur source d'importation :

L'icône du serveur montre la source à partir de laquelle les OU et les groupes ont été importés.

Icônes pour le raccourci vers le serveur (création d'un lien en le copiant)

Icône pour une OU importée d'un serveur.

Raccourci vers une OU importée.

Icône pour un groupe importé d'un serveur.

Raccourci vers le groupe importé.

Icône pour un fichier à partir duquel ont été importés les utilisateurs et les groupes.

Raccourci vers le fichier importé.

Icône pour un groupe importé d'un fichier.

Raccourci vers le groupe importé.

Groupe ajouté manuellement.

Raccourci vers un groupe ajouté manuellement.

3.11 Assignation de responsables de la sécurité à des OU

Après l'importation d'OU, de groupes et d'utilisateurs dans conpal LAN Crypt Administration, les responsables principaux de la sécurité peuvent assigner des responsables de la sécurité individuels aux diverses OU.

Le responsable de la sécurité peut ensuite utiliser les droits qui lui ont été accordés pour traiter les OU qui lui ont été assignées.

Pour s'assurer qu'un responsable de la sécurité peut seulement modifier l'OU dont il est responsable, le responsable principal de la sécurité peut lui "cacher" les autres nœuds. Le nœud est donc visible mais ne peut être modifié.

Si le responsable de la sécurité se connecte à conpal LAN Crypt Administration, il pourra voir uniquement la partie de la structure organisationnelle dont il est responsable.

3.11.1 Groupe parent d'un utilisateur

Dans conpal LAN Crypt, un utilisateur peut être membre de plusieurs groupes, mais dispose d'un groupe dédié qui est son groupe parent :

- Lors de l'importation de l'utilisateur via LDAP, le groupe parent est l'OU à laquelle cet utilisateur appartient.
- Lors de l'importation de l'utilisateur via un fichier, le groupe parent est celui dont l'utilisateur est membre, tel que défini dans le fichier.
- Lors de la création d'un nouvel utilisateur via la boîte de dialogue des propriétés du groupe, le groupe parent est celui à partir duquel la boîte de dialogue des propriétés du groupe a été ouverte.

Dans la console conpal LAN Crypt Administration, le groupe parent apparaît sous la forme d'une colonne dans le nœud Utilisateurs et certificats sélectionnés ou dans le noeud Membres et certificats du groupe (lors de la configuration dans l'onglet Paramètres d'utilisateurs, *see Paramètres d'utilisateurs* on page 38).

Le groupe parent d'un utilisateur affecte l'évaluation des droits dans les situations suivantes :

- Affichage des propriétés d'un utilisateur : Les responsables de la sécurité peuvent afficher les propriétés d'un utilisateur s'ils ont le droit Lire et Visible pour le groupe parent de l'utilisateur.
- Modification des propriétés d'un utilisateur : Les responsables de la sécurité peuvent modifier les propriétés d'un utilisateur s'ils ont l'autorisation globale Administrer les utilisateurs ainsi que les droits Ajouter utilisateur et Supprimer utilisateur sur le groupe parent de l'utilisateur.
- Création des profils : Si Créer des profils est paramétré pour le groupe d'un responsable de la sécurité, ce dernier est autorisé à créer des profils pour tous les membres du groupe, où le

groupe est aussi l'objet parent du groupe. Le responsable de la sécurité n'est pas autorisé à créer des profils pour les utilisateurs qui sont uniquement membres du groupe et qui ont un groupe parent différent. Pour cela, le droit Créer des profils est nécessaire pour tous les membres.

- Assignation de certificats : Si Assigner des certificats est paramétré pour un groupe, le responsable de la sécurité est autorisé à assigner des certificats à tous les membres du groupe, où le groupe est aussi l'objet parent du groupe. Le responsable de la sécurité n'est pas autorisé à assigner des certificats pour les utilisateurs qui sont uniquement membres du groupe et qui ont un groupe parent différent. Pour cela, le droit Assigner des certificats est nécessaire pour tous les membres.
- Copie d'utilisateurs : Lorsqu'un responsable de la sécurité souhaite ajouter un utilisateur à un groupe en utilisant la boîte de dialogue des propriétés d'un groupe (sur l'onglet Membres avec le bouton Ajouter), il doit avoir le droit Copier des utilisateurs pour le groupe parent de l'utilisateur.

3.11.2 Autorisation d'un responsable de la sécurité à visualiser et modifier des groupes

1. Pour autoriser un responsable de la sécurité à voir un nœud dans la console Administration, vous devez activer le droit **Visible** dans le nœud de base de l'arborescence de l'organisation.
2. Pour ce faire, sélectionnez le nœud de base dans l'arborescence puis cliquez sur **Propriétés** dans le menu contextuel pour ouvrir la boîte de dialogue *Propriétés* de ce nœud.
3. Basculer sur l'onglet *Sécurité*, puis cliquez sur **Ajouter**.
   Vous pouvez y sélectionner le responsable de la sécurité de votre choix pour traiter les groupes.

Remarque : il est possible d'assigner plusieurs responsables de la sécurité au même groupe.

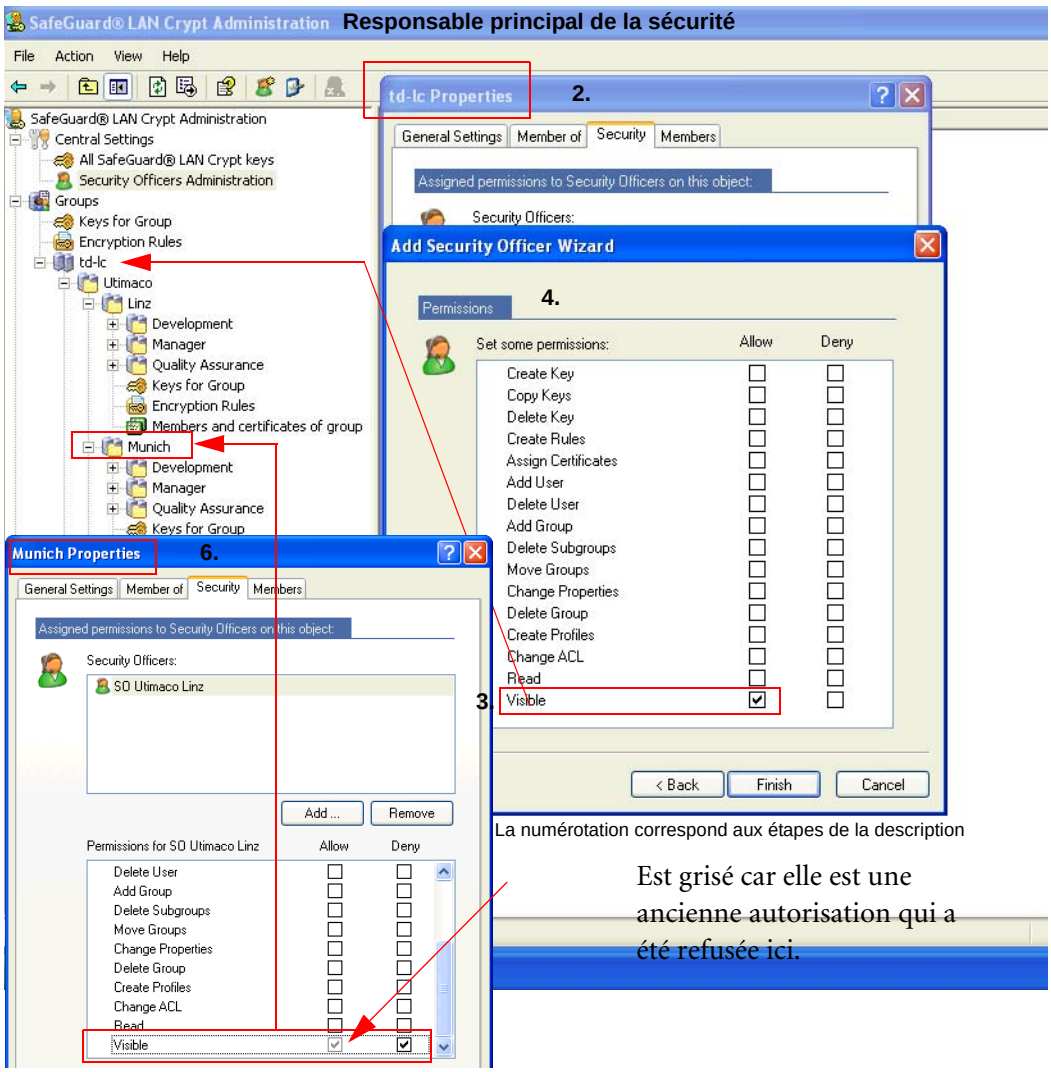
4. Cliquez sur **Suivant** pour afficher la boîte de dialogue *Autorisations* concernant ce responsable de la sécurité. Sélectionnez l'autorisation *Visible* puis cliquez sur **Terminer**. Cette autorisation est héritée en aval dans la hiérarchie du groupe, ce qui signifie que le responsable de la sécurité peut maintenant afficher tous les groupes.
   Si le responsable de la sécurité se connecte à la base de données avec ces paramètres, il peut visualiser l'arborescence complète de la console Administration mais ne peut pas la modifier.
5. L'étape suivante vous permet de masquer (occulter) les groupes dans la console Administration qui ne devront pas être vus par le responsable de la sécurité parce qu'il ne possède pas les droits d'accès correspondants.
6. Pour ce faire, sélectionnez ces groupes, ouvrez leurs *Propriétés*, puis cliquez sur l'onglet *Sécurité*.
7. Renseignez l'option **Visible** sur **Refuser** pour les groupes qui seront masqués pour le

responsable de la sécurité.

Remarque : si un droit d'accès à un groupe de niveau supérieur a été refusé de façon explicite à un responsable de la sécurité, ce droit ne peut pas être assigné à un groupe subordonné. Nous recommandons par conséquent d'assigner uniquement au responsable de la sécurité des autorisations de lecture et d'affichage à un groupe de niveau supérieur, de façon à ce qu'ils puissent assigner des droits à des groupes subordonnés sans provoquer de problèmes.

Remarque : conpal LAN Crypt peut être configuré pour automatiquement créer une ACL en détenant le droit visible sur le groupe racine d'un responsable de la sécurité nouvellement créé. Le responsable de la sécurité doit avoir l'autorisation globale Administrer les groupes ou Administrer les utilisateurs.Il peut ainsi accéder (consulter et/ou modifier) tous les groupes dont il est responsable.
Ce comportement doit être activé sur l'onglet *Autres paramètres* dans les **Paramètres centraux**.

Exemple :



La numérotation correspond aux étapes de la description

Est grisé car elle est une ancienne autorisation qui a été refusée ici.

Lorsqu'un responsable de la sécurité se connecte avec ces paramètres en place, ils voient :

Le responsable de la sécurité voit seulement les groupes dont il détient l'autorisation **Visible**. Ces groupes sont grisés car le responsable de la sécurité ne possède à cet instant aucun droit pour les traiter.

Si les autorisations **Visible** et **Lire** ont été simultanément assignées au responsable de la sécurité, le système affichera également les composants logiciels enfichables pour les *Règles de chiffrement*, *Membres et certificats du groupe* et *Clé du groupe* en dessous de ces groupes. Le responsable de la sécurité peut voir le contenu des composants enfichables, mais ne peut pas le modifier.

Vous pouvez utiliser l'autorisation **Lire** pour communiquer au responsable de la sécurité des informations sur les autres groupes sans l'autoriser à les modifier : le système inclut simplement ces informations dans l'affichage du responsable de la sécurité.

Remarque : si l'autorisation **Lire** a été également accordée au responsable de la sécurité, vous devrez le refuser à nouveau de manière spécifique afin de pouvoir remasquer les groupes. Il ne suffit pas de refuser l'autorisation **Visible**.

3.11.3 Octroi d'autorisations au responsable de la sécurité pour traiter les groupes

Dès que vous avez configuré le responsable de la sécurité pour qu'il visualise les groupes à modifier, vous pouvez lui accorder les autorisations correspondantes.

Ces autorisations sont héritées en aval dans la hiérarchie organisationnelle et vous pouvez le refuser ailleurs, plus bas dans la hiérarchie.

1. Sélectionnez le groupe pour lequel vous voulez accorder des droits au responsable de la sécurité, ouvrez la boîte de dialogue *Propriétés*, puis cliquez sur l'onglet *Sécurité*.

2. Tous les responsables de la sécurité assignés à ce groupe sont affichés sous Responsables de la sécurité. Lorsque vous sélectionnez un responsable de la sécurité, le système affiche ses autorisations valides dans la partie inférieure de la boîte de dialogue.
   Les autorisations **héritées** d'un autre groupe sont signalées par une coche grise.
   Les autorisations verrouillées par la configuration des droits globaux sont signalés par une case à cocher complètement grisée.

Remarque : la configuration des autorisations globales détermine quelles autorisations peuvent être assignées à un responsable de la sécurité en particulier. Les droits globaux sont déterminés à la génération du responsable de la sécurité.

Remarque : Cliquez sur **Accepter/Refuser** pour accepter ou refuser tous les droits. Cliquez à nouveau pour annuler la sélection de tous les droits globaux. Si tous les droits sont sélectionnés, vous pourrez à tout moment annuler ou activer leur sélection en fonction des besoins. La configuration des autorisations globales indique qu'il est impossible d'accorder les droits désactivés au responsable de la sécurité.

Vous pouvez assigner les droits suivants :

Droits	Description
Créer une clé	Le responsable de la sécurité a le droit de générer des clés dans le groupe.
Copier des clés	Le responsable de la sécurité a le droit de copier des clés.
Supprimer la clé	Le responsable de la sécurité a le droit de supprimer des clés.
Créer des règles	Le responsable de la sécurité est autorisé à générer des règles de chiffrement pour les utilisateurs.
Assigner des certificats	Le responsable de la sécurité a le droit d'assigner des certificats aux utilisateurs. Le responsable de la sécurité peut lancer l'assistant pour assigner les certificats. Cette autorisation permet au responsable de la sécurité d'assigner des certificats aux utilisateurs du groupe qui est aussi le groupe parent.
Assigner des certificats à tous les membres	Cette autorisation requiert que l'autorisation Assigner des certificats soit paramétrée. Assigner des certificats à tous les membres permet au responsable de la sécurité d'assigner des certificats à tous les utilisateurs du groupe : aux utilisateurs dont le groupe est le groupe parent et à ceux membres du groupe et qui ont un groupe parent différent. **Remarque :** si vous paramétrez Assigner des certificats à tous les membres sur Autoriser, l'autorisation Assigner des certificats est automatiquement paramétrée sur Autoriser. Si vous paramétrez Assigner des certificats sur Refuser, l'autorisation Assigner des certificats à tous les membres est automatiquement paramétrée sur Refuser.
Ajouter un utilisateur	Le responsable de la sécurité a le droit d'ajouter des clés dans le groupe manuellement. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.

Droits	Description
Copier un utilisateur	Le responsable de la sécurité a le droit d'ajouter des utilisateurs de ce groupe dans un autre groupe. Ceci est autorisé seulement pour les membres où ce groupe est aussi l'objet parent.
Supprimer un utilisateur	Le responsable de la sécurité est autorisé à utiliser le composant logiciel enfichable *Membres et certificats du groupe* pour supprimer des utilisateurs. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Ajouter un groupe	Le responsable de la sécurité est autorisé à utiliser le menu contextuel d'un groupe pour ajouter de nouveaux groupes. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Supprimer des sous-groupes	Le responsable de la sécurité est autorisé à supprimer des sous-groupes pour ce groupe. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Déplacer des groupes	Le responsable de la sécurité a le droit de déplacer des groupes créés manuellement dans la console Administration (par glisser-déposer). Impossible de déplacer les groupes importés. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Modifier les propriétés	Le responsable de la sécurité a le droit de modifier les propriétés d'un groupe.
Supprimer un groupe	Le responsable de la sécurité a le droit de supprimer des groupes. Cela suppose que le responsable de la sécurité a retiré l'autorisation "Supprimer des sous-groupes" du groupe ci-dessus. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.

Droits	Description
Créer des profils	Le responsable de la sécurité a l'autorisation de lancer le programme de résolution des profils et de générer des fichiers de stratégie pour les utilisateurs sélectionnés. Créer des profils permet au responsable de la sécurité de créer des profils pour les utilisateurs du groupe qui est aussi le groupe parent.
Créer des profils pour tous les membres	Cette autorisation requiert que l'autorisation Créer des profils soit paramétrée. Créer des profils pour tous les membres permet au responsable de la sécurité de créer des profils pour tous les utilisateurs du groupe : Les utilisateurs dont le groupe est le groupe parent et ceux membres du groupe et qui ont un groupe parent différent. **Remarque :** si vous paramétrez Créer des profils pour tous les membres sur Autoriser, l'autorisation Créer des profils est automatiquement paramétrée sur Autoriser. Si vous paramétrez Créer des profils sur Refuser, l'autorisation Créer des profils pour tous les membres est automatiquement paramétrée sur Refuser.
Modifier une ACL	Le responsable de la sécurité a le droit de modifier l'ACL d'un groupe (par exemple, en ajoutant un autre responsable de la sécurité).
Lire	Le responsable de la sécurité dispose des droits en lecture sur ce groupe et peut voir le contenu des composants logiciels enfichables. Activation automatique si des autorisations de modification sont accordées.
Visible	Le responsable de la sécurité peut voir le groupe. Est défini dans le nœud de base et hérité en aval. En cas de refus pour un responsable de la sécurité, le groupe est masqué (avec refus de "Lecture").

3. Sélectionnez les droits que vous voulez accorder au responsable de la sécurité. Cliquez sur **Transférer** pour enregistrer les paramètres dans la base de données.

4. Si vous avez assigné d'autres responsables de la sécurité à ce groupe, vous pourrez maintenant également configurer leurs autorisations. Pour afficher les droits définis pour les responsables de la sécurité, sélectionnez-les sous *Responsables de la sécurité*.

Remarque : les changements apportés aux autorisations d'un responsable de la sécurité pour un groupe ne prennent effet qu'une fois que le responsable de la sécurité correspondant s'est de nouveau connecté à conpal Enterprise LAN Crypt Administration.

3.12 Propriétés des groupes

La boîte de dialogue *Propriétés* pour un groupe (<Groupe>/menu contextuel/Propriétés) comprend quatre onglets dans lesquels vous pouvez modifier les propriétés d'un groupe.

3.12.1 Onglet Propriétés

L'onglet Propriétés affiche les éléments suivants :

- Nom
- Nom DNS
- GUID
- Commentaire

associé au groupe concerné

3.12.2 Onglet Membre de

L'onglet *Membre de* affiche les groupes qui incluent le groupe actuel comme membre.

3.12.3 Ajout/Suppression de membres

Vous pouvez ajouter des membres au groupe dans l'onglet *Membres*. Cette liste affiche tous les utilisateurs et groupes existants appartenant à ce groupe. Vous pouvez uniquement modifier les utilisateurs de cette liste, pas les groupes !

Ajouter :

Ouvre une boîte de dialogue permettant de sélectionner des utilisateurs et de les ajouter au groupe.

Permet d'afficher tous les utilisateurs ou de sélectionner des groupes ou des individus, grâce à des paramètres fictifs SQL.

Comme l'affichage de tous les utilisateurs peut prendre beaucoup de temps, conpal LAN Crypt vous permet de définir des critères de recherche pour filtrer le processus de recherche.

Sélectionnez l'option *Afficher les utilisateurs correspondants* pour activer les champs de saisie en vue de définir vos critères de recherche :

Les informations suivantes sur l'utilisateur sont récupérées dans la base de données de conpal LAN Crypt :

- Nom de connexion
- Nom d'utilisateur
- Assignation entre l'utilisateur et le certificat
- Demandeur du certificat
- Numéro de série du certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Nom du groupe parent

Vous pouvez définir des critères de recherche d'après ces attributs. conpal LAN Crypt recherche la chaîne de caractères définie dans les attributs de l'utilisateur récupérés.

Dans la première liste déroulante, vous pouvez sélectionner le ou les attributs sur lesquels doit porter le processus de recherche.

En outre, vous pouvez définir si l'attribut sélectionné doit correspondre à la chaîne de caractères saisie (*faut être*) ou si seuls doivent être affichés les utilisateurs pour lesquels l'attribut sélectionné ne correspond pas à la chaîne de caractères saisie (*ne faut pas être*).

Dans la liste déroulante située sur la droite, saisissez la chaîne de caractères que conpal LAN Crypt recherche dans l'attribut défini.

Utilisez les caractères génériques SQL suivants pour saisir la chaîne de caractères :

%	n'importe quelle séquence de caractères
_	caractère unique (par exemple, a__ recherchera tous les noms contenant trois caractères et commençant par a)
[]	caractère unique d'une liste (par exemple, [a-cg]% recherchera tous les noms commençant par a, b, c ou g)
[^]	caractère unique non inclus dans une liste (par exemple, [^a]% recherchera tous les noms ne commençant pas par a)

Vous pouvez indiquer jusqu'à trois conditions dans le processus de recherche.

Si vous entrez plusieurs conditions, définissez la façon dont ces conditions sont à associer (ET/ OU).

Si vous cliquez sur OK, tous les utilisateurs dont le nom est sélectionné dans la liste sont transférés vers le groupe actuel.

Nouveau :
Ouvre une boîte de dialogue dans laquelle vous pouvez créer un nouvel utilisateur.

Supprimer :
Supprime l'utilisateur sélectionné et ses relations dans le groupe en cours.
Si l'utilisateur n'est membre d'aucun autre groupe, il est supprimé de la base de données conpal LAN Crypt.
Si l'utilisateur est membre de plusieurs groupes et si le groupe en cours est le groupe parent de l'utilisateur, l'action résultante dépend du type du groupe :

- si le groupe est une OU ou un groupe racine et si l'utilisateur est membre d'une autre OU ou d'un autre groupe racine, cette OU ou ce groupe racine devient le groupe parent de l'utilisateur. S'il n'y a aucune autre OU ou groupe racine dont l'utilisateur est membre, l'utilisateur est supprimé (comme dans Active Directory où un utilisateur est supprimé, lorsque l'OU à laquelle l'utilisateur appartient est supprimée).
- si le groupe est un groupe simple (non pas une OU ou un groupe racine), l'un des autres groupes auquel l'utilisateur appartient devient le groupe parent de l'utilisateur.

Propriétés :
Affiche les propriétés de l'utilisateur sélectionné.

Remarque : un utilisateur peut exister seulement une fois dans un conteneur précis. Si vous essayez de créer/ajouter un utilisateur dans un conteneur dans lequel il est déjà présent, un message s'affiche vous informant que l'opération n'est pas possible.
En revanche, plusieurs utilisateurs portant le même nom peuvent être présent dans le système, à condition qu'ils ne soient pas dans le même conteneur.

3.12.4 Ajout de responsable de la sécurité

Dans l'onglet *Sécurité*, un responsable de la sécurité peut aussi ajouter d'autres responsables de la sécurité au groupe et assigner des droits à ce groupe. La condition préalable à cette action est la détention du droit **Modifier ACL** par le responsable de la sécurité qui veut procéder à cet ajout.

Remarque : si le responsable de la sécurité ajoute des responsables de la sécurité au groupe, il peut leur assigner ses propres autorisations (et seulement celles-là).
Un responsable de la sécurité ne peut pas s'ajouter à une ACL ou modifier ses droits dans une ACL.

3.13 Propriétés des utilisateurs

La boîte de dialogue *Propriétés* pour un utilisateur (<utilisateur>/menu contextuel/Propriétés) comprend quatre onglets dans lesquels vous pouvez modifier les propriétés d'un utilisateur :

Onglet Certificats

L'onglet *Certificats* affiche tous les certificats assignés à un utilisateur. Cet onglet vous permet également de créer un nouveau certificat conpal LAN Crypt pour l'utilisateur, d'ajouter un nouveau certificat au dépôt de certificats ou d'importer un certificat à partir d'un fichier (see *Assignation d'un certificat à un utilisateur* on page 119).

Onglet Groupes

L'onglet *Groupes* affiche les groupes dont l'utilisateur en cours est membre.

Onglet Règles

L'onglet *Règles* affiche toutes les règles de chiffrement pour l'utilisateur. C'est une manière commode de visualiser toutes les règles de chiffrement en cours de validité pour un utilisateur précis, même s'il provient de groupes différents.

Les colonnes S, X, I renseignent sur le type de règle :

- **S** (sous-répertoires) : les sous-répertoires sont inclus dans le chiffrement.
- **X** (exclure ce chemin) : le chemin est exclu du chiffrement.
- **I** (ignorer ce chemin) : le dossier est ignoré par conpal LAN Crypt.
  Pour plus d'informations, reportez-vous à la section see *Génération des règles de chiffrement* on page 113.

Sous **Hérité de**, vous pouvez voir le groupe à partir duquel cette règle précise a été héritée.

Onglet Détails

Les données de l'utilisateur sont affichées et peuvent être modifiées dans l'onglet *Détails*.

L'adresse de messagerie est ajoutée au fichier journal des mots de passe pour les certificats générés par conpal LAN Crypt. Elle peut servir, par exemple, à créer à un courrier de codes PIN transmis par messagerie électronique.

Remarque : modifiez avec précaution les données de l'utilisateur. Les modifications apportées peuvent avoir des effets secondaires indésirables.
Par exemple, si vous changez le nom de connexion dans cet onglet, il se peut que l'utilisateur ne puisse plus accéder
à son fichier de stratégie car le client emploie un nom de connexion différent (ancien) pour rechercher un fichier de stratégie.

3.14 Conception de l'environnement de sécurité

Grâce à sa grande flexibilité, conpal LAN Crypt peut être facilement adapté à toutes les exigences de sécurité d'une entreprise.

Néanmoins, il est nécessaire d'avoir défini une stratégie de sécurité applicable à l'entreprise avant de créer l'environnement conpal LAN Crypt.

Nous recommandons généralement de commencer par une stratégie de sécurité relativement restrictive car il est plus facile de rendre ultérieurement une stratégie plus souple que plus stricte sur le système conpal LAN Crypt. Passer à une stratégie libérale plus restrictive peut causer des problèmes de sécurité difficiles à résoudre. Pour éviter cette situation, il est essentiel qu'une stratégie de sécurité applicable à l'entreprise ait été définie avant la génération et la distribution des profils de chiffrement.

3.15 Génération d'une clé

Les nouvelles clés sont générées sous le nœud du groupe dans lequel elles doivent être utilisées. Vous pouvez indiquer pour chacune des clés si elles sont héritées en aval dans la hiérarchie du groupe.

Remarque : toutes les clés existantes sont affichées dans **Paramètres Centraux\Toutes les Clés conpal LAN Crypt**. Mais il est impossible de les traiter à cet emplacement. Cet affichage est une vue d'ensemble des clés utilisées dans conpal LAN Crypt.

Remarque : un responsable de la sécurité qui détient seulement le droit **Créer des clés** et pas **Créer des profils** ne peut pas ajouter de valeur pendant la génération de clés. La valeur est générée automatiquement lorsqu'une clé est transmise à un profil.

Une clé conpal LAN Crypt comprend les composants suivants :

- **un nom**
  Pour une clarté optimale, nous vous recommandons que le nom du groupe d'utilisateurs fasse partie du nom de la clé.
  Les noms que vous attribuez sont particulièrement importants car conpal LAN Crypt est également capable de trier les clés.
  conpal LAN Crypt emploie des noms de clés spécifiques pour générer un nom de clé de 16 caractères destiné à un usage interne. Il joint le préfixe de la région concernée au début de ce nom de clé.

- **une valeur de clé**
  La longueur de la clé dépend de l'algorithme utilisé. La valeur de la clé peut être définie en caractères ANSI ou en numérotation hexadécimale (numéros et caractères valides : 0123456789abcdef). L'autre valeur associée est mise à jour automatiquement.

Vous n'avez pas besoin d'entrer une valeur de clé. Dans ce cas, la valeur est générée de façon aléatoire lorsque la clé est utilisée pour la première fois dans un profil utilisateur.

- **un algorithme de chiffrement**
  AES-128, AES-256, DES, 3DES, IDEA, XOR
- **un commentaire** (facultatif)
- **un GUID de clé** (facultatif)
  Ceci permet d'entrer manuellement un GUID de clé, de façon à ce que les fichiers chiffrés puissent être échangés entre deux installations distinctes de conpal LAN Crypt (see *Onglet Clés* on page 40).
  Si ce champ est vide, le GUID est créé de façon automatique.

Pour générer une nouvelle clé

1. Sélectionnez **Clé de groupe** sous le groupe ciblé pour la génération d'une clé.
2. Cliquez sur l'icône jaune en forme de clé ou cliquez avec le bouton droit de la souris dans le volet droit de la console pour afficher le menu contextuel puis cliquez sur **Nouvelle clé** dans ce menu.
3. Entrez un nom pour la nouvelle clé dans le champ de saisie supérieur. Les noms de clés ne doivent pas inclure de barre oblique inverse (\), de barre oblique (/), de guillemets et le caractère &.
   conpal LAN Crypt utilise ce nom pour générer un nom de clé unique de 16 caractères destiné à un usage interne. Il ajoute également le préfixe de la région (si celle-ci a été désignée dans les propriétés du responsable de la sécurité) au début de ce nom unique. Le nom interne est affiché à droite, en regard de la liste déroulante des algorithmes.
   Vous pourrez modifier ultérieurement le nom de la clé, mais pas le nom interne qui en a été dérivé.
4. Sélectionnez un algorithme de chiffrement dans la liste déroulante (AES-128, AES-256, DES, 3DES, IDEA, XOR).
   La liste affiche uniquement les algorithmes que vous avez rendus disponibles dans *Paramètres centraux*.
5. Indiquez si la clé peut être héritée du groupe :
   - **Non**
     La clé n'est pas héritée et est ainsi disponible uniquement dans le groupe actuel.
   - **Une fois**
     La clé est héritée dans le ou les groupes du niveau d'arborescence suivant, au-dessous du groupe actuel.

- **Oui**
  La clé est héritée dans tous les groupes des niveaux d'arborescence situés au-dessous du groupe actuel. Elle est accessible à ce niveau pour générer les règles de chiffrement.

6. Entrez un commentaire pour cette clé dans le champ de saisie suivant.

7. Si nécessaire cliquez sur la case à cocher **Entrez le GUID de clé manuellement au format {88888888-4444-4444-4444-CCCCCCCCCCCC}** et entrez le GUID requis (ceci n'est possible que si l'option spécifiant que les responsables de la sécurité peuvent définir le GUID des nouvelles clés est active dans la section "Paramètres centraux"). Le GUID prédéfini, {88888888-4444-4444-4444-CCCCCCCCCCCC}, ne peut pas être utilisé tel quel à ce stade. Vous devez le modifier dans tous les cas.

8. Saisissez une valeur hexadécimale (lettres A à F, chiffres 0 à 9) ou une chaîne de caractères dans le champ de saisie ANSI pour la valeur de clé. L'autre valeur associée est mise à jour automatiquement. Vous avez également la possibilité de cliquer sur **Aléatoire** (recommandé) pour que conpal LAN Crypt calcule une valeur.

9. Cliquez sur **OK**.

▶ La nouvelle clé est affichée dans la console Administration.

3.15.1 Clés spécifiques

Outre la génération manuelle de clés, conpal LAN Crypt permet aussi d'utiliser des clés spécifiques aux utilisateurs et aux groupes.

Lorsque des clés sont assignées à des chemins de chiffrement, dans la liste de clés, une clé <**USERKEY**> est toujours affichée. Il s'agit d'un paramètre fictif pour une clé spécifique à un utilisateur que le système génère automatiquement pour chaque utilisateur lorsqu'il établit les règles de chiffrement.
<**GROUPKEY**>
Vous pouvez utiliser <GROUPKEY> de la même façon que <USERKEY> pour générer une clé commune à tous les membres d'un groupe. Le système génère la clé de groupe automatiquement lorsqu'il établit les règles de chiffrement.

Exemple : Il est possible d'utiliser <USERKEY> si tous les utilisateurs se servent d'une unité de réseau, U:, qui contient un répertoire par utilisateur avec l'accès à ce répertoire réservé uniquement à l'utilisateur approprié.
La règle de chiffrement utilisée pour spécifier ceci ressemblerait à ceci :
`U:\*.* <USERKEY>`
Un autre exemple consisterait à utiliser <USERKEY> pour chiffrer des répertoires temporaires locaux.

Les clés spécifiques aux utilisateurs et aux groupes n'apparaissent pas dans la fenêtre affichée par défaut sous Paramètres centraux/Toutes les clés conpal LAN Crypt puisqu'elles ne sont généralement pas nécessaires. Toutefois, si nécessaire, un responsable de principal de la sécurité ou un responsable de la sécurité avec l'autorisation globale Utiliser des clés spécifiques peut afficher ces clés afin que les données soient visibles.

Si nécessaire, les valeurs de ces clés spécifiques peuvent être aussi affichées dans la boîte de dialogue *Propriétés* (*menu contextuel*/**Propriétés**) des clés correspondantes.

Pour afficher ces clés spécifiques, cliquez sur **Afficher clés spécifiques** dans le menu contextuel de la liste des clés. Seules ces clés spécifiques seront désormais affichées. Pour rétablir l'affichage par défaut, cliquez de nouveau sur **Afficher clés spécifiques**.

Remarque : les clés spécifiques ne sont pas effacées de la base de données lorsque l'utilisateur ou le groupe auquel elles appartiennent est supprimé. Elles sont stockées dans la base de données et peuvent être affichées dans Paramètres centraux/Toutes les clés conpal LAN Crypt /Afficher clés spécifiques.

Réaffectation de clés spécifiques

Dans certains cas, vous devrez peut-être réassigner une clé spécifique à un utilisateur ou à un groupe.

Exemple : Un utilisateur est importé de Active Directory dans conpal LAN Crypt Administration.
Une clé spécifique à l'utilisateur est générée pour cet utilisateur. Si vous supprimez le groupe auquel appartient l'utilisateur dans conpal LAN Crypt Administration puis le réimportez, conpal LAN Crypt générera automatiquement une nouvelle clé spécifique à l'utilisateur lorsqu'il génère les fichiers de stratégie de cet utilisateur.
L'utilisateur ne peut plus accéder aux données chiffrées avec "l'ancienne" clé spécifique à l'utilisateur.

Pour résoudre ce type de situation, vous pouvez configurer conpal LAN Crypt de manière à pouvoir réassigner les clés spécifiques d'utilisateurs ou de groupes supprimés.

Pour ce faire, ajoutez la `valeur DWORD "ShowUserKeyPage"` au registre de Windows avec la valeur de données `"1"` sous la clé :

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Sophos\
SGLANCrypt
```

Vous pouvez aussi effectuer cette entrée dans le registre de Windows pour un utilisateur spécifique sous `HKEY_CURRENT_USER\.....`

Si cette valeur est trouvée dans le registre de Windows, l'onglet *Clé spécifique* sera ajouté aux boîtes de dialogue *Propriétés*.
(<utilisateur/groupe>/menu contextuel/Propriétés) des utilisateurs et des groupes.

Dans cet onglet, vous pouvez assigner des clés spécifiques. Elles figurent dans la base de données et ne sont pas assignées à un utilisateur ou à un groupe, ni à des utilisateurs, ni même encore à des groupes spécifiques.

Si une clé spécifique est assignée à un utilisateur ou à un groupe, elle sera affichée dans l'onglet *Clé spécifique*. Si aucune clé spécifique n'est affichée, vous pouvez remplacer la clé en cours par une clé spécifique différente ou assigner une nouvelle clé. Vous pouvez utiliser n'importe quelle clé présente dans la base de données qui n'a pas encore été assignée à un utilisateur ou à un groupe.

Remarque : pour effectuer la modification, un responsable de la sécurité doit avoir l'autorisation **Utiliser clés spécifiques**. Si tel n'est pas le cas, il dispose seulement d'un accès en lecture.

Cliquez sur le bouton **Parcourir...** pour afficher la liste des clés disponibles. Choisissez une clé et cliquez sur **OK**.

Dans l'onglet Clé spécifique, cliquez sur **OK**.

Si la clé spécifique actuelle a été remplacée par une autre clé, elle continue à figurer dans la base de données en tant que clé non affectée.

3.15.2 Importation de clés

Vous pouvez toujours utiliser les clés générées dans les versions 2.x de conpal LAN Crypt. Il vous suffit d'importer les clés créées dans les versions 2.x à partir des fichiers de clés de la version 2x.

Vous pouvez uniquement importer une clé marquée comme **exportable** dans les fichiers de clés, à condition d'avoir l'identifiant et le mot de passe maîtres de ce fichier de clé et de détenir les droits correspondants. Le fichier n'est pas forcément protégé en écriture.

Pour importer une clé, sélectionnez le nœud *Clé de groupe* en dessous du groupe correspondant puis cliquez sur **Importer la clé à partir du fichier clé** dans le menu contextuel.

Sélectionnez le fichier de clé et saisissez son identifiant maître dans le champ *Nom d'utilisateur* et son mot de passe maître dans le champ *Mot de passe*.

Cliquez sur **OK**. Les clés sont affichées dans le volet droit.

3.15.3 Activer/Désactiver les clés

conpal LAN Crypt vous permet d'activer ou de désactiver une clé existante. Si vous la désactivez, elle ne sera plus disponible au moment de définir les règles de chiffrement.

Mais vous pourrez toujours utiliser cette clé dans les règles de chiffrement en cours d'utilisation. Elle reste enregistrée dans la base de données d'administration et vous pouvez la réactiver si nécessaire.

Pour désactiver/activer (et vice-versa) une clé, sélectionnez cette clé puis cliquez sur **Désactivé/ Activé** dans le menu contextuel.

Une clé désactivée est reconnaissable à l'icône en forme de clé rouge placée en début de ligne.

3.15.4 Relations entre les clés

En plus de la génération de clés pour le groupe auquel elles sont destinées, il est également possible de mettre des clés à la disposition des utilisateurs d'un groupe en créant une relation (raccourci) vers une clé d'un groupe différent.

Exemple : Par exemple : Si vous voulez accorder aux membres d'une équipe les mêmes droits que ceux d'une équipe différente pendant un laps de temps limité, il vous suffit d'ajouter un raccourci vers une clé de groupe vers un autre groupe. Vous pouvez alors utiliser le raccourci vers la clé pour créer des règles de chiffrement.
S'il vous est impossible d'utiliser un raccourci vers une clé, vous devrez créer un nouveau groupe, ajouter les utilisateurs des deux groupes au nouveau groupe et créer de nouvelles clés et règles de chiffrement pour que cet échange simple de données soit possible. Un raccourci vers une clé est un moyen rapide et simple d'échanger des données.

Pour ajouter une clé à un autre groupe via un raccourci, glissez-déposez la clé à partir du nœud *Clés pour groupe* d'un groupe dans le nœud du groupe destinataire. Vous pouvez également copier la clé dans le groupe source et le coller dans le groupe cible.

Une clé importée de cette manière est affichée sous forme de raccourci  .

Un responsable de la sécurité doit détenir ces autorisations globales avant de pouvoir insérer des raccourcis vers des clés :

- **Créer des clés**
- **Copier des clés**

Dans le groupe source, il doit également détenir les **droits spécifiques au groupe**

- **Copier des clés**

et

- **Créer des clés**

dans le groupe cible.

Pour supprimer un raccourci, le responsable de la sécurité doit détenir le droit global et le droit spécifique au groupe **Supprimer clé**.

Les clés insérées comme des raccourcis ont les propriétés suivantes :

- Elles ne seront PAS héritées et seront donc uniquement disponibles dans le groupe dans lequel elles ont été créées. PAS dans les sous-groupes.
- Si la clé "d'origine" est supprimée, tous les raccourcis le seront également.

Remarque : comme pour les clés de groupe normales, si vous supprimez une référence, cela ne signifie pas que la règle utilisée par ces clés ne sera plus valide. Pour supprimer l'accès aux données, vous devez supprimer la règle de chiffrement correspondante et générer un nouveau fichier de stratégie. Pour la première fois, le client doit charger le nouveau fichier de stratégie pour éviter qu'un utilisateur ne puisse accéder à ces données.

3.15.5 Suppression des clés dans un groupe

Vous pouvez supprimer une clé uniquement dans le groupe dans lequel elle a été générée. Vous devez la désactiver avant de la supprimer.

Si vous supprimez des clés en cours d'utilisation, elles sont supprimées du groupe mais restent dans la base de données sous forme de clés non assignées et sont affichées dans *Paramètres centraux/Toutes les clés conpal LAN Crypt*.

Nouvel ajout de clés

Au cas où vous auriez besoin de cette clé ultérieurement (par exemple, pour accéder à une sauvegarde chiffrée de données anciennes), il vous suffit de sélectionner cette clé dans la liste de toutes les clés conpal LAN Crypt pour la glisser-déposer vers le groupe concerné où vous pourrez l'utiliser à nouveau. Un responsable de la sécurité peut ajouter une clé à n'importe quel groupe détenant le droit **Créer des clés**. La clé est effectivement ajoutée au groupe ; ce n'est pas un raccourci.

Remarque : si vous supprimez une clé qui n'a jamais été utilisée dans une règle de chiffrement, elle est effectivement supprimée de la base de données. La clé n'est plus affichée dans Toutes les clés conpal LAN Crypt.

3.15.6 Suppression de clés dans la base de données

Si les conditions suivantes sont remplies, il est possible de supprimer effectivement des clés (sous le nœud *Toutes les clés conpal LAN Crypt*) dans la base de données :

- Vous devez être connecté comme responsable principal de la sécurité.
- Les clés ne doivent pas être utilisées dans une règle de chiffrement.
- La clé ne doit pas être présente dans un groupe quelconque.
- La clé ne doit pas être une clé spécifique assignée à un utilisateur ou à un groupe.
- La clé doit être désactivée.

3.15.7 Modification des clés

Après avoir généré une clé, vous pouvez modifier son nom, le type d'héritage spécifié et le commentaire.

Vous pouvez voir si une clé est déjà utilisée ou non dans la colonne *utilisée*.

Pour modifier une clé, allez dans le groupe dans lequel la clé a été générée et cliquez deux fois sur le nom de la clé concernée. Vous pouvez changer la clé dans la boîte de dialogue qui s'affiche.

3.15.7.1 La boîte de dialogue Propriétés

La boîte de dialogue *Propriétés* affiche les informations relatives à la clé sélectionnée. Vous pouvez y modifier le nom long de la clé et les paramètres d'héritage de la clé. Vous ne pouvez pas modifier le nom de clé unique à 16 caractères qui a été généré par conpal LAN Crypt.

Remarque : pour modifier une clé, le responsable de la sécurité doit détenir le droit **Générer une clé**, spécifique pour les groupes dans lesquels la clé a été générée.
Il est impossible de modifier les clés n'appartenant pas à un groupe spécifique.

Cliquez deux fois sur une clé pour afficher ses propriétés.

La boîte de dialogue *Propriétés* comprend trois onglets :

- L'onglet *Clé* affiche les données d'une clé. Vous pouvez y modifier le nom long de la clé et les paramètres d'héritage de la clé.
  Cliquez sur **Afficher la valeur de la clé** pour afficher la valeur de la clé.
- L'onglet *Groupes* affiche tous les groupes dans lesquels la clé est disponible et sert à créer des règles de chiffrement.
- L'onglet *Règles* affiche toutes les règles de chiffrement dans lesquelles la clé est utilisée.

Les onglets *Groupes* et *Règles* donnent uniquement des renseignements. Ils ne permettent pas de procéder à des modifications.

3.16 Règles de chiffrement

Les règles de chiffrement de conpal LAN Crypt définissent précisément quelles données peuvent être chiffrées avec chacune des clés. Une règle de chiffrement comprend un chemin de chiffrement et une clé.

Les règles de chiffrement définies pour un groupe constituent un profil de chiffrement conpal LAN Crypt.

Le profil de chiffrement pour un groupe peut contenir différentes règles de chiffrement, chacune servant à chiffrer un type de données spécifique.

Vous pouvez chiffrer des répertoires entiers (y compris des sous-répertoires), des types de fichiers particuliers (identifiés par leur extension de fichier) et des fichiers individuels (identifiés par leur nom de fichier entier ou partiel).

Lorsque vous générez des règles de chiffrement individuelles, le système affiche toutes les clés présentes dans le groupe. Le responsable de la sécurité de conpal LAN Crypt peut alors assigner les clés appropriées pour définir quelles données seront accessibles à un utilisateur.

Les règles de chiffrement sont toujours générées par groupe. Elles comprennent un chemin et une clé et sont créées dans le nœud **Règles et balises de chiffrement**. Il est facile de générer une règle de chiffrement parce que vous entrez les détails du chemin, choisissez une clé et sélectionnez les différentes options dans la même boîte de dialogue.

Les règles de chiffrement sont toujours héritées par les groupes subordonnés.

Remarque : ne définissez pas de règle de chiffrement pour le dossier "Fichiers Internet temporaires".

3.16.1 Chemins de chiffrement

Les chemins de chiffrement définissent quelles données doivent être chiffrées. Vous les définissez dans le nœud **Règles et balises de chiffrement** *en dessous du nœud du groupe concerné*. Ils s'appliquent alors à tous les utilisateurs présents dans ce groupe.

Remarque : les chemins vers les fichiers .zip ou les dossiers compressés ne peuvent pas être utilisés comme chemins de chiffrement.

Chemins relatifs :

conpal LAN Crypt accepte les définitions de chemin relatif. Une définition de chemin relatif indique un chemin vers un répertoire ou un fichier qui n'identifie pas le lecteur de disque

concerné, ou le répertoire du niveau hiérarchique supérieur suivant. Si vous sélectionnez une définition de chemin relatif, le système chiffrera chaque répertoire correspondant à la définition du chemin.

Vous pouvez utiliser les chemins relatifs de deux manières :

- **Entrée :** `\mes_données\*.*`
  chiffre tout répertoire `mes_données` des répertoires RACINE.

  EXEMPLE

  `C:\mes_données\*.*`

  `D:\mes_données\*.*`

  `Z:\mes_données\*.*`

- **Entrée :** `mes_données\*.*`
  chiffre **TOUS LES** répertoires `mes_données`.

  EXEMPLE

  `C:\société\mes_données\*.*`

  `Z:\Départements\développement\Equipe1\mes_données\*.*`

Dans les deux cas, tous les fichiers du répertoire `mes_données` sont chiffrés.

Si un chemin de répertoire commence par une barre oblique inverse, la définition du chemin relatif s'appliquera uniquement aux répertoires de la racine.

%USERNAME%

conpal LAN Crypt accepte l'utilisation de la variable d'environnement %NOMUTILISATEUR% dans les définitions de chemin.
La variable d'environnement locale %NOMUTILISATEUR% dans une définition de chemin est résolue automatiquement par conpal LAN Crypt. Si vous voulez résoudre d'autres variables d'environnement, vous devez l'indiquer dans la configuration de conpal LAN Crypt (voir le chapitre Résoudre toutes les variables d'environnement).

Répertoire par défaut

Pour faciliter le chiffrement de dossiers spécifiques à l'utilisateur, conpal LAN Crypt prend en charge les répertoires par défaut prédéfinis par Windows (par exemple, Mes Documents, Fichiers communs, etc.). Le responsable de la sécurité ne doit donc pas considérer les variations spécifiques au système dans la configuration du client. conpal LAN Crypt détermine le chemin spécifique à l'utilisateur correct dans la langue correcte depuis le répertoire par défaut correspondant et chiffre les fichiers stockés dans ce répertoire.

Pour spécifier d'autres répertoires dans LAN Crypt, saisissez l'identifiant correspondant.
Exemple :
<0x002f>*.*

Il s'agit du répertoire qui contient les outils d'administration pour tous les utilisateurs de l'ordinateur (CSIDL_COMMON_ADMINTOOLS).

Pour une liste de tous les identifiants possibles, reportez-vous aux documents suivants : *http://msdn2.microsoft.com/en-us/library/ms649274.aspx*

3.16.2 Clés

Vous créez les clés servant à chiffrer les données avant de générer les règles de chiffrement. Toutes les clés disponibles pour le groupe concerné sont affichées dans la boîte de dialogue dans laquelle vous créez une règle de chiffrement et vous pourrez les sélectionner dans cette liste.

3.16.3 Séquence des règles de chiffrement

Lorsque vous chargez les fichiers de stratégie dans le client, conpal LAN Crypt trie les règles de chiffrement en fonction de la méthode que vous avez sélectionnée dans l'onglet Résolution des règles des Paramètres centraux :

- Méthode de tri 1
  1. Règles d'ignorance
  2. Règles d'exclusion
  3. Règles de chiffrement

- Méthode de tri 2
  1. Règles d'ignorance
  2. Règles d'exclusion
  3. Règles de chiffrement spécifiées comme chemins absolus sans caractères génériques
  4. Règles de chiffrement spécifiées comme chemins absolus avec caractères génériques n'incluant pas les sous-dossiers
  5. Règles de chiffrement spécifiées comme chemins absolus avec caractères génériques incluant les sous-dossiers
  6. Toutes les autres règles de chiffrement

  Un chemin absolu est un chemin UNC (commençant par une double barre oblique inverse) ou <lettre de lecteur>:\
  Par exemple : \\serveur\partage*.* ou c:\chiffrer*.*.

- Méthode de tri 3 (par défaut)
  La méthode de tri 3 ne fait pas de distinction entre les règles d'ignorance, d'exclusion et de chiffrement.
  Les règles sont triées dans l'ordre suivant :
  1. Tous les chemins absolus sans caractères génériques
  2. Tous les chemins absolus avec caractères génériques n'incluant pas les sous-dossiers
  3. Tous les chemins absolus avec caractères génériques incluant les sous-dossiers
  4. Toutes les autres règles

Un chemin absolu est un chemin UNC (commençant par une double barre oblique inverse) ou <lettre de lecteur>:\"
Par exemple : \\serveur\partage*.* ou c:\chiffrer*.*.

Dans l'une des sections ci-dessus (par exemple : Méthode de tri 3 - Toutes les autres règles), les règles sont ordonnées en fonction de la précision de la définition du chemin.

L'ordre et le suivant :
1. Chemins UNC
2. Chemins commençant par <lettre du lecteur>: La barre oblique inverse après la lettre de lecteur n'est ici pas considérée.
2. Tous les autres chemins
En outre :
- Les chemins comportant davantage de barres obliques inverses apparaissent avant ceux en comportant moins
- Les chemins sans caractères joker apparaissent avant les chemins avec les caractères joker *. et *.*

3.16.4 Génération des règles de chiffrement

1. Cliquez avec le bouton droit de la souris sur **Règles et balises de chiffrement** en dessous du nœud de groupe correspondant et cliquez sur **Nouvelle** règl**e de chiffrement** dans le menu contextuel.
   Vous pouvez également accéder à la commande **Nouvelle** règl**e de chiffrement** dans un menu contextuel que vous affichez par un clic droit sur le volet droit de la console. Celui-ci affiche toutes les règles de chiffrement qui ont été générées.

2. Entrez un chemin relatif ou absolu dans le champ de saisie en dessous de *Chemin de chiffrement*.
   Vous pouvez utiliser des caractères génériques (`?`) ou (`*`) dans les noms de fichiers (mais pas dans le reste du chemin) (par exemple, *.doc). Cliquez sur le bouton **Parcourir** ("…") pour sélectionner un chemin.

Programmes prenant en charge des spécifications de fichier ou de chemin en notation 8.3 uniquement
Si vous utilisez des programmes qui prennent uniquement en charge des spécifications de fichier ou de chemin en notation 8.3 et que vous souhaitez accéder à des fichiers chiffrés dont le nom contient plus de 8 caractères ou à des fichiers dans des répertoires dont le nom contient plus de 8 caractères, vous devez utiliser la notation 8.3 pour nommer les règles de chiffrement.
En outre, vous devez définir ces règles de chiffrement. Sinon, les programmes à 32 bits ne fonctionneront plus.
Employez la commande `dir /x` pour afficher le nom 8.3 correct des noms de fichiers longs.

3. Trois options apparaissent sous *Chemin de chiffrement*:

- Inclure sous-répertoires
- Exclure ce chemin
- Ignorer ce chemin

Inclure sous-répertoires

Les sous-répertoires ne sont pas inclus dans les règles de chiffrement sauf mention contraire. Pour inclure tous les sous-répertoires dans le chiffrement, cochez l'option **Inclure sous-répertoires**.

Exemple

Entrée : `mes_données\*.* Inclure sous-répertoires`

Cette règle de chiffrement chiffre tous les fichiers contenus dans

```
C:\société\mes_données
C:\société\mes_données\projet NT
C:\société\mes_données\projet 2000\demo
```

Exclure ce chemin

Vous devez définir ici une règle de chiffrement excluant ces données du chiffrement. Pour ce faire, cochez l'option **Exclure ce chemin** dans la boîte de dialogue *Chiffrement des fichiers*. Par conséquent, les fichiers désignés dans la règle de chiffrement ne seront pas chiffrés. Par défaut, cette option n'est pas activée.

Exemple

Tous les fichiers avec l'extension `.TXT` doivent être exclus du chiffrement.

Première ligne :

L'entrée `C:\MYDIR\*.TXT` avec l'option **Exclure ce chemin** sans clé, exclut du chiffrement tous les fichiers avec l'extension `.TXT` du répertoire `MYDIR`.

Deuxième ligne :

l'entrée `C:\MYDIR\*.*`, avec l'option **Exclure ce chemin** non cochée, chiffre tous les fichiers contenus dans `MYDIR` (à l'exception du fichier `.TXT`) avec la clé spécifiée.

Ignorer ce chemin

conpal LAN Crypt comprend l'option **Ignorer ce chemin**. conpal LAN Crypt ignore simplement les fichiers concernés par ce type de règle de chiffrement.

Au contraire de l'option **Exclure ce chemin**, cela signifie également qu'il n'existe pas de contrôle d'accès à ces fichiers. Vous pouvez les ouvrir (le contenu chiffré est affiché), les déplacer, les supprimer, etc. Néanmoins, le système vérifie les fichiers dans les répertoires qui sont exclus du chiffrement pour contrôler s'ils sont effectivement chiffrés ou non. conpal LAN Crypt peut

ainsi détecter si les fichiers dans les répertoires de ce type sont chiffrés ou non. Vous ne pouvez pas accéder aux données chiffrées. conpal LAN Crypt ignore simplement les fichiers dans les répertoires pour lesquels l'option **Ignorer ce chemin** a été cochée ! conpal LAN Crypt ne les vérifie pas et les utilisateurs peuvent accéder aux fichiers chiffrés.

Cette option est généralement activée pour les fichiers d'un accès très fréquent et ne nécessitant pas de chiffrement. Elle accroît les performances du système.

4. Sélectionnez une clé dans la liste.

Remarque : dans la vue par défaut, les paramètres fictifs pour <USERKEY> et <GROUPKEY>, ainsi que les clés créées par un responsable de la sécurité s'affichent. Avec le bouton Clé spécifique, vous pouvez rechercher et afficher les clés spécifiques.

Le chemin de chiffrement et la clé forment une règle de chiffrement conpal LAN Crypt. Les règles de chiffrement que vous définissez pour l'utilisateur/groupe au total forment le profil de chiffrement de l'utilisateur/du groupe.

<USERKEY>

Une clé <USERKEY> est toujours insérée dans la liste des clés. Il s'agit d'un paramètre fictif pour une clé spécifique à un utilisateur que le système génère automatiquement pour chaque utilisateur lorsqu'il établit les règles de chiffrement.

<GROUPKEY>

Vous pouvez utiliser <GROUPKEY>, de la même façon que <USERKEY>, pour générer une clé commune à tous les membres d'un groupe.

Remarque : lorsque vous utilisez <USERKEY>, assurez-vous que l'accès aux données est réservé exclusivement à l'utilisateur auquel cette clé a été assignée. Les autres utilisateurs ne peuvent pas déchiffrer ces données !

Exemple : Exemple d'utilisation de <USERKEY> : tous les utilisateurs travaillent sur le même lecteur de réseau, U:, qui contient un répertoire par utilisateur. Seul l'utilisateur approprié doit pouvoir accéder à ce répertoire.
Une règle de chiffrement utilisée pour spécifier ceci pourrait ressembler à ceci :
`U:\*.* <USERKEY>`
Un autre exemple consisterait à utiliser <USERKEY> pour chiffrer des répertoires temporaires locaux.

Assigner une clé sans chemin

La liste des chemins de chiffrement définis contient un espace réservé appelé *Assigner une clé sans chemin*.
Il permet de donner aux utilisateurs une clé servant pour les données chiffrées sans chemin de chiffrement. Cela peut se produire lorsque des fichiers chiffrés sont copiés dans un emplacement

pour lequel aucune règle de chiffrement n'a été définie (avec chiffrement désactivé). Ils peuvent alors utiliser cette clé pour accéder aux fichiers avec la clé appropriée.
Si une clé est créée sans chemin, le système génère automatiquement un nouveau paramètre fictif pour autoriser la génération d'autres clés sans chemin.

5. Sélectionnez les options nécessaires.
6. Sous *Commentaire*, saisissez une description ou des informations sur la règle de chiffrement créée.
7. Cliquez sur **OK**.

La nouvelle règle de chiffrement s'affiche dans conpal LAN Crypt Administration.

Pour modifier les clés de chiffrement existantes, sélectionnez-les, puis cliquez sur **Propriétés** dans le *menu contextuel*. Vous pouvez également cliquer deux fois sur l'entrée correspondante.

3.16.5 Rechercher une clé spécifique

Appuyez sur le bouton Clé spécifique pour lancer un assistant de recherche de clés spécifiques. Une clé sélectionnée dans l'assistant sera ajoutée à la liste des clés et pourra être utilisée pour les règles de chiffrement. La clé est seulement ajoutée temporairement. Si l'assistant est de nouveau exécuté et une clé différente est sélectionnée, la clé précédemment ajoutée sera retirée de la liste.

Sur la première page, vous pouvez définir des critères de recherche. Les critères suivants peuvent être sélectionnés dans la liste déroulante :

- **Clé attribuée à un utilisateur**
  Recherche toutes les clés spécifiques assignées à un utilisateur. Saisissez le nom d'utilisateur ou le nom de connexion dans le champ d'édition (condition de recherche). Pour effectuer une recherche par caractère générique, vous pouvez utiliser les caractères génériques SQL. Par exemple, "Utilisateur Jean Aymar 1%" retrouve toutes les clés assignées aux utilisateurs dont les noms ou les noms de connexion commencent par "Jean Aymar 1").
- **Clé attribuée à un groupe**
  Recherche toutes les clés spécifiques qui sont assignées à un groupe. Saisissez le nom du groupe.
- **Nom de la clé**
  Recherche toutes les clés spécifiques assignées portant un nom donné. Saisissez le nom long ou court de la clé.
- **GUID de la clé**
  Recherche toutes les clés spécifiques avec un GUID donné. Saisissez le GUID de la clé.
- **Clés actuellement non attribuées**
  Affiche toutes les clés actuellement non assignées à un utilisateur ou à un groupe.

Le résultat de la recherche apparaît sur la seconde page

Si une clé est actuellement assignée, le nom d'utilisateur ou de groupe apparaît sous Assignée à. La liste contient seulement des clés spécifiques, même si les clés non spécifiques correspondent aux critères de recherche.

Sélectionnez une clé et cliquez sur Terminer pour ajouter la clé à la liste de la boîte de dialogue de création des règles de chiffrement.

3.17 Balises de chiffrement

Si un produit de prévention des fuites de données (DLP ou Data Leakage Prevention) identifie des données nécessitant une opération de chiffrement, il utilise l'API de conpal LAN Crypt Client pour chiffrer ces fichiers. Dans conpal LAN Crypt Administration, vous pouvez définir différentes balises de chiffrement qui indiqueront la clé conpal LAN Crypt à utiliser.

L'API Client utiliser des balises de chiffrement prédéfinies afin d'appliquer des clés spéciales selon le contenu. Par exemple, la balise de chiffrement <CONFIDENTIEL> est utilisée pour chiffrer tous les fichiers que votre produit DLP considère comme étant confidentiels.

Par exemple :

```
SGFEAPI encrypt /Balise:CONFIDENTIEL c:\documents\encrypt.doc
```

chiffre le fichier encrypt.doc dans le dossier \documents à l'aide de la clé associée à la balise <CONFIDENTIEL>.

Retrouvez plus de renseignements dans la documentation Client API dans le dossier \DOC de votre package d'installation décompressé.

Pour générer une balise de chiffrement :

1. Cliquez avec le bouton droit de la souris sur **Règles et balises de chiffrement** en dessous du nœud de groupe correspondant et cliquez sur **Nouvelle** balise**de chiffrement** dans le menu contextuel.
   Vous pouvez également accéder à la commande **Nouvelle** balise**de chiffrement** dans un menu contextuel que vous affichez par un clic droit sur le volet droit de la console. Celui-ci affiche toutes les règles de chiffrement qui ont été générées.

2. Nommez la balise de chiffrement dans le champ de saisie en dessous de *Balise de chiffrement*.

3. Sélectionnez une clé.

Remarque : dans la vue par défaut, les paramètres fictifs pour <USERKEY> et <GROUPKEY>, ainsi que les clés créées par un responsable de la sécurité s'affichent. Avec le bouton Clé spécifique, vous pouvez rechercher et afficher les clés spécifiques.

<USERKEY>

Une clé <USERKEY> est toujours insérée dans la liste des clés. Il s'agit d'un paramètre fictif pour une clé spécifique à un utilisateur que le système génère automatiquement pour chaque utilisateur lorsqu'il établit les règles de chiffrement.

<GROUPKEY>

Vous pouvez utiliser <GROUPKEY>, de la même façon que <USERKEY>, pour générer une clé commune à tous les membres d'un groupe.

Remarque : lorsque vous utilisez <USERKEY>, assurez-vous que l'accès aux données est réservé exclusivement à l'utilisateur auquel cette clé a été assignée. Les autres utilisateurs ne peuvent pas déchiffrer ces données !

4. Sous Commentaire, saisissez une description ou des informations sur la balise de chiffrement créée.

5. Cliquez sur OK.

La nouvelle balise de chiffrement s'affiche dans conpal LAN Crypt Administration.

Pour modifier les balises de chiffrement existantes, sélectionnez-les, puis cliquez sur Propriétés dans le menu contextuel. Vous pouvez également cliquer deux fois sur l'entrée correspondante.

3.18 Assignation de certificats

Chaque profil est protégé par la clé publique de son propriétaire. Cette clé publique doit être assignée à l'utilisateur dans conpal LAN Crypt Administration via son certificat.

Remarque : vous n'avez pas besoin de réaliser cette étape dans la séquence décrite ci-dessous. Vous pouvez également la réaliser avant.

Nous vous recommandons de vérifier que les certificats sont déjà disponibles et prêts à être utilisés dans le magasin de certificats ou dans un annuaire (par exemple, LDAP) avant de commencer à les assigner. Vous pouvez employer les outils standard Windows pour importer les certificats dans le magasin de certificats concerné.

conpal LAN Crypt intègre un assistant effectuant automatiquement l'assignation des certificats.

Remarque : si un utilisateur Windows qui assigne un certificat ne détient pas le droit de modifier le fichier journal des mots de passe dans le système de fichiers, il sera impossible de générer des certificats conpal LAN Crypt.

3.18.1 Assignation d'un certificat à un utilisateur

Pour assigner un certificat :

1. Sélectionnez **Membres et certificats du groupe** dans le noeud du groupe correspondant.
   La liste de tous les utilisateurs est affichée dans le volet droit de la console.

2. Cliquez deux fois sur un utilisateur ou cliquez avec le bouton droit sur l'utilisateur puis sur **Propriétés** dans le menu contextuel.
   La boîte de dialogue *Propriétés* s'affiche.

3. Vous pouvez y sélectionner une des options suivantes pour assigner un ou plusieurs certificats à l'utilisateur.

- **Nouveau**
  Cliquez sur **Nouveau** si vous souhaitez que conpal LAN Crypt génère un nouveau certificat pour l'utilisateur.
  Si aucun certificat n'est disponible, conpal LAN Crypt Administration peut générer lui-même des certificats. Toutefois, seulement conpal LAN Crypt devrait utiliser ces certificats ! Le certificat ainsi généré est enregistré sous forme de fichier PKCS#12 dans le répertoire par défaut.

Remarque : tout certificat généré de cette manière doit être distribué à l'utilisateur concerné. Sinon, l'utilisateur ne sera pas en mesure d'accéder à son profil de chiffrement.

- **Importer …**
  Si le certificat recherché n'est pas présent dans le magasin de certificats, il n'apparaîtra pas dans la liste des certificats disponibles.
  Dans ce cas, cliquez sur **Importer …** Le système ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner le certificat nécessaire. Puis cliquez sur **OK** et le système assigne le certificat à l'utilisateur.
  Le certificat est automatiquement importé dans le magasin de certificats appelé *Autres personnes*.

Remarque : seuls les fichiers de certificats ayant le format .cer, .crt ou .der peuvent être importés. L'importation des fichiers .p12 ou .pfx est impossible.

- **Ajouter …**

Ouvre une boîte de dialogue dans laquelle vous assignez un certificat existant à un utilisateur. Cette boîte de dialogue affiche la liste de tous les certificats présents dans le magasin de certificats.
Assignation de certificats à l'aide d'une source LDAP
conpal LAN Crypt vous autorise à assigner des certificats à partir d'une source LDAP.

Pour ce faire, sélectionnez **LDAP** dans la liste déroulante de la boîte de dialogue *Sélectionner un certificat*.

Dans le champ d'édition qui apparaît, vous pouvez entrer l'URL de la source LDAP. Après avoir cliqué sur **Actualiser**, le contenu de la source LDAP s'affiche.
Les termes entre crochets (par exemple, Sub_OU_1]) correspond aux unités organisationnelles (OU) dans la source LDAP. Pour afficher les certificats d'une OU, cliquez simplement deux fois dessus.
Cliquez deux fois sur [**..**] pour remonter d'un niveau hiérarchique.
Sélectionnez un certificat et cliquez sur **OK**. Le certificat est maintenant assigné au responsable de la sécurité.

Remarque : si le serveur LDAP n'autorise aucune connexion anonyme, les informations d'identification destinées au serveur doivent être entrées sous forme de nom unique (exemple : CN= Jean Bouvier,O=Marketing) dans l'onglet **Serveur** des **Paramètres centraux**.

Remarque : si vous avez un certificat assigné à partir d'un annuaire LDAP, la clé privée associée au certificat doit être disponible sur le poste de l'utilisateur.

4. Employez une des options décrites pour sélectionner un certificat, puis cliquez sur **OK**.
   Le système affiche le certificat dans le volet de la console, à droite à côté de l'utilisateur. Dans ce volet, le système affiche les informations sur le certificat utilisé (période de validité, numéro de série, émetteur).

Remarque : le composant logiciel enfichable Certificat est disponible sous chaque nœud d'utilisateur/de groupe. Le système affiche uniquement les utilisateurs membres du groupe concerné.

3.18.2Génération et assignation de certificats conpal LAN Crypt

Vous utilisez cet assistant pour générer des certificats destinés à **tous** les utilisateurs pour lesquels aucun certificat n'a encore été assigné, puis pour assigner automatiquement ces certificats à ces utilisateurs.

Pour lancer cet assistant, cliquez sur **Générer des certificats** dans le menu contextuel de chaque nœud *Membres et certificats pour le groupe* ou sur l'icône correspondante dans la barre d'outils.

Dans la boîte de dialogue suivante, indiquez si vous générez et assignez des certificats **pour ce groupe uniquement**, **pour ce groupe et tous ses sous-groupes** ou **réservé aux utilisateurs sélectionnés**.

Réservé aux utilisateurs sélectionnés

Cette option s'affiche uniquement si un ou plusieurs utilisateurs sont sélectionnés. Lorsque vous cliquez sur *Membres et certificats pour le groupe* sous le nœud de groupe désiré, dans le volet

gauche de la console, les membres du groupe sont affichés dans le volet droit de la console. La sélection des utilisateurs s'opère comme dans l'Explorateur Windows (en cliquant sur le bouton gauche de la souris tout en appuyant sur la touche MAJ ou Ctrl).

Le système génère et crée les certificats automatiquement. Cliquez sur **Terminer** pour fermer l'assistant.

Remarque : les fichiers de clés (.p12) générés ici et la partie publique du certificat du responsable de la sécurité sont enregistrés dans le répertoire désigné dans les paramètres centraux et doivent être mis à la disposition des utilisateurs.
Pour établir cette configuration, désignez le dossier dans lequel conpal LAN Crypt doit rechercher un fichier.p12 pour l'utilisateur si la clé privée du fichier de stratégie n'est pas présente. La même procédure s'applique à la partie publique du certificat du responsable de la sécurité. Le nom des fichiers doit correspondre au nom de connexion des utilisateurs (`"Connexion*.p12"`) de sorte que conpal LAN Crypt puisse automatiquement reconnaître les fichiers de clés des utilisateurs.
Lorsque conpal LAN Crypt trouve le fichier correspondant, il affiche une boîte de dialogue avec les codes PIN. Vous devez envoyer à l'utilisateur un courrier d'information sur son code PIN (contenu dans le fichier journal des mots de passe). Le certificat et la clé associée sont automatiquement importés après la saisie du code par l'utilisateur.

Si conpal LAN Crypt trouve un fichier .cer contenant la partie publique du certificat du responsable de la sécurité, il l'importe automatiquement.
Vous pouvez aussi distribuer manuellement les fichiers de clés des utilisateurs et la partie publique du certificat de l'administrateur. Dans ce cas, assurez-vous que les clients importent les deux.

3.18.3 Assistant d'assignation de certificats

conpal LAN Crypt intègre un assistant effectuant la plupart des tâches relatives à l'assignation de certificats aux utilisateurs. Pour lancer l'assistant, sélectionnez **Assistant d'assignation de certificats** dans le menu contextuel pour les *Membres et certificats pour le groupe*.

Dans la première étape de l'assistant, indiquez si vous assignez des certificats aux membres **uniquement dans ce groupe**, **de ce groupe et de tous les sous-groupes** ou **uniquement pour les utilisateurs sélectionnés**.

Réservé aux utilisateurs sélectionnés

Cette option s'affiche uniquement si un ou plusieurs utilisateurs sont sélectionnés. Lorsque vous cliquez sur *Membres et certificats pour le groupe* sous le nœud de groupe désiré, dans le volet gauche de la console, les membres du groupe sont affichés dans le volet droit de la console. La sélection des utilisateurs s'opère comme dans l'Explorateur Windows (en cliquant sur le bouton gauche de la souris tout en appuyant sur la touche MAJ ou Ctrl).

L'assistant prend en charge l'affectation des certificats provenant des sources suivantes :

- Assigner les certificats à partir de **Active Directory**
- Assigner les certificats à partir d'un **annuaire LDAP**
- Assigner les **certificats à partir d'un répertoire du système de fichiers**
- Assigner les **certificats à partir de la mémoire de certificats**

3.18.3.1 Assignation des certificats à partir de Active Directory

Pour sélectionner l'option Assigner les certificats à partir de **Active Directory**, entrez l'adresse DNS du serveur Active Directory au cours de la deuxième étape de l'assistant. Il s'agit généralement du contrôleur de domaine.

Si vous cliquez sur **Utiliser valeurs par défaut**, le système appliquera l'adresse du contrôleur de domaine auquel vous êtes actuellement connecté.

Pour lancer l'assistant, cliquez sur **Suivant**. Le système importe et assigne les certificats automatiquement. Il affiche un message pour confirmer que l'assignation des certificats a réussi. Cliquez sur **Terminer** pour fermer l'assistant.

3.18.3.2 Assigner des certificats à partir d'un annuaire LDAP

Si vous sélectionnez l'option **Assigner les certificats à partir d'un annuaire LDAP**, vous devrez entrer l'adresse de l'annuaire LDAP à partir duquel vous voulez importer les certificats, au cours de la deuxième étape de l'assistant.

Dans le champ *Adresse*, entrez le nom complet de l'ordinateur du serveur LDAP (par exemple : Server.MyDomain.com) et désignez le port concerné. Le port standard du serveur LDAP est paramétré par défaut.

Dans le DN (nom absolu), entrez le nœud dans l'arborescence LDAP à partir duquel le système lancera la recherche dans l'annuaire. Entrez le nœud dans l'annuaire LDAP à l'aide de son nom absolu (DN). Vous ne devez pas entrer de nouveau le nom de l'ordinateur (dc=nomordinateur...) ici.

Remarque :
Microsoft AD :
Le champ de saisie ne doit pas rester vide. Vous devez entrer au moins ici le domaine et le pays.
Exemple 1 : DC=mondomaine,DC=De
Exemple 2 : OU=marketing,DC=mondomaine,DC=DE

Si vous cliquez sur **Utiliser valeurs par défaut**, le système appliquera l'adresse du contrôleur de domaine auquel vous êtes actuellement connecté.

Pour assigner les certificats, le système établit une concordance entre les propriétés de l'utilisateur LDAP et celles de l'utilisateur conpal LAN Crypt.

Vous pouvez utiliser les propriétés suivantes de l'utilisateur LDAP :

- l'adresse de messagerie ;
- le nom courant ;
- le nom complet ;
- le nom de compte NT 4.0 ;
- le nom principal utilisateur.
- l'attribut défini par l'utilisateur.

Vous pouvez indiquer que ces propriétés concordent avec les propriétés suivantes de l'utilisateur conpal LAN Crypt :

- l'adresse de messagerie ;
- le nom d'utilisateur ;
- le nom de connexion.
- Commentaire

Sélectionnez la propriété de l'utilisateur LDAP que vous voulez faire concorder avec chaque propriété de l'utilisateur conpal LAN Crypt.
En cas de concordance, le système importe le certificat de l'utilisateur LDAP et l'assigne automatiquement à l'utilisateur approprié de conpal LAN Crypt.

Remarque : pour éviter les incohérences, nous vous recommandons d'utiliser l'adresse de messagerie comme critère d'assignation car elle est toujours unique.

Pour lancer l'assistant, cliquez sur **Suivant**. Le système importe et assigne les certificats automatiquement. Il affiche un message pour confirmer que l'assignation des certificats a réussi. Cliquez sur **Terminer** pour fermer l'assistant.

3.18.3.3 Assigner les certificats à partir d'un répertoire

Si vous sélectionnez l'option **Assigner les certificats à partir d'un répertoire**, vous devrez entrer l'adresse du répertoire à partir duquel vous voulez importer les certificats, pendant la deuxième étape de l'assistant.

Après avoir indiqué le répertoire, une boîte de dialogue apparaît afin que vous définissiez la méthode qu'utilisera conpal LAN Crypt pour assigner les certificats aux utilisateurs.

- **Nom d'utilisateur identique à nom de fichier**
  Sélectionnez cette option si les noms de fichiers du certificat sont identiques au nom d'utilisateur.

Tous les utilisateurs qui correspondent à un nom de fichier sont assignés au certificat approprié.

- **Nom d'utilisateur dans DN**
  Si le nom d'utilisateur est contenu dans le nom absolu du certificat, conpal LAN Crypt le trouvera et assignera le certificat à l'utilisateur approprié. conpal LAN Crypt utilise un mode de recherche pour identifier le nom d'utilisateur dans le DN.
  Vous pouvez spécifier ce motif de recherche dans le champ de saisie sous l'option **Nom d'utilisateur dans DN**. Le système recherche le nom d'utilisateur tel qu'il apparaît entre les deux chaînes de caractères spécifiées dans le DN.
  Exemple :
  Dans le certificat, le nom d'utilisateur est toujours présent sous CN=.
  (par exemple, CN=JBouvier,OU=conpal LAN Crypt)
  Si vous entrez `CN=` dans le premier champ de saisie et `,OU=conpal` dans le second champ de saisie, conpal LAN Crypt trouvera le nom d'utilisateur placé entre ces deux chaînes de caractères (dans notre exemple : JBouvier). Le certificat est automatiquement assigné à l'utilisateur.

- **Coupler comme spécifié dans un fichier**
  Vous pouvez également chercher l'assignation requise dans un fichier.
  Par exemple, la partie publique du certificat généré avec conpal Smartcard Administration est enregistrée dans un fichier d'un répertoire prédéfini. conpal Smartcard Administration utilise ces fichiers pour générer un fichier qui enregistre quel certificat est assigné à chaque utilisateur.
  D'autres PKI peuvent également générer des listes de ce type. Cette liste peut évidemment se générer d'elle-même.

  Elle doit avoir le format suivant :
  ```
  Nom d'utilisateur;nom de fichier
  ```
  Exemple :
  ```
  Guest;Guestcer.cer
  HansMeier;Meier.cer
  ....
  ```
  Le système assigne les certificats en fonction de l'assignation dans ce fichier.

- Cliquez sur **Suivant** pour lancer l'assistant et assigner automatiquement les certificats.

3.18.3.4 Assignation des certificats à partir de la mémoire de certificats

Si vous avez sélectionné l'option **Assigner les certificats à partir des magasins de certificats**, la deuxième étape de l'assistant vous invitera à indiquer s'il faut générer une liste de tous les certificats disponibles et les importer ou importer une liste existante. conpal LAN Crypt utilise cette liste pour assigner les certificats.

Par exemple, vous pouvez utiliser l'option "Importer une liste précédemment créée" si l'assignation a déjà été lancée une fois, mais a été interrompue après la génération de la liste. Le système peut utiliser de nouveau le fichier créé à cette occasion.

Si vous sélectionnez l'option **Créer et importer une liste de tous les certificats disponibles**, le système affiche cette boîte de dialogue.

Sélectionnez un nom de fichier de sortie pour la liste.

conpal LAN Crypt crée une liste de tous les certificats disponibles dans les magasins de certificats. Cette liste contient des paramètres fictifs pour les noms des utilisateurs auxquels le certificat doit être assigné.

Exemple :

*****; My; OU=conpal LAN Crypt Certificate, CN=LAN Crypt Admin; 0010-ae671e47...
*****; Root; CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com; 0010-4cad...

Les paramètres fictifs (*****) peuvent être remplacés par les noms des utilisateurs.

Si le certificat contient le nom de l'utilisateur, vous pouvez employer l'option suivante :

- **Essayer d'insérer des noms**
  conpal LAN Crypt essaie de reconnaître un utilisateur : si le nom absolu (DN) du certificat contient le nom d'utilisateur, conpal LAN Crypt pourra le trouver et assigner le certificat à l'utilisateur approprié. conpal LAN Crypt utilise un motif de recherche pour identifier le nom d'utilisateur dans le DN.
  Vous pouvez spécifier ce motif de recherche dans le champ de saisie sous l'option Nom d'utilisateur dans le DN. Le système recherche le nom de l'utilisateur tel qu'il est trouvé entre les deux chaînes de caractères spécifiées dans le DN.

  Exemple :

  Dans le certificat, le nom d'utilisateur est toujours présent sous CN=.
  (par exemple, CN=JBouvier,OU=conpal LAN Crypt)
  Si vous entrez `CN=` dans le premier champ de saisie et `,OU=conpal` dans le second champ de saisie, conpal LAN Crypt trouvera le nom d'utilisateur placé entre ces deux chaînes de caractères (dans notre exemple : JBouvier). Le système remplace le paramètre fictif par le nom d'utilisateur et assigne automatiquement le certificat à l'utilisateur.

- **Ouvrir le fichier de sortie pour édition avec le Bloc-notes à la fin de l'opération**
  Si cette option est sélectionnée, le système ouvrira la liste des certificats après sa génération. Vous pouvez maintenant modifier cette liste. Vous pouvez remplacer le paramètre fictif par le nom de l'utilisateur dans les certificats concernés. Lorsque vous enregistrez la liste, le système utilise la version modifiée pour assigner les certificats.

Cliquez sur **Suivant** pour lancer l'assistant et assigner automatiquement les certificats.

3.19 Fourniture des règles de chiffrement – génération des fichiers de stratégie

conpal LAN Crypt enregistre chaque profil généré (ou modifié) dans sa base de données Administration. Ces profils n'affectent pas encore les divers utilisateurs.

Pour résoudre les profils individuels et générer les fichiers de stratégie, un responsable de la sécurité conpal LAN Crypt doit lancer le résolveur de profils conpal LAN Crypt. Il génère des fichiers de stratégie pour chaque utilisateur en fonction des paramètres définis dans la console Administration. Le système charge le nouveau profil de chiffrement lors de la connexion suivante de l'utilisateur.

Remarque : vous devez toujours générer de nouveaux fichiers de stratégie après avoir modifié les paramètres dans conpal LAN Crypt Administration (ajout de nouvelles clés, de nouvelles règles, etc.). Les modifications sont prises en compte pour les utilisateurs dès qu'ils chargent les nouveaux fichiers de stratégie sur leurs postes.

3.19.1 Création (résolution) de fichiers de stratégie pour un groupe entier ou une sélection d'utilisateurs

Les fichiers de stratégie sont créés avec l'Assistant de compilation des profils. Si plusieurs utilisateurs sont sélectionnés et la création de profils est lancée depuis la barre d'outils ou depuis le menu contextuel des utilisateurs, l'assistant est lancé.

Si un utilisateur unique et l'option Préparer / Effacer un profil est sélectionnée dans le menu contextuel, le profil est créé immédiatement. Un message informe le responsable de la sécurité du résultat.

En fonction de l'affichage à partir duquel l'assistant est lancé, il y a différents points d'entrée pour l'assistant :

- **Sélection de l'étendue** (par défaut)
- **Collecte d'informations sur les utilisateurs et vérification des certificats :**
  Si aucune sélection d'étendue n'est possible ou autorisée, par exemple, si la création de profils est lancée pour les utilisateurs sélectionnés du nœud Utilisateurs et certificats sélectionnés.
- **Création de profils :**
  Si l'option Effacer le profil est démarrée pour plusieurs utilisateurs. Cette action ne peut pas être démarrée pour un groupe entier. Aucune vérification de certificat n'est nécessaire.

Sur la première page de l'assistant, vous pouvez sélectionner l'étendue pour la création de profils. Des profils peuvent être créés pour :

- les utilisateurs de ce groupe uniquement
- les utilisateurs de ce groupe et de tous les sous-groupes
- des utilisateurs sélectionnés seulement.

Activez l'option Résoudre les groupes modifiés uniquement pour restreindre la création de fichiers de stratégie aux utilisateurs pour lesquels de nouveaux fichiers de stratégie sont nécessaires suite aux modifications effectuées. La génération de fichiers de stratégie dans les grandes entreprises peut ainsi être accélérée.

Sur la deuxième page de l'assistant, la progression apparaît pendant que les données sont recueillies et les certificats d'utilisateurs vérifiés. Après que tous les utilisateurs ont été traités, la page suivante s'affiche.

Sur la troisième page de l'assistant, des avertissements de certificats s'affichent. Si les utilisateurs n'ont pas de certificat valide assigné ou si le certificat d'un utilisateur expire bientôt, les utilisateurs apparaissent sur cette page. Les avertissements et les erreurs de certificats suivants s'affichent :

- Le certificat de l'utilisateur va bientôt expirer (avertissement).
- Tous les certificats assignés de l'utilisateur ont expiré (erreur).
- Un utilisateur n'a pas de certificat assigné (erreur).
- L'utilisateur n'a pas de certificat assigné et est signalé pour être ignoré (avertissement).

En cas d'erreur, au moins une des options de cette page doit être sélectionnée avant que la création de profils ne puisse continuer :

- **Ne plus m'avertir à propos de utilisateurs de la liste**
  Ignore tous les utilisateurs dont les certificats ont expiré ou qui n'ont pas de certificats assignés. Ces utilisateurs sont ignorés lors de la création de profils jusqu'à ce que de nouveaux certificats leur soient assignés.
- **Ignorer toujours les utilisateurs sans certificat valide assigné**
  Ignore tous les utilisateurs sans certificat valide. Il s'agit d'un paramètre global qui peut aussi être configuré dans les Paramètres centraux.

Cliquez sur le bouton **Précédent**pour retourner à la page de sélection de l'étendue de l'assistant.

La quatrième page de l'assistant affiche une barre de progression lors de la création de tous les profils. L'assistant peut être annulé, mais cela ne fait qu'interrompre la création de profils. Les fichiers de stratégie qui ont été créés ne sont pas supprimés ou annulés.

La cinquième page de l'assistant et la dernière affichent le nombre de profils créés. Si une erreur s'est produite qui a forcé la création de profils à s'arrêter, un message d'erreur s'affiche.

Remarque : si vous apportez des modifications sur l'onglet Antivirus, l'onglet Résolution des règles ou l'onglet Autres paramètres dans Paramètre centraux, les fichiers de stratégie de tous les utilisateurs sont toujours modifiés. Après un changement de ce type, de nouveaux fichiers de stratégie pour tous les utilisateurs doivent être créés.

3.19.2 Fourniture via le composant logiciel enfichable Certificat

Vous pouvez également utiliser le composant Certificat pour fournir les fichiers de stratégie. Vous pouvez y accéder via le nœud *Membres et* certificats *pour le groupe* et via chaque nœud de groupe.

Si vous avez recours au composant enfichable Certificat pour générer les fichiers de stratégie, vous pourrez également utiliser les fonctions supplémentaires suivantes :

- Sélection des utilisateurs auxquels un certificat doit être assigné. Il n'est pas nécessaire de générer de nouveaux fichiers de stratégie pour tous les utilisateurs.
  Comme dans l'Explorateur Windows, vous pouvez sélectionner simultanément plusieurs utilisateurs (clic souris + appui sur touche MAJ ou Ctrl).
- Le responsable de la sécurité voit immédiatement quels utilisateurs sont présents dans le groupe.
- Le système affiche les icônes correspondant aux certificats en regard du nom d'utilisateur pour en préciser le statut.
  - **rouge**
    signifie que le certificat a expiré.
  - **jaune**
    signifie que le certificat approche du délai d'expiration configuré.
  - **vert**
    signifie que tout va bien.
  - l'icône grise **signifie :**
    soit qu'aucun certificat n'a été assigné à l'utilisateur, soit que cet utilisateur a été omis pendant l'assignation de certificats par le système.

Pour fournir les fichiers de stratégie, sélectionnez les utilisateurs nécessaires puis cliquez sur l'icône bleue en forme de roue dentée dans la barre d'outils ou sur **Préparer le profil** dans le menu contextuel de l'utilisateur sélectionné.

3.19.3 Effacement des profils

Vous pouvez utiliser le composant enfichable Certificat pour effacer les profils d'un ou de plusieurs utilisateurs. L'effacement d'un profil entraîne la génération d'un profil vide. L'utilisateur doit se connecter une fois à un fichier de stratégie vide pour remplacer les paramètres du fichier

de stratégie en cours enregistré dans la mémoire cache de la machine. Ensuite, il ne pourra plus accéder aux données chiffrées.

Pour effacer un profil, sélectionnez l'utilisateur dans le composant enfichable Certificat, puis cliquez sur l'icône **Effacer le profil pour l'utilisateur sélectionné** ou sur **Effacer le profil** dans le menu contextuel.

Vous pouvez sélectionner plusieurs utilisateurs (par un clic sur le bouton gauche de la souris tout en enfonçant la touche MAJ enfoncée), puis effacer leurs profils en cliquant sur l'icône .

Remarque : les paramètres définis dans les Paramètres centraux de conpal LAN Crypt déterminent la manière dont seront effacés les profils. La procédure de suppression des profils est similaire à celle de leur création. Si le nom Novell est utilisé (deux fichiers de stratégie sont créés), les deux profils seront supprimés si ce paramètre n'est pas modifié. Si ce paramètre est changé à l'exécution, il est possible que deux fichiers de stratégie aient été créés, seul celui portant le nom d'utilisateur Windows soit supprimé. Cela s'explique par le fait que l'option Créer des fichiers de stratégie supplémentaires selon le nom Novell a été désactivée et que seul le fichier de stratégie portant le nom d'utilisateur Windows est donc supprimé. Le fichier de stratégie Novell reste dans l'emplacement de stockage défini et en théorie peut être utilisé pour la connexion. Le système se comporte de la même façon quel que soit le format du fichier sélectionné pour les fichiers de stratégie (.po/.pol.biz/.xml.bz2). Dans ce cas, jusqu'à quatre fichiers de stratégie sont générés pour chaque utilisateur.
Si besoin, n'oubliez pas d'effectuer la coordination avec l'administrateur du système.

3.20 Journaux de la base de données

conpal LAN Crypt crée un journal des événements déclenchés par conpal LAN Crypt Administration dans la base de données de conpal LAN Crypt. La fonction de journalisation de conpal LAN Crypt vous permet d'indiquer quels événements doivent être enregistrés dans le journal, de les archiver et de vérifier les entrées.

Les droits globaux **Lire les entrées du journal** et **Gérer la journalisation** contrôlent le mode d'accès des responsables de la sécurité au module de journalisation. Le responsable principal de la sécurité peut accorder ces droits aux responsables de la sécurité.

Lire les entrées du journal	Le responsable de la sécurité peut voir les paramètres de journalisation ainsi que les événements.
Gérer la journalisation	Le responsable de la sécurité peut modifier les paramètres de journalisation. Il peut archiver, supprimer et vérifier les entrées.

Vous pouvez définir les paramètres de base de la fonction de journalisation dans conpal *LAN Crypt Administration* sous le nœud *Journalisation* de *Paramètres centraux*. Ce nœud est visible uniquement pour les responsables de la sécurité qui détiennent au moins le droit **Lire les entrées du journal**.

Seul un responsable principal de la sécurité peut effectuer ce paramétrage de base. Une sécurité supplémentaire peut être mise en place en ajoutant un deuxième niveau d'autorisation (scénario **Gérer la journalisation** nécessitant les autorisations globales **Lire les entrées du journal** et **Gérer la journalisation**).

Les paramètres de base indiquent également quels événements doivent être journalisés. Seul un responsable principal de la sécurité peut effectuer cette action.

Remarque : tout événement se produisant avant la connexion d'un responsable de la sécurité ne peut pas être journalisé directement dans la base de données. Ces événements seront mis dans la mémoire cache puis écrits dans la base de données lors de la prochaine tentative de connexion réussie.

3.20.1 Paramètres

Cliquez sur *Propriétés* dans le menu contextuel du nœud *Journalisation* pour afficher la fenêtre de configuration des paramètres de base.

Onglet Paramètres

Dans cet onglet, vous pouvez définir la période d'ancienneté des entrées des journaux pouvant être supprimées.

Avec une base de données distribuée, ce paramètre garantit la copie des entrées au niveau central avant leur suppression sur les sites individuels.

Onglet État

L'onglet *État* affiche les informations sur l'état actuel du module.

3.20.2 Événements journalisés

Si vous sélectionnez le nœud *Journalisation*, tous les événements pouvant être journalisés s'afficheront dans le volet droit de la console. Vous pouvez alors choisir quel événement doit être journalisé.

Remarque : seul le responsable principal de la sécurité peut sélectionner les événements à journaliser.

Cliquez sur l'intitulé de colonne *Niveau* pour trier les événements par catégorie (Urgence, Alerte, Erreur, Avertissement, Note, Information).

Pour sélectionner un événement à journaliser, cliquez deux fois sur celui-ci et cliquez sur l'icône correspondante dans la barre d'outils.

Active la journalisation des événements sélectionnés.

Désactive la journalisation des événements sélectionnés.

Vous pouvez sélectionner simultanément plusieurs événements (clic sur la souris + touche MAJ ou Ctrl).

Après avoir sélectionné les événements, cliquez sur l'icône en forme de disquette dans la barre d'outils pour enregistrer les paramètres. Néanmoins, le système vous demandera toujours si vous voulez conserver ou non les paramètres chaque fois que vous quitterez cet écran sans enregistrer les données.

3.20.3 Visualisation et exportation des entrées

Remarque : pour pouvoir visualiser et exporter les entrées, un responsable de la sécurité doit détenir l'autorisation globale **Lire les entrées du journal**.

Un responsable de la sécurité détenteur de l'autorisation globale "Lire les entrées du journal" peut afficher les entrées et les exporter dans un fichier.

Pour afficher les entrées, cliquez sur **Afficher et exporter les entrées** dans le menu contextuel du nœud *Journalisation* ou cliquez sur l'icône correspondante dans la barre d'outils.

Une boîte de dialogue apparaît. Vous pouvez afficher les entrées des journaux et les exporter.

Elle affiche tous les événements sélectionnés pour la journalisation.

Cliquez sur les en-têtes de colonnes pour trier les entrées.

Cliquez deux fois sur une entrée pour afficher ses détails.

conpal LAN Crypt possède également un filtre définissant les conditions d'affichage des entrées.

3.20.4 Filtrage des événements

Cliquez sur le bouton **Filtre** dans cette boîte de dialogue pour ouvrir une deuxième fenêtre dans laquelle vous définissez le filtre d'affichage des événements.

Vous pouvez filtrer les événements selon les contraintes suivantes :

- **Afficher uniquement les entrées d'un événement précis**

  Si vous sélectionnez cette option, seules les entrées de l'événement sélectionné dans la liste déroulante seront affichées. La liste contient tous les événements pouvant être journalisés.

- **Afficher uniquement les entrées d'un responsable de la sécurité précis**

  Si vous sélectionnez cette option, vous pouvez sélectionner un responsable de la sécurité dans la liste déroulante. L'affichage montrera seulement les événements qui ont été journalisés lorsque le responsable de la sécurité désigné était connecté. La liste déroulante contient seulement les responsables de la sécurité pour lesquels les entrées existent.

- **Afficher uniquement les entrées d'un niveau précis**

  Si vous sélectionnez cette option, vous pouvez sélectionner un niveau de sévérité donné ou une plage de sévérité pour lesquels les entrées doivent les entrées doivent être affichées.
  Inférieur ou égal à et *Supérieur ou égal à* fait référence au nombre avant le niveau de sévérité.

- **Afficher uniquement les entrées d'un intervalle de temps précis**

  Si vous sélectionnez cette option, vous pourrez définir un intervalle de temps pendant lequel les entrées ont été journalisées.

- **Afficher uniquement les entrées d'un état d'archive précis**

  Si vous sélectionnez cette option, vous pourrez définir si l'affichage inclut les **entrées archivées uniquement** ou les **entrées non encore archivées uniquement** (les entrées déjà archivées restent dans la base de données jusqu'à leur suppression). Si vous ne sélectionnez pas cette option, les deux types d'entrée seront affichés.

- **Afficher uniquement les entrées d'un emplacement précis**

  Sélectionnez cette option pour spécifier un emplacement à partir duquel les entrées doivent être affichées.
  Si vous utilisez une base de données distribuée, il peut y avoir plusieurs emplacements concernés. Le mode de réplication de la base de données détermine quels emplacements peuvent être affichés.

3.20.5 Archivage, suppression et vérification des entrées

Remarque : un responsable de la sécurité a besoin de l'autorisation globale **Gérer la journalisation** avant de pouvoir archiver, supprimer ou vérifier les entrées.

Un responsable de la sécurité détenant l'autorisation globale ***Gérer la journalisation*** peut archiver, supprimer ou vérifier les entrées des journaux.

Cliquez sur **Archiver, supprimer et vérifier les entrées** dans le menu contextuel du nœud *Journalisation* ou cliquez sur l'icône correspondante dans la barre de tâches pour lancer un assistant et mener à bien ces tâches.

Lance l'assistant permettant d'archiver, de supprimer et de vérifier les entrées journalisées.

Archivage des entrées

Pour archiver les entrées, cochez l'option **Archiver les entrées** puis cliquez sur **Suivant**.

Dans la boîte de dialogue suivante, entrez :

- Date et heure de la dernière entrée qui doit être archivée.
  Toutes les entrées à partir de ce moment jusqu'au moment présent seront archivées.
- L'emplacement (si disponible) où doivent être archivées les entrées.
- Le nom du fichier dans lequel seront écrites les entrées.

Cliquez sur **Suivant**. La boîte de dialogue suivante affiche le nombre d'entrées sélectionnées. Cliquez sur **Suivant**. Lorsque toutes les entrées ont été archivées, la dernière boîte de dialogue de l'assistant s'affiche. Cliquez sur **Terminer** pour fermer l'assistant.

Les entrées déjà archivées restent dans la base de données et peuvent être supprimées. Elles prennent l'état *Archivé*.

Suppression des entrées archivées

Pour supprimer les entrées archivées, sélectionnez *Supprimer les entrées* puis cliquez sur **Suivant**.

Dans la boîte de dialogue suivante, entrez :

- Date et heure de la dernière entrée qui doit être archivée.
  Toutes les entrées à partir de ce moment jusqu'au moment présent seront archivées.

Remarque : la dernière heure possible dépend de l'ancienneté minimale des entrées des journaux définie dans les paramètres de base.

- L'emplacement (si disponible) où doivent être supprimées les entrées.

Cliquez sur **Suivant**. La boîte de dialogue suivante affiche le nombre d'entrées sélectionnées. Cliquez sur **Suivant**. Lorsque toutes les entrées ont été supprimées, la dernière boîte de dialogue de l'assistant s'affiche. Cliquez sur **Terminer** pour fermer l'assistant.

Vérification de l'intégrité des archives

Pour vérifier l'intégrité des événements journalisés, sélectionnez *Vérifier l'intégrité des archives* puis cliquez sur **Suivant**.

Dans la boîte de dialogue suivante, sélectionnez les données que vous voulez vérifier. Vous pouvez sélectionner les entrées dans la base de données ou les entrées archivées.

Pour vérifier les entrées dans une base de données distribuée, sélectionnez les entrées de l'emplacement à vérifier.

Pour vérifier une archive, sélectionnez un fichier en cliquant sur le bouton **Parcourir ...**.

Cliquez sur **Suivant**. La boîte de dialogue suivante affiche le nombre d'entrées sélectionnées. Cliquez sur **Suivant**. Lorsque toutes les entrées ont été vérifiées, la dernière boîte de dialogue de l'assistant s'affiche. Le résultat du contrôle d'intégrité est affiché. Si les données ont été manipulées, vous en êtes averti par un message.

Cliquez sur **Terminer** pour fermer l'assistant.

4 Configuration de conpal LAN Crypt

Remarque : les paramètres de configuration doivent être définis avec le Group Policy Management Editor 32 bits ou le Local Group Policy Editor 32 bits. Si vous utilisez un système 64 bits, démarrez ces éditeurs en cliquant sur l'entrée respective sous Démarrer\Tous les programmes\Sophos\conpal LAN Crypt. Ceci permet de s'assurer que la version appropriée est lancée.

Les paramètres suivants sont spécifiques au poste ou à l'utilisateur. Pour les modifier, vous devez disposer de droits administratifs relatifs aux domaines ou à Active Directory. Ces paramètres doivent être définis uniquement par un administrateur système.

Sélectionnez les paramètres de configuration dans le nœud *Configuration LAN Crypt*. Ce nœud s'affiche lorsque vous travaillez avec des stratégies système dans le nœud utilisateur de la console de gestion de chacun des postes.

Dans l'environnement Active Directory, le nœud *Configuration LAN Crypt* se trouve dans le GPO, sous *Configuration ordinateur* ou sous *Configuration utilisateur/Paramètres Windows/conpal*.

Remarque : vous pouvez également choisir d'utiliser un modèle administratif fourni dans le dossier \config de votre package d'installation décompressé. Vous pouvez l'utiliser sur les ordinateurs sur lesquels conpal LAN Crypt Administration n'est pas installé.

Les paramètres de configuration sont généralement destinés aux machines. Toutefois, vous pouvez définir des paramètres spécifiques aux utilisateurs pour assigner des droits particuliers à des utilisateurs sélectionnés. Dans ce cas, les **paramètres spécifiques à l'utilisateur prévalent** sur les paramètres machine.

Pour annuler un paramètre utilisateur afin qu'un paramètre machine s'applique, vous devez définir le statut de ce paramètre sur *Non configuré*. Pour ce faire, sélectionnez un paramètre et appuyez sur la touche **Suppr**. Dans la console de gestion, **Non** s'affiche alors dans la colonne *Configuré*.

4.1 Paramètres client

Si le nœud *Paramètres client* est sélectionné, les paramètres configurables seront affichés dans le volet droit de la console. Cliquez deux fois sur une entrée pour ouvrir une boîte de dialogue dans laquelle vous pourrez procéder au paramétrage nécessaire.

4.1.1 Autoriser le chiffrement/déchiffrement

Tout utilisateur de conpal LAN Crypt peut chiffrer ou déchiffrer des fichiers en sélectionnant une option du menu contextuel de ces fichiers. Cela signifie que les utilisateurs peuvent même chiffrer des fichiers pour lesquels aucune règle n'a été définie.

Pour éviter cette action, vous pouvez décider ici que cette option ne doit pas être affichée dans le menu contextuel des fichiers.

Autoriser le chiffrement/déchiffrement : non
Évite le chiffrement ou le déchiffrement de fichiers, via leur menu contextuel, lorsqu'aucune règle de chiffrement n'a été définie.

4.1.2 Ignorer pendant la vérification du certificat

conpal LAN Crypt vous permet de spécifier s'il faut ignorer ou non les erreurs détectées en cours de vérification des certificats.

Cette procédure est utile si la période de validité d'un certificat a expiré et si aucun nouveau certificat n'est disponible. Pour permettre à un utilisateur de continuer à accéder à son profil de chiffrement, le contrôle de la période de validité peut être ignoré jusqu'à l'émission d'un nouveau certificat. Il en découle qu'il est encore possible d'utiliser le même certificat, effectivement parvenu à expiration. Dès qu'un nouveau certificat est disponible, vous pouvez désactiver l'option **Ignorer la durée d'invalidité**.

Remarque : le fait d'ignorer les erreurs pendant la vérification des certificats se traduit toujours par une réduction de la sécurité.

- **Ignorer le certificat révoqué**

  Si le certificat est sur une **L**iste des **C**ertificats **R**évoqués, qui est évaluée à la connexion, il se peut qu'il ne puisse être utilisé pour la connexion. Néanmoins, un utilisateur peut continuer à accéder à son profil de chiffrement même si cette option est activée.

- **Ignorer la durée d'invalidité**

  Même si la période de validité d'un certificat a expiré et que cette option est activée, l'utilisateur peut continuer à accéder à son profil de chiffrement.

- **Ignorer la chaîne de certificat incorrect**

  L'utilisateur peut continuer à accéder à son profil de chiffrement même si la partie publique du certificat de l'émetteur n'est pas disponible sur la machine client ou est conservée dans le mauvais magasin de certificats.

- **Ignorer une révocation inconnue**

  Lorsque les PKI de certains constructeurs écrivent les raisons de révocation d'un certificat dans une CRL, ils ne respectent pas les normes courantes. Il est généralement impossible d'utiliser un certificat dont la raison de la révocation est inconnue. Néanmoins, un utilisateur peut continuer à accéder à son profil de chiffrement même si cette option est activée.

Remarque : n'oubliez pas qu'en ignorant les erreurs détectées au moment de la vérification des certificats des utilisateurs, vous compromettez généralement la stratégie de sécurité de l'entreprise.

Ces paramètres peuvent être définis également dans Paramètres serveur. Les certificats sont vérifiés lorsqu'un responsable de la sécurité se connecte à la console conpal LAN Crypt Administration et lorsqu'une autorisation supplémentaire est octroyée.

4.1.3 Utiliser le nom Novell

Vous indiquez ici si le système utilise ou non le nom de connexion Novell pour rechercher les fichiers de stratégie. Si vous indiquez que les fichiers de stratégie doivent être générés avec les noms Novell dans Administration sous Paramètres centraux/Répertoires, conpal LAN Crypt génère deux fichiers de stratégie pour chaque utilisateur. Un fichier comporte le nom de connexion Novell et l'autre le nom d'utilisateur Windows. Ces fichiers ont des contenus identiques.

Lorsque vous vous connectez à un serveur Novell, vous devez toujours utiliser le nom de connexion Novell.

Si les paramètres du système indiquent que le nom d'utilisateur Windows doit être utilisé comme nom de connexion, paramétrez **Utiliser le nom de connexion Novell** sur **non**.

Remarque : si un client n'arrive pas à se connecter à un serveur Novell (par exemple, en cas de défaillance de la liaison) et si l'utilisateur se connecte en local avec son nom d'utilisateur Windows, le profil de chiffrement sera tout de même chargé correctement à partir du fichier de stratégie puisque conpal LAN Crypt peut aussi utiliser le nom d'utilisateur Windows pour identifier le fichier de stratégie approprié. Dans ce cas, le fichier est lu à partir du cache. La mise à jour du cache remonte à la dernière connexion Novell.

4.1.4 Résoudre toutes les variables d'environnement

conpal LAN Crypt résout la variable d'environnement %USERNAME% pour les chemins.

Vous pouvez indiquer ici si d'autres variables d'environnement doivent être résolues dans des chemins.

Cependant, l'utilisation d'autres variables d'environnement dans les chemins peut être source de problèmes si les utilisateurs peuvent les modifier. Il est ainsi possible que les données du chemin ne fonctionnent plus correctement dans le profil de chiffrement.

4.1.5 Options de menu activées

Vous pouvez définir ici quelles options du menu conpal LAN Crypt seront visibles sur un poste client. Par défaut, toutes les options de menu sont affichées. Si vous désactivez ici une option du menu, elle ne sera pas visible sur le poste client. Le client ne dispose donc pas de cette fonctionnalité. Cela vous permet, par exemple, d'éviter que le chiffrement sur un poste client ne soit désactivé.

4.1.6 Règles d'ignorance par défaut

Étant donné que le pilote de conpal LAN Crypt se charge systématiquement à chaque démarrage d'un poste, tous les fichiers ont déjà été contrôlés pour vérifier s'ils étaient chiffrés et possédaient donc les droits d'accès appropriés même si aucun profil de chiffrement spécifique à l'utilisateur n'a été chargé. Une baisse des performances est possible pendant cette phase.
Toutefois, si vous définissez un paramètre spécifique à la machine dans la configuration de conpal LAN Crypt, vous pourrez configurer le pilote conpal LAN Crypt de sorte qu'il ignore les répertoires spécifiques jusqu'au chargement du profil de chiffrement de l'utilisateur.

Cliquez deux fois sur **Règles d'ignorance par défaut** dans les Paramètres client pour ouvrir la boîte de dialogue dans laquelle vous indiquerez les répertoires (par exemple, `"c:\*.*;d:\*.*"`) que devra ignorer le pilote de conpal LAN Crypt.

Si vous saisissez plusieurs chemins, séparez chacun d'entre eux par un point-virgule.

Cependant, si vous utilisez cette règle, n'oubliez pas que le contrôle d'accès conpal LAN Crypt ne sera pas effectué tant que le profil de chiffrement de l'utilisateur ne sera pas chargé.

Exemple :

Si vous saisissez `"c:\*.*;d:\*.*"` dans les Règles d'ignorance par défaut, le pilote ignorera tous les répertoires des disques C et D jusqu'au chargement du profil de chiffrement.

Même si vous utilisez conpal LAN Crypt sur un serveur de terminal, vous pouvez accélérer ses performances à l'aide du paramètre Règles d'ignorance par défaut. Par exemple, si plusieurs utilisateurs travaillent sur le même serveur de terminal mais qu'un seul a recours à conpal LAN Crypt, vous pouvez indiquer au pilote d'ignorer les sessions de tous les autres utilisateurs. Aucun profil de chiffrement n'a été chargé pour ces utilisateurs. Ils sont donc uniquement concernés par l'option Règles d'ignorance par défaut.

4.1.7 Emplacement pour les certificats des responsables de la sécurité

Pour désigner l'emplacement de stockage, sélectionnez *Paramètres client*, puis dans le volet droit de la console, cliquez deux fois sur **Emplacement client pour les certificats des responsables de la sécurité**.

Après la saisie du chemin, conpal LAN Crypt tente automatiquement d'importer le certificat du responsable de la sécurité de ce répertoire si le certificat du fichier de stratégie utilisateur correspondant est absent. En conséquence, il importe tous (!) les fichiers .cer du répertoire indiqué.

4.1.8 Emplacement client du fichier de clé

Pour désigner l'emplacement de stockage, sélectionnez *Paramètres client*, puis dans le volet droit de la console, cliquez deux fois sur **Emplacement client du fichier de clé**.

Après la saisie du chemin, conpal LAN Crypt tente automatiquement d'importer un fichier de clé .p12 en cas d'absence de la clé privée du fichier de stratégie. Ce fichier doit être nommé "`nomconnexion*.p12`" afin que le système puisse reconnaître qu'il appartient à un utilisateur en particulier.

Les deux chemins ci-dessus ne constituent pas des paramètres par défaut, ce qui signifie que la partie publique de l'administrateur de sécurité et les différents certificats ne sont pas chargés automatiquement tant que le responsable de la sécurité n'a pas spécifié les chemins.

conpal LAN Crypt Administration stocke dans le même répertoire les fichiers .p12, ainsi que la partie publique des certificats du responsable de la sécurité. Cependant, du point de vue du client, il est possible de configurer ces chemins séparément de manière à pouvoir désactiver l'une ou l'autre fonction, si nécessaire. Malgré tout, ces chemins sont généralement les mêmes. Si vous souhaitez un chargement automatique du certificat du responsable de la sécurité et des certificats des utilisateurs à partir de répertoires différents, vous devez les copier manuellement dans les répertoires concernés.

4.1.9 Emplacement client du fichier de stratégie

Pour désigner l'emplacement de stockage, sélectionnez *Paramètres client*, puis dans le volet droit de la console, cliquez deux fois sur **Emplacement client du fichier de stratégie**.

Saisissez le chemin correspondant à l'emplacement du fichier de stratégie spécifique à l'utilisateur. Pour garantir l'accès des clients à leurs fichiers de stratégie (par exemple, sur une unité réseau partagée), le chemin doit être entré du point de vue des clients.

Il s'agit généralement du répertoire dans lequel ils ont été générés par conpal LAN Crypt. Vous devez suivre les règles de capitalisation des chemins UNC car aucune unité de disque n'est associée à ces fichiers à ce stade de la configuration !

Vous pouvez utiliser la variable d'environnement %LOGONSERVER% dans ce paramètre (pour équilibrer la charge, etc.).

4.1.10 Répertoire cache du fichier de stratégie

Pour désigner l'emplacement de stockage du cache, sélectionnez *Paramètres client*, puis dans le volet droit de la console, cliquez deux fois sur **Répertoire cache du fichier de stratégie**.

Une copie locale du fichier de stratégie est enregistrée dans ce répertoire. Cette copie est généralement chargée à partir d'un répertoire réseau. L'utilisateur doit posséder l'autorisation d'écrire des données dans ce répertoire local. Ceci garantit la disponibilité d'un profil de chiffrement d'un utilisateur même en l'absence de connexion à un réseau.

Vous pouvez utiliser l'un des emplacements de stockage de la liste ou sélectionner <autre> et saisir un emplacement différent dans ce champ.

Remarque : les emplacements affichés dans la liste sont des répertoires Windows par défaut qui dépendent du système d'exploitation que vous utilisez. <Données des applications locales> se rapporte toujours à un répertoire de la machine locale tandis que les autres répertoires (par exemple, les utilisateurs itinérants) peuvent être également présents sur des unités réseau.
Si vous entrez manuellement un emplacement de stockage, vous devez vous assurer que ce répertoire existe sur l'ordinateur client.

Remarque : si vous souhaitez effacer un utilisateur de votre environnement conpal LAN Crypt, n'oubliez pas que la copie locale restera sur l'ordinateur. Cet utilisateur peut ensuite exploiter les autorisations de cette copie locale pour accéder aux données aussi longtemps que la copie reste sur l'ordinateur.
Pour éviter ceci, créez un fichier de stratégie vide pour cet utilisateur. Pour ce faire, choisissez d'Effacer le fichier de stratégie et de supprimer l'utilisateur de tous les groupes.

4.1.11 Délai de chargement des profils

Indiquez ici un intervalle de temps (en secondes) qui s'écoulera avant que le profil utilisateur ne soit chargé. Ce délai est par exemple important si un certificat sur un jeton est utilisé. Le délai de chargement du profil garantit que le jeton est accessible lorsque le certificat est requis. Valeur type : 20 secondes.

4.1.12 Types de fichiers pour l'assistant de chiffrement initial

Si vous définissez ici des types de fichiers spécifiques, seuls les fichiers du type indiqué seront traités par l'assistant de chiffrement initial. L'utilisateur ne peut pas modifier ce paramètre dans l'assistant de chiffrement initial.

Ce paramètre affecte uniquement les fichiers pour lesquels une règle de chiffrement existe.

Si un répertoire contient également d'autres fichiers d'un type indiqué ici, ils ne feront pas partie du chiffrement initial. Ils ne feront l'objet d'un chiffrement que si l'utilisateur les ouvre et les enregistre à nouveau.

Si vous prévoyez de laisser les utilisateurs définir eux-mêmes ce paramètre dans l'assistant de chiffrement initial, ne configurez pas ce paramètre.

Si vous avez indiqué ici des types de fichiers et que vous prévoyez de laisser les utilisateurs effectuer leur sélection ultérieurement, redéfinissez ce paramètre de sorte à ce qu'il ne soit pas configuré.

Remarque : ce paramètre concerne uniquement l'assistant de chiffrement initial. Si le chiffrement initial est lancé via l'extension propre à l'Explorateur, ce paramètre n'a plus aucun effet.

Indiquez les types de fichiers dans une liste et séparez-les par des points-virgules.

Exemple : `doc;xls;txt`

4.1.13 Durée de vie du fichier de stratégie en cache

Comportement standard de conpal LAN Crypt

Lorsqu'un utilisateur se connecte à Windows, le chargement de son profil mis en cache intervient en premier. conpal LAN Crypt vérifie ensuite la disponibilité pour l'utilisateur d'un nouveau fichier de stratégie. L'application établit pour cela une connexion vers l'emplacement indiqué du fichier de stratégie (lecteur réseau). Si un nouveau fichier de stratégie y figure, le profil en cache de l'utilisateur sera mis à jour.

Cette approche a pour avantage que l'utilisateur peut commencer à travailler avec des fichiers chiffrés pendant que conpal LAN Crypt vérifie l'existence d'une nouvelle version du fichier de stratégie.

Si le lecteur réseau n'est pas accessible, l'utilisateur travaille avec le profil utilisateur mis en cache jusqu'à ce que celui-ci puisse être mis à jour.

Si cette option est définie sur *non configuré*, conpal LAN Crypt adopte le comportement décrit ci-après.

Utilisez ce paramètre pour modifier le comportement standard

Remarque : pour définir une option comme n'étant pas configurée, cliquez sur celle-ci avec le bouton droit de la souris, puis sélectionnez Supprimer dans le menu contextuel qui s'affiche. Dans la colonne ***Configuré***, **non** apparaîtra en regard de l'option correspondante.

Vous pouvez définir ici la durée de validité des stratégies mises en cache sur les ordinateurs client.

Au cours de la période définie ici, le fichier de stratégie reste valide sur le client et l'utilisateur peut accéder aux données chiffrées, même si aucune connexion n'existe à l'emplacement du dossier partagé de stratégie.

La durée durant laquelle les fichiers de stratégie sont mis en cache et ainsi considérés comme valides peut être définie en jours ou en semaines.

Une fois ce délai expiré, conpal LAN Crypt tente de charger le fichier de stratégie du lecteur réseau afin de le mettre à nouveau à jour. Si cela se révèle impossible, le fichier de stratégie n'est pas chargé. L'utilisateur n'est alors plus en mesure d'accéder aux données chiffrées. Le fichier de stratégie ne peut être mis à jour et chargé à nouveau que si un fichier de stratégie valide est disponible (par exemple, lors de la connexion suivante avec une connexion à l'emplacement client des fichiers de stratégie). L'utilisateur accède alors à nouveau aux données chiffrées. Le compteur réservé à la durée de stockage en mémoire cache est réinitialisé.

D'un côté, en indiquant la durée du stockage en mémoire cache, vous pouvez vous assurer que les ordinateurs client reçoivent à intervalles réguliers des fichiers de stratégie mis à jour et que les utilisateurs travaillent à tout moment avec des stratégies actualisées. D'un autre côté, vous évitez aux utilisateurs de travailler indéfiniment avec les mêmes fichiers de stratégie. Un utilisateur peut en effet travailler indéfiniment avec une version mise en cache du fichier de stratégie si cette option est définie sur *non configurée*.

Le compteur correspondant à la durée autorisée de stockage en mémoire cache est réinitialisé dans les cas suivants :

- L'emplacement de stockage des fichiers de stratégie est accessible et un fichier de stratégie valide a été transféré sur le client (par exemple, au moment de la connexion de l'utilisateur ou par déclenchement après un intervalle de mise à jour défini). Cependant, il ne s'agit pas d'un nouveau fichier de stratégie.
- Un nouveau fichier de stratégie est disponible et a été chargé correctement.

Le compteur correspondant à la durée autorisée de stockage en mémoire cache n'est PAS réinitialisé dans les cas suivants :

- L'ordinateur client tente de recevoir un nouveau fichier de stratégie. Cependant, l'emplacement de stockage des fichiers de stratégie n'est pas accessible.
- Un nouveau fichier de stratégie a été transféré. Cependant, une erreur empêche son chargement.
- Un nouveau fichier de stratégie est disponible. Cependant, il exige un nouveau certificat.

L'utilisateur ne dispose pas de ce certificat ou n'est pas en mesure de le charger.

En cas d'échec de la mise à jour du fichier de stratégie, la durée d'expiration du fichier de stratégie mis en cache s'affiche dans une infobulle, sur l'ordinateur client. L'utilisateur peut alors lancer une mise à jour manuelle via l'icône de la barre d'état conpal LAN Crypt. Une mise à jour automatique sera également effectuée en fonction de l'*intervalle de mise à jour du profil utilisateur*.

Les fichiers de stratégie ne sont pas mis en mémoire cache

Si cette option est définie sur 0, le fichier de stratégie ne sera pas mis en mémoire cache. Cela signifie que les utilisateurs reçoivent leurs profils utilisateurs en se connectant, à condition que l'emplacement du fichier de stratégie soit accessible. S'il ne l'est pas, une erreur survient lors du chargement du profil et l'utilisateur ne peut pas accéder aux fichiers chiffrés.

Clients de la version 3.12

Cette fonctionnalité n'est pas disponible dans les versions client précédentes. Toutefois, il est tout à fait possible d'utiliser les clients de la version 3.12 avec cette version Administration. Au moment du chargement des fichiers de stratégie, les clients de ce type adoptent le comportement suivant :
le client tente toujours de charger le fichier de stratégie depuis l'emplacement de fichier indiqué. Si cet emplacement n'est pas accessible, une version mise en cache du fichier de stratégie est chargée. Ce fichier de stratégie mis en cache ne possède aucune date d'expiration et n'est pas mis à jour tant qu'une version plus récente n'est pas correctement chargée. En outre, il est impossible de définir un intervalle de mise à jour pour ces stratégies (see *Intervalle de mise à jour du profil* on page 145). Les fichiers de stratégie mis en cache restent valides tant que l'emplacement indiqué des fichiers de stratégie est accessible et le fichier de stratégie mis en cache est remplacé par un fichier de stratégie provenant de cet emplacement.

4.1.14 Décompresser les fichiers au format NTFS

Ce paramètre permet à l'assistant de chiffrement initial de traiter les fichiers NTFS compressés. Si vous définissez l'option **Décompresser les fichiers au format NTFS** sur **oui**, l'assistant décompresse les fichiers NTFS compressés puis les chiffre, si une règle de chiffrement existe.

Si vous définissez l'option **Décompresser les fichiers au format NTFS** sur **non**, l'assistant de chiffrement initial ignore les fichiers NTFS compressés. Ils ne seront pas chiffrés, même si une règle de chiffrement a été indiquée les concernant.

Une fois cette option configurée, les utilisateurs ne peuvent pas la modifier dans l'assistant de chiffrement initial ! Les utilisateurs peuvent uniquement configurer cette option eux-mêmes dans l'assistant de chiffrement initial si elle a été définie ici sur *non configuré*.

4.1.15 Déchiffrement des fichiers EFS

Ce paramètre permet à l'assistant de chiffrement initial de traiter les fichiers EFS chiffrés. Si vous définissez l'option **Déchiffrement des fichiers EFS** sur **oui**, l'assistant déchiffre les fichiers EFS chiffrés puis les chiffre à nouveau, dans les cas où une règle de chiffrement conpal LAN Crypt existe.

Si vous définissez l'option **Déchiffrement des fichiers EFS** sur non, l'assistant de chiffrement initial ignore les fichiers EFS chiffrés. Ils ne seront pas chiffrés de nouveau par conpal LAN Crypt, même si une règle de chiffrement a été définie les concernant.

Une fois cette option configurée, les utilisateurs ne peuvent pas la modifier dans l'assistant de chiffrement initial ! Les utilisateurs peuvent uniquement configurer cette option eux-mêmes dans l'assistant de chiffrement initial si elle a été définie ici sur *non configuré*.

Remarque : pour définir une option comme n'étant *pas configurée*, cliquez sur celle-ci avec le bouton droit de la souris, puis sélectionnez **Supprimer** dans le menu contextuel qui s'affiche. Dans la colonne ***Configuré***, **non** apparaîtra en regard de l'option correspondante.

4.1.16 Intervalle de mise à jour du profil

Ce paramètre définit la fréquence selon laquelle conpal LAN Crypt vérifie l'existence de nouveaux fichiers de stratégie et les met à jour si nécessaire.

Pour mettre à jour les fichiers de stratégie, conpal LAN Crypt doit accéder à l'unité réseau sur laquelle ces fichiers sont enregistrés. conpal LAN Crypt vérifie l'existence d'une nouvelle version du fichier de stratégie sur l'unité réseau, puis met à jour le fichier de stratégie sur l'ordinateur client, si nécessaire.

conpal LAN Crypt procède automatiquement à toutes les étapes requises pour réussir le chargement du profil utilisateur (si besoin, il recherche de nouveaux certificats, les vérifie, etc.). Le nouveau profil remplacera l'ancien uniquement et ne sera chargé que si aucune erreur n'intervient au cours du traitement. Le compteur réservé à la durée de stockage en mémoire cache sera ensuite réinitialisé. Le compteur est réinitialisé même si les fichiers de stratégie sont identiques.

Si cette option est définie sur non configuré, les fichiers de stratégie ne sont pas mis à jour.

L'intervalle de mise à jour peut être défini en minutes, heures, jours et semaines.

Remarque : conpal LAN Crypt n'autorise aucun intervalle de mise à jour inférieur à 15 minutes. Si cette option est définie sur 0, la mise à jour de la stratégie désactivée.

4.1.17 Mode silencieux en cas d'absence du profil utilisateur

Si le paramètre par défaut est utilisé et que le système ne détecte aucun profil utilisateur, conpal LAN Crypt affiche un message d'erreur.

Cette section vous permet d'indiquer si ce message d'erreur doit être supprimé dans les cas où le profil utilisateur est absent.

Si vous définissez **Masquer le message d'erreur** sur **oui**, le message d'erreur ne s'affichera pas.

4.1.18 Chiffrement persistant

Les fichiers demeurent chiffrés tant qu'ils sont soumis à une règle de chiffrement. Par exemple, si un utilisateur copie un fichier chiffré dans un dossier qui n'est associé à aucune règle de chiffrement, ce fichier sera enregistré en clair dans le dossier cible. En activant le chiffrement persistant, vous pouvez garantir que les fichiers restent chiffrés lorsqu'ils sont déplacés ou copiés.

Pour désactiver cette fonction, cliquez deux fois sur **Chiffrement persistant** et sélectionnez **Non** dans le champ de liste **Activer le chiffrement persistant**.

4.1.19 Protection forte de la clé privée

Indiquez ici que l'utilisateur est invité à s'authentifier chaque fois que la clé privée est utilisée par conpal LAN Crypt.

4.1.20 CSP et algorithmes

Indiquez ici le CSP et l'algorithme de hachage.

Pour la plus récente version du client, seul le **CSP à utiliser pour importer une clé privée** doit être sélectionné.

Pour les clients antérieurs à la version 3.90, des paramètres **supplémentaires** doivent être configurés. Vous devez sélectionner un **CSP à utiliser pour vérifier les signatures des fichiers de stratégie** et un **algorithme de hachage à utiliser pour signer/vérifier le fichier de stratégie**.

4.2 Paramètres serveur

Remarque : vous devez définir ces paramètres pour le serveur. Ils n'affectent pas les ordinateurs client.
Il est néanmoins essentiel que vous définissiez ces paramètres serveur avant de lancer la fonction d'administration pour la première fois.

4.2.1 Protection forte de la clé privée

Indiquez ici que l'utilisateur est invité à s'authentifier chaque fois que la clé privée est utilisée par conpal LAN Crypt.

4.2.2 Langage SQL

Indiquez ici le langage SQL qui sera utilisé pour les communications avec la source de données ODBC.

Sélectionnez :

- MS SQL Server
- Oracle
- Standard SQL

Votre choix sera ensuite utilisé dans la configuration de votre système.

4.2.3 Propriétaire de la base de données

Saisissez ici le propriétaire de la base de données pour garantir que la base de données utilisée peut être adressée correctement.

Pour le serveur MS SQL, la valeur par défaut "dbo" du générateur ne doit pas être changée. Elle ne doit être changée que si vous utilisez une base de données Oracle.

Remarque : si vous utilisez une base de données Oracle, vous devez saisir ici le propriétaire de la base de données en LETTRES MAJUSCULES. Il doit s'agir du même nom que celui qui a été utilisé lors de la création des tables de base de données.

4.2.4 Source de données ODBC

Saisissez ici le nom d'accès à la source de données ODBC.

conpal LAN Crypt utilise SGLCSQLServer comme nom par défaut pour la source de données ODBC. Pour utiliser un nom différent, saisissez ce nom avant de lancer conpal LAN Crypt Administration pour la première fois.

Remarque : respectez les minuscules et majuscules lors de la saisie de la source de données ODBC. Le nom que vous saisissez doit être identique à celui saisi au moment de la création de la source de données ODBC. Seules les sources de données ODBC 32 bits peuvent être utilisées.

4.2.5 Ignorer pendant la vérification du certificat

Indiquez ici l'état de certificat à ignorer lorsqu'un responsable de la sécurité se connecte ou lorsque des certificats sont assignés dans la console d'administration.

4.2.6 Algorithme de hachage

L'algorithme de hachage doit être configuré dans les **Paramètres client**.

4.2.7 Vérifier les extensions de certificats

Par défaut, lorsque conpal LAN Crypt assigne des certificats à partir du magasin, il fait appel uniquement à des certificats dont les valeurs *Chiffrement de clé* et/ou *Chiffrement de données* sont définies pour la propriété "keyusage".

Toutefois, vous pouvez renseigner le champ **Vérifier les extensions de certificats** de manière à ce que cette vérification ne soit pas effectuée, permettant ainsi à conpal LAN Crypt d'utiliser des certificats dotés d'autres propriétés.

Vérifier les extensions : **non**
autorise le recours à des certificats dotés d'autres propriétés.

Remarque : cependant, la possibilité ou non d'employer ces certificats avec conpal LAN Crypt dépend du CSP que vous utilisez.
Si vous décidez de désactiver cette vérification, assurez-vous que le type de certificat que vous souhaitez utiliser est effectivement accepté par conpal LAN Crypt.

4.3 Lecteurs non gérés Application non gérée Périphériques non gérés

Dans conpal LAN Crypt, vous pouvez indiquer les lecteurs, applications et périphériques (systèmes de fichiers en réseau) qui doivent être "non gérés (ignorés) par le pilote de filtrage de conpal LAN Crypt et donc exclus d'un chiffrement/déchiffrement transparent.

Un programme de sauvegarde est un exemple d'application qui peut ne pas être gérée ("non gérée"). Si vous souhaitez que les données de sauvegarde restent chiffrées, vous pouvez exclure cette application de la procédure de chiffrement/déchiffrement. Les données restent alors chiffrées au moment de leur sauvegarde.

Vous pouvez accroître les performances de façon significative en excluant des lecteurs entiers. Par exemple, si aucun chiffrement ne doit être effectué sur le lecteur E, indiquez simplement qu'il doit

être "ignoré". Vous pouvez également spécifier une règle de chiffrement qui exclut ce lecteur de la procédure de chiffrement, avec l'option "Ignorer la règle de chiffrement".

Lorsque vous marquez un lecteur comme "non géré", le pilote de filtrage ne traite pas le profil, ce qui accélère les opérations sur les fichiers.

Vous trouverez ces paramètres dans le nœud **Configuration LAN Crypt**.

Remarque : comme il s'agit de paramètres machines, ils seront pris en compte au redémarrage de l'ordinateur client.

4.3.1 Ajout de lecteurs de disque ignorés

Sélectionnez *Lecteurs non gérés* et cliquez sur **Ajouter ou ou des lecteurs non gérés** dans le menu contextuel.

Sélectionnez les lecteurs de disques qui doivent être ignorés par conpal LAN Crypt, puis cliquez sur **OK**.

4.3.2 Ajout d'applications ignorées

Sélectionnez *Applications non gérées* et cliquez sur **Ajouter une application non gérée** dans le menu contextuel.

Utilisation générale :

- Il est possible de définir les programmes de sauvegarde comme "non gérés" afin qu'ils lisent et sauvegardent toujours les données chiffrées.
- Il est généralement possible d'exclure de la procédure de chiffrement les applications susceptibles de provoquer des erreurs en cas d'utilisation simultanée avec conpal LAN Crypt alors qu'elles n'exigent pas de chiffrement.

Pour spécifier une application non gérée, vous devez saisir le nom complet de son fichier exécutable.

Saisissez le nom de l'application et son chemin (si nécessaire) et cliquez sur OK.

4.3.3 Ajout de périphériques ignorés

Sélectionnez *Périphériques non gérés*, puis cliquez sur **Ajouter un périphérique non géré** dans le menu contextuel.

La boîte de dialogue *Périphériques non gérés* affiche les systèmes de fichiers en réseau que vous pouvez exclure de la procédure de chiffrement conpal LAN Crypt. Pour des raisons

techniques, vous ne pouvez pas exclure des unités de réseau isolées. Vous pouvez seulement exclure des systèmes entiers de fichiers en réseau. La liste des périphériques prédéfinis est la suivante :

- Mappage du lecteur du client Citrix
- Client pour réseaux Microsoft
- Client Microsoft pour Netware
- Fournisseur UNC multiple
- Client Novell pour Netware

Remarque : les responsables de la sécurité peuvent exclure les lecteurs de disques individuels (réseau) de la procédure de chiffrement en créant une règle de chiffrement à cet effet.

Outre ces systèmes standard de fichiers en réseau, vous pouvez également exclure des périphériques particuliers en saisissant leur nom de périphérique. Cela peut être utile si vous disposez de systèmes de fichiers tiers et si vous souhaitez les exclure de la procédure de chiffrement.

Les administrateurs peuvent employer un utilitaire tel que Device Tree de OSR pour afficher les noms des systèmes de fichiers en cours d'utilisation par le système.

Windows Vista et Windows 7

Pour Windows Vista et Windows 7, seule l'option **Fournisseur UNC multiple** est considérée.

Sous Windows Vista et Windows 7, les redirecteurs individuels ont été remplacés par le fournisseur UNC multiple. Il n'est ainsi plus possible d'exclure les systèmes individuels de gestion de fichiers en réseau du chiffrement. Sous Windows Vista et Windows 7, vous pouvez exclure tous les systèmes de gestion de fichiers en réseau du chiffrement ou bien activer le chiffrement pour chacun d'entre eux.

Si l'option **Fournisseur UNC multiple** est utilisée, les lecteurs réseau ne seront pas chiffrés.

Tous les paramètres restants seront ignorés sous Windows Vista et Windows 7.

4.4 Programmes au comportement spécifique lors de l'enregistrement des fichiers

Certains programmes (par exemple, Microsoft Office 2007 et versions supérieures) utilisent une approche particulière d'enregistrement des fichiers. Dans ce cas, des problèmes peuvent survenir au moment de l'ouverture d'un fichier non chiffré pour lequel une règle de chiffrement existe (par exemple en raison du fait qu'aucun chiffrement initial n'a été exécuté), puis de son réenregistrement. En raison de cette règle de chiffrement, le fichier devra être chiffré au moment

de son enregistrement. Toutefois, en raison du comportement spécifique du programme lors de l'enregistrement du fichier (création d'un fichier temporaire - renommage du fichier --> modification du statut de chiffrement), conpal LAN Crypt ne peut pas chiffrer le fichier.

Pour résoudre ce problème, vous devez définir ces programmes ici. Grâce aux informations définies ici, conpal LAN Crypt peut également chiffrer correctement les fichiers de ce type.

Pour ajouter un programme de ce type :

1. Sélectionnez *Programmes au comportement spécifique lors de l'enregistrement des fichiers*, puis cliquez sur **Ajouter un programme au comportement spécifique lors de l'enregistrement des fichiers** dans le menu contextuel.
2. Saisissez le nom de l'exécutable du programme.
   Exemple : `WINWORD.EXE`
3. Cliquez sur **OK**.
4. Répétez ces étapes pour chacun des programmes que vous souhaitez ajouter.

Ces programmes exigent une prise en charge spéciale de conpal LAN Crypt du fait de leur comportement particulier à l'enregistrement des fichiers. Ils s'affichent dans la vue de droite.

Remarque : ce problème n'apparaît qu'au moment de l'enregistrement d'un fichier qui a été déchiffré à l'ouverture et doit être chiffré du fait de la présence d'une règle de chiffrement (modification du statut de chiffrement).

Si vous utilisez Microsoft Office 2007, nous vous recommandons vivement de définir son exécutable ici.

5 ANNEXE

5.1 Journalisation

```
.... Droits pour 'SO_Sophos-Linz' ajoutés. Autorisé : 0x86000000 -
Refusé : 0x0)...
```

Les valeurs après **Autorisé :** et **Refusé :** indiquent les droits effectivement modifiés. Les tableaux suivants vous permettent d'interpréter ces valeurs.

Autorisé : 0x86000000

ACL pour RS : Lire	0x80000000
ACL pour RS : Modifier le certificat	0x02000000
ACL pour RS : Modifier la région	0x04000000
Autorisé :	0x86000000

Droits globaux d'un responsable de la sécurité

Droits	Valeurs
Créer des responsables de la sécurité	0x000001
Génération de profils	0x000002
Génération de clés	0x000004
Copier des clés	0x000008
Supprimer des clés	0x000010
Lecture de clés	0x000020
Génération de certificats	0x000040
Assigner des certificats	0x000080
Modifier les groupes	0x000200
Connexion à la base de données	0x000400
Autoriser les opérations	0x000800
Modification des utilisateurs	0x001000
Génération de règles	0x002000

Droits	Valeurs
Modifier les droits globaux	0x004000
Modifier les ACL	0x008000
Utiliser des clés spécifiques	0x010000
Modifier la configuration	0x020000
Lire les entrées du journal	0x040000
Gérer la journalisation	0x080000
Importer des objets répertoire	0x100000

ACL pour un groupe

Autorisations	Valeurs
Créer une clé	0x00000001
Copier des clés	0x00000002
Supprimer une clé	0x00000004
Créer des règles	0x00000008
Assigner des certificats	0x00000010
Ajouter un utilisateur	0x00000020
Supprimer un utilisateur	0x00000040
Ajouter un groupe	0x00000080
Supprimer des sous-groupes	0x00000100
Déplacer des groupes	0x00000200
Modifier les propriétés	0x00000400
Supprimer un groupe	0x00000800
Créer des profils	0x00001000
Modifier une ACL	0x00002000
Lire	0x00004000
Visible	0x00008000

ACL pour un RS

Autorisations	Valeurs
Modifier le nom	0x01000000

Autorisations	Valeurs
Modifier le certificat	0x02000000
Modifier la région	0x04000000
Assigner la configuration	0x08000000
Supprimer un SO	0x10000000
Modifier les autorisations globales	0x20000000
Modifier une ACL	0x40000000
Lire	0x80000000

5.2 Autorisations

5.2.1 Autorisations globales

Autorisations	Description
Créer un responsable de la sécurité	Le responsable de la sécurité est autorisé à créer des responsables de la sécurité supplémentaires.
Créer des profils	Le responsable de la sécurité a l'autorisation globale de lancer le résolveur de profils et de générer des fichiers de stratégie pour les utilisateurs individuels. Cette autorisation est nécessaire pour paramétrer l'autorisation "Créer des profils d'un groupe donné" pour un responsable de la sécurité. Créer des profils permet au responsable de la sécurité de créer des profils pour les utilisateurs où le responsable de la sécurité possède le droit Créer des profils pour le groupe parent de l'utilisateur. Cette autorisation est une condition préalable requise pour l'assignation de valeurs aux clés. Un utilisateur ayant l'autorisation Créer des clés peut uniquement générer des clés sans valeur !
Créer des profils pour tous les membres	Cette autorisation requiert que l'autorisation Créer des profils soit paramétrée. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Créer des profils pour tous les membres pour un groupe donné. Créer des profils pour tous les membres permet à un responsable de la sécurité de créer des profils pour tous les utilisateurs où ce responsable à l'autorisation Créer des profils sur le groupe parent ou l'autorisation Créer des profils pour tous les membres sur l'un des groupes auquel l'utilisateur est membre. **Remarque :** Étant donné que l'autorisation globale Créer des profils est une condition préalable requise pour Créer des profils pour tous les membres, les conditions suivantes s'appliquent : La désactivation de l'autorisation Créer des profils désactive également l'autorisation Créer des profils pour tous les membres. L'activation de l'autorisation Créer des profils pour tous les membres active automatiquement l'autorisation Créer des profils.

Autorisations	Description
Créer des clés	Le responsable de la sécurité peut générer des clés dans les groupes individuels. Un utilisateur ayant l'autorisation *Créer des clés* peut uniquement générer des clés sans valeur ! Au sein de la console Administration, les clés sans valeur peuvent être assignées aux règles de chiffrement. La valeur elle-même est générée au moment de la création des fichiers de stratégie. Pour générer manuellement des clés avec valeurs, le responsable de la sécurité doit avoir l'autorisation *Créer des profils*.
Copier des clés	Le responsable de la sécurité a le droit de copier des clés.
Supprimer des clés	Le responsable de la sécurité peut supprimer des clés dans les groupes individuels.
Lire clé	Le responsable de la sécurité peut voir les données des différentes clés d'un groupe.
Créer des certificats	Le responsable de la sécurité peut générer des certificats pour les utilisateurs.
Assigner des certificats	Le responsable de la sécurité a le droit d'assigner des certificats aux utilisateurs. Le responsable de la sécurité peut lancer l'assistant pour assigner les certificats. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Assigner des certificats d'un groupe donné pour un responsable de la sécurité. L'assignation des certificats permet au responsable de la sécurité d'assigner des certificats aux utilisateurs où le responsable de la sécurité possède le droit Assigner des certificats pour le groupe parent de l'utilisateur.

Autorisations	Description
Assigner des certificats à tous les membres	Cette autorisation requiert que l'autorisation Assigner des certificats soit paramétrée. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Assigner des certificats à tous les membres d'un groupe donné. Assigner des certificats à tous les membres permet à un responsable de la sécurité d'assigner des certificats à tous les utilisateurs où le responsable de la sécurité possède le droit Assigner des certificats sur le groupe parent de l'utilisateur ou le droit Assigner des certificats à tous les membres sur l'un des groupes auquel l'utilisateur est membre. **Remarque :** Étant donné que l'autorisation globale Assigner des certificats est une condition préalable requise pour Assigner des certificats à tous les membres, les conditions suivantes s'appliquent : La désactivation de l'autorisation Assigner des certificats désactive aussi automatiquement l'autorisation Assigner des certificats à tous les membres. L'activation de l'autorisation Assigner des certificats à tous les membres active l'autorisation Assigner des certificats.
Administrer des groupes	Le responsable de la sécurité peut effectuer des modifications dans les groupes. Ajout de sous-groupes, déplacement, synchronisation ou suppression de groupes.
Connexion à la base de données	Le responsable de la sécurité peut se connecter à la base de données conpal LAN Crypt. Le paramètre par défaut est activé pour cette autorisation. Cette autorisation permet à un responsable de la sécurité de modifier facilement la base de données (par exemple, en cas de départ d'un membre du personnel dans une entreprise). Ce droit n'est pas accordé aux personnes qui sont habilitées à agir uniquement si une autre personne les y autorise. Cela garantit que ces personnes pourront uniquement autoriser des actions nécessitant une confirmation et n'auront aucun moyen de procéder à des modifications dans conpal LAN Crypt.
Autoriser les opérations	Le responsable de la sécurité peut participer à des actions nécessitant une confirmation.
Administrer des utilisateurs	Le responsable de la sécurité peut ajouter ou retirer un utilisateur au sein d'un groupe et synchroniser les groupes.

Autorisations	Description
Copier des utilisateurs	Le responsable de la sécurité est autorisé à ajouter (copier) des utilisateurs dans les groupes. Cette autorisation globale est la condition préalable requise pour paramétrer l'autorisation Copier des utilisateurs d'un groupe donné pour un responsable de la sécurité. Pour ajouter un utilisateur à un groupe, le responsable de la sécurité doit avoir l'autorisation Copier des utilisateurs sur le groupe parent de l'utilisateur.
Créer des règles	Le responsable de la sécurité est autorisé à générer des règles de chiffrement pour les utilisateurs.
Modifier les autorisations globales	Le responsable de la sécurité peut modifier les droits globaux octroyés à un autre responsable de la sécurité.
Modifier les ACL	Le responsable de la sécurité peut modifier l'ACL d'un groupe.
Utiliser clés spécifiques	Le responsable de la sécurité peut utiliser des clés spécifiques dans les règles de chiffrement et peut afficher des clés spécifiques dans *Toutes les clés conpal® LAN Crypt.*
Modifier la configuration	Le responsable de la sécurité peut modifier la configuration (chemins). Cette autorisation est nécessaire pour afficher l'onglet Configurations dans les Paramètres centraux et pour que le responsable de la sécurité puisse effectuer des changements dans l'onglet Répertoires s'il est connecté à la base de données.
Lire les entrées du journal	Le responsable de la sécurité peut consulter les paramètres de journalisation ainsi que les événements.
Gérer la journalisation	Le responsable de la sécurité peut modifier les paramètres de journalisation. Il peut archiver, supprimer et vérifier les entrées.
Importer des objets répertoire	Le responsable de la sécurité peut importer des OU, des groupes et des utilisateurs à partir d'un service d'annuaire et les ajouter à la base de données conpal LAN Crypt. Avant de pouvoir importer des objets de l'annuaire, le responsable de la sécurité a aussi besoin des autorisations *Administrer les groupes* et *Administrer les utilisateurs*. Elles sont activées automatiquement lorsque l'autorisation *Importation des objets du répertoire* est sélectionnée. Si un responsable de la sécurité ne possède pas cette autorisation, le nœud *Objets du répertoire*, qui sert à importer les OU, groupes et utilisateurs, n'est pas visible dans la console Administration.

5.2.2 Autorisations de modification des paramètres d'un responsable de la sécurité

Autorisations	Description
Modifier le nom	Permet de modifier le nom du responsable de la sécurité auquel est assigné le détenteur de l'autorisation.
Modifier le certificat	Permet de modifier le certificat du responsable de la sécurité auquel est assigné le détenteur du droit.
Modifier la région	Permet de modifier le préfixe de la région du responsable de la sécurité auquel est assigné le détenteur du droit.
Assigner la configuration	Permet de modifier la configuration du responsable de la sécurité auquel est assigné le détenteur du droit.
Supprimer un responsable de la sécurité	Permet de supprimer le responsable de la sécurité auquel est assigné le détenteur de l'autorisation.
Modifier les autorisations globales	Permet de modifier les autorisations globales du responsable de la sécurité auquel est assigné le détenteur de l'autorisation.
Modifier ACL	Permet de modifier les autorisations globales de l'ACL à laquelle est assigné le détenteur du droit.
Lire	Affiche le responsable de la sécurité auquel est assigné le détenteur de l'autorisation dans *Paramètres centraux\Administration des responsables de la sécurité*. C'est la condition préalable à tous les droits permettant la gestion de ce responsable de la sécurité. Activation automatique si un droit de ce type est sélectionné.

5.2.3 Autorisations du responsable de la sécurité concernant la gestion des groupes

Autorisations	Description
Créer une clé	Le responsable de la sécurité a le droit de générer des clés dans le groupe.
Copier des clés	Le responsable de la sécurité a le droit de copier des clés.

Autorisations	Description
Supprimer la clé	Le responsable de la sécurité a le droit de supprimer des clés.
Créer des règles	Le responsable de la sécurité est autorisé à générer des règles de chiffrement pour les utilisateurs.
Assigner des certificats	Le responsable de la sécurité a le droit d'assigner des certificats aux utilisateurs. Le responsable de la sécurité a le droit de lancer l'assistant d'assignation des certificats. Assigner des certificats permet au responsable de la sécurité d'assigner des certificats aux utilisateurs du groupe qui est aussi le groupe parent.
Assigner des certificats à tous les membres	Cette autorisation requiert que l'autorisation Assigner des certificats soit paramétrée. Assigner des certificats à tous les membres permet au responsable de la sécurité d'assigner des certificats à tous les utilisateurs du groupe : aux utilisateurs dont le groupe est le groupe parent et à ceux membres du groupe et qui ont un groupe parent différent. Remarque : Si vous paramétrez Assigner des certificats à tous les membres sur Autoriser, Assigner des certificats est automatiquement paramétré sur Autoriser. Si vous paramétrez Assigner des certificats sur Refuser, Assigner des certificats est automatiquement paramétré sur Refuser.
Ajouter un utilisateur	Le responsable de la sécurité a le droit d'ajouter des clés dans le groupe manuellement. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Copier un utilisateur	Le responsable de la sécurité a le droit d'ajouter des utilisateurs de ce groupe dans un autre groupe. Ceci est autorisé seulement pour les membres où ce groupe est aussi l'objet parent.
Supprimer un utilisateur	Le responsable de la sécurité est autorisé à utiliser le composant logiciel enfichable *Membres et certificats du groupe* pour supprimer des utilisateurs. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.

Autorisations	Description
Ajouter un groupe	Le responsable de la sécurité est autorisé à utiliser le menu contextuel d'un groupe pour ajouter de nouveaux groupes. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Supprimer des sous-groupes	Le responsable de la sécurité est autorisé à supprimer des sous-groupes pour ce groupe. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Déplacer des groupes	Le responsable de la sécurité a le droit de déplacer des groupes créés manuellement dans la console Administration (par glisser-déposer). Impossible de déplacer les groupes importés. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Modifier les propriétés	Le responsable de la sécurité a le droit de modifier les propriétés d'un groupe.
Supprimer un groupe	Le responsable de la sécurité a le droit de supprimer des groupes. Cela suppose que le responsable de la sécurité a retiré l'autorisation "Supprimer des sous-groupes" du groupe ci-dessus. Cette autorisation est une condition préalable à l'importation/la synchronisation des groupes et utilisateurs.
Créer des profils	Le responsable de la sécurité a l'autorisation de lancer le résolveur de profils et de générer des fichiers de stratégie pour les utilisateurs sélectionnés. Créer des profils permet au responsable de la sécurité de créer des profils pour les utilisateurs du groupe qui est aussi le groupe parent.

Autorisations	Description
Créer des profils pour tous les membres	Cette autorisation requiert que l'autorisation Créer des profils soit paramétrée. Créer des profils pour tous les membres permet au responsable de la sécurité de créer des profils pour tous les utilisateurs du groupe : aux utilisateurs dont le groupe est le groupe parent et à ceux membres du groupe et qui ont un groupe parent différent. Remarque : Si vous paramétrez Créer des profils pour tous les membres sur Autoriser, Créer des profils est automatiquement paramétré sur Autoriser. Si vous paramétrez Créer des profils sur Refuser, Créer des profils pour tous les membres est automatiquement paramétré sur Refuser.
Modifier une ACL	Le responsable de la sécurité a le droit de modifier l'ACL d'un groupe (par exemple, en ajoutant un autre responsable de la sécurité).
Lire	Le responsable de la sécurité dispose des droits en lecture sur ce groupe et peut voir le contenu des composants logiciels enfichables. Activation automatique si des autorisations de modification sont accordées.
Visible	Le responsable de la sécurité peut voir le groupe. Est défini dans le nœud de base et hérité en aval. En cas de refus pour un responsable de la sécurité, le groupe est masqué (avec refus de "Lecture").

6 Mentions légales

7 Support technique

Vous bénéficiez du support technique des produits conpal de l'une des manières suivantes:

- Rendez-vous sur la base de connaissances du support de Sophos sur https://support.conpal.de.
- Téléchargez la documentation des produits sur https://docs.lancrypt.com/fr/client/sglc_397_hfra.pdf https://docs.lancrypt.com/fr/admin/sglc_397_ahfra.pdf
- Ouvrez un incident support sur support@conpal.de.