Creating Trust in
the Digital Society

utimaco®

u.trust

LAN Crypt

Version du produit : 13.0.1
Date du document : Août 2026

Table des matières

1 Aperçu 3

1.1 Qu'est-ce qu'u.trust LAN Crypt ? 3

1.2 Protection des données à l'aide d'u.trust LAN Crypt 5

1.3 Chiffrement transparent 8

1.4 Architecture 13

2 Prise en main 17

2.1 Certificats 17

2.2 Installation 24

2.3 Installation sans surveillance 27

2.4 Mise à niveau 28

2.5 Paramètres de langue 33

2.6 Désinstallation 34

3 Administration 35

3.1 Étapes requises 36

3.2 Préparatifs pour l'administration d'u.trust LAN Crypt 37

3.3 Responsables de la sécurité principaux 42

3.4 Administration : vue d'ensemble 47

3.5 Paramètres centraux 51

3.6 Affichage de toutes les clés u.trust LAN Crypt 83

3.7 Affichage des utilisateurs et des certificats sélectionnés 85

3.8 Créer un responsable de la sécurité 88

3.9 Connexion à l'administration 103

3.10 Importation de groupes et d'utilisateurs 104

3.11 Assignation de responsables de la sécurité aux unités d'organisation 119

3.12 Propriétés des groupes 127

3.13 Propriétés des utilisateurs 132

3.14 Conception de l'environnement de sécurité 135

3.15 Génération de clés 136

3.16 Règles de chiffrement 144

3.17 Balises de chiffrement 161

3.18 Assignation de certificats 163

3.19 Fournir des règles de chiffrement - générer des fichiers de stratégie 175

3.20 Journalisation de la base de données 178

4 Configuration d’u.trust LAN Crypt 187

4.1 Paramètres client 188

4.2 Paramètres du serveur 200

4.3 Lecteurs non gérés, applications non gérées, périphériques non gérés 204

5 ANNEXE 207

5.1 Journalisation 207

5.2 Autorisations 209

6 Mentions légales 217

7 Support technique 218

1 Aperçu

1.1 Qu'est-ce qu'u.trust LAN Crypt ?

u.trust LAN Crypt fournit un chiffrement de fichier transparent. Il a été conçu pour permettre aux utilisateurs des grandes organisations d'échanger des données de manière confidentielle. Dans ce cas de figure, les fichiers chiffrés peuvent être stockés localement sur le disque dur de l'utilisateur, sur un support amovible ou même sur des lecteurs réseau.

Le processus de chiffrement est totalement transparent pour les utilisateurs. Il a lieu automatiquement lorsque les fichiers sont créés ou enregistrés. Ces fichiers sont également déchiffrés de manière transparente lors de la lecture de leurs données. Ce processus est effectué par un pilote de filtre qui est intégré dans le système de fichiers sur un ordinateur Windows.

Le fonctionnement du pilote de filtre d'*u.trust LAN Crypt* est similaire à celui d'un scanner antivirus. Il identifie en effet les fichiers auxquels il faut accéder et effectue l'opération de chiffrement ou de déchiffrement appropriée sur ceux-ci. Chaque fois qu'un utilisateur déplace un fichier dans un répertoire de confiance, le fichier est chiffré sur son ordinateur, et chaque fois qu'un autre utilisateur de confiance membre du même groupe lit le fichier à partir de ce répertoire, il est transféré à cet utilisateur sous forme chiffrée. Le fichier n'est déchiffré que lorsqu'il atteint l'ordinateur cible, où l'utilisateur peut le modifier. Il est alors chiffré à nouveau avant d'être renvoyé dans le répertoire chiffré.

Les fichiers chiffrés ne sont pas « assignés » à des utilisateurs individuels. Tout utilisateur disposant de la bonne clé peut accéder au fichier chiffré. Cela permet aux administrateurs de créer des groupes d'utilisateurs logiques dont les membres peuvent partager des fichiers chiffrés. Ce processus peut être comparé à un trousseau de clés similaire à celui que vous utilisez au quotidien : *u.trust LAN Crypt* fournit aux utilisateurs et aux groupes d'utilisateurs un trousseau de clés, et les clés individuelles peuvent être utilisées pour ouvrir différentes portes ou coffres-forts.

Les utilisateurs non autorisés peuvent être en mesure d'accéder physiquement à ces fichiers chiffrés (mais uniquement à partir de postes de travail sans *u.trust LAN Crypt*). Cependant, sans l'autorisation d'*u.trust 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, si le réseau est attaqué ou si les employés ne respectent pas la stratégie de sécurité de l'organisation.

Si vous avez besoin de protéger votre propriété intellectuelle stockée dans des fichiers contre tout accès non autorisé via le réseau local, sur des serveurs de fichiers, sur des disques durs locaux ou même sur des supports amovibles, *u.trust LAN Crypt* est le produit qu'il vous faut.

Le responsable de la sécurité peut spécifier les fichiers et dossiers qu'*u.trust LAN Crypt* doit protéger de manière centralisée, en définissant une ou plusieurs règles de chiffrement. Par exemple, pour s'assurer que tous les documents Word sont protégés, le responsable de la

sécurité doit définir la règle **.docx*. Dès que cette règle est déployée dans un système client dans le cadre d'un fichier de stratégie, tous les documents Word sont chiffrés, peu importe où ils sont stockés. Si nécessaire, plusieurs règles de chiffrement peuvent être combinées pour former un profil de chiffrement.

Dans cet exemple, trois règles différentes ont été regroupées dans un même profil de chiffrement :

Règle	Clé	Description
*.docx	Clé1	Cela chiffre tous les documents Word avec « Clé1 », peu importe où ils sont stockés.
D:\Data*.*	Clé2	Cela chiffre tous les fichiers du dossier spécifié avec « Clé2 ».
\\Server1\Share1\HR*.xlsx	Clé3	Cela chiffre tous les fichiers Excel du dossier de serveur spécifié avec « Clé3 ».

Avec *u.trust LAN Crypt*, le responsable de la sécurité peut définir des règles très complexes pour garantir que seules les données réelles requises sont chiffrées dans des emplacements très spécifiques. Ces règles sont déployées dans des fichiers de stratégie (voir « Création de fichiers de stratégie ») qui peuvent être stockés sur un serveur de fichiers ou dans le dossier d'ouverture de session réseau sur un contrôleur de domaine Windows. Le responsable de la sécurité peut facilement créer une stratégie personnalisée pour chaque utilisateur. Cette stratégie contient toutes les clés et règles qui s'appliquent à cet utilisateur.

Le responsable de la sécurité utilise l'interface utilisateur graphique de l'administration *u.trust LAN Crypt* pour générer et administrer ces fichiers de stratégie. Ensuite, la *Microsoft Management Console* (MMC) est utilisée comme interface. Les composants logiciels enfichables fournissent de nombreux outils au responsable de la sécurité, lui facilitant ainsi les tâches.

Les fichiers de stratégie sont protégés séparément, au moyen de certificats, pour chaque utilisateur. Ainsi, entre autres choses, toutes les clés contenues dans ce fichier sont chiffrées avec la clé publique du certificat de son utilisateur respectif. Par conséquent, seul l'utilisateur autorisé, qui possède également la clé privée du certificat utilisé, peut ouvrir ce fichier via l'application cliente *u.trust LAN Crypt*. Une PKI (**P**ublic **K**ey **I**nfrastructure) déjà mise à disposition au sein de l'organisation peut être utilisée ici. Sinon, le responsable de la sécurité peut choisir l'option qui consiste à générer les certificats lui-même en utilisant *u.trust LAN Crypt*.

Les données de l'administration *u.trust LAN Crypt* sont ensuite stockées dans une base de données SQL. Bien entendu, tous les enregistrements de données importantes sont chiffrés dans la base de données SQL, en particulier les données de clés. Étant donné que la base de données utilisée ici ne dépend pas de la fonctionnalité d'administration du système, les fonctions de sécurité et d'administration du système peuvent être maintenues strictement séparées. *u.trust LAN Crypt* peut également être utilisé pour configurer différents rôles pour les responsables de la sécurité, dont les autorisations peuvent être restreintes de manière à correspondre à des tâches spécifiques dans des domaines spécifiques.

Seul le responsable principal de la sécurité (MSO) dispose de tous les droits en tout temps. Un responsable principal de la sécurité est également en mesure de déléguer des tâches et droits individuels relatifs à l'administration *u.trust LAN Crypt* à d'autres responsables de la sécurité, créant ainsi une hiérarchie d'administration qui répond à la structure organisationnelle de chaque entreprise.

1.2 Protection des données à l'aide d'u.trust LAN Crypt

u.trust LAN Crypt garantit que les fichiers sensibles peuvent être stockés en toute sécurité sur les serveurs de fichiers et les postes de travail. Les données sont transmises de manière sécurisée sur les réseaux LAN ou WAN, car le chiffrement et le déchiffrement sont effectués dans la RAM sur le poste de travail du client. L'installation d'un logiciel de sécurité spécial sur le serveur de fichiers lui-même n'est pas nécessaire.

Les fichiers de stratégie comprennent toutes les règles, tous les droits d'accès et toutes les clés nécessaires au chiffrement transparent.

Pour qu'un utilisateur puisse chiffrer et déchiffrer des données avec *u.trust LAN Crypt* sur son poste de travail, il doit pouvoir accéder à son fichier de stratégie. Cela se fait via un partage réseau pour l'emplacement où se trouve le fichier de stratégie. Le fichier de stratégie est chiffré et protégé contre toute utilisation non autorisée par un certificat. Pour pouvoir les utiliser, l'utilisateur doit avoir la clé privée de son certificat et connaître le mot de passe.

Toutes les tâches de chiffrement/déchiffrement s'exécutent de manière transparente sur le poste de travail du client, avec une interaction utilisateur minimale.

u.trust LAN Crypt permet aux utilisateurs de confiance d'être organisés en divers groupes de confiance grâce à la définition de différents droits pour les répertoires et fichiers. Ces droits sont regroupés dans des profils de chiffrement pour les utilisateurs. S'il possède la clé privée assignée au certificat, l'utilisateur peut accéder au fichier de stratégie qui contient le profil de chiffrement.

Tous les utilisateurs d'*u.trust 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 soucier du chiffrement ou de l'échange de clés. Il leur suffit de pouvoir accéder aux fichiers de stratégie pour que leurs données soient chiffrées ou déchiffrées de manière transparente dès leur ouverture ou fermeture.

Les profils de chiffrement étant distribués via des fichiers de stratégie, toutes les formes organisationnelles peuvent être mappées à partir d'un modèle LAN centralisé, dans lequel les utilisateurs sont administrés de manière centralisée, vers un modèle distant dans lequel les utilisateurs travaillent sur des ordinateurs portables.

u.trust LAN Crypt prend en charge Windows ainsi que macOS et pour les appareils mobiles Android et iOS / iPadOS.

Remarque : Même en fonctionnement normal, Windows transfère souvent des parties de la mémoire de travail sur le disque dur. Dans certains cas, par exemple lors d'un plantage ou d'un « écran bleu », l'intégralité du contenu de la mémoire peut même être écrite sur le disque dur. Ainsi, des informations sensibles qui ne sont normalement disponibles que dans la mémoire principale (comme le contenu des documents ouverts) peuvent être stockées dans un fichier sur le disque dur. Un chiffrement du disque dur (comme, par exemple avec *BitLocker* ou *Utimaco DiskEncrypt*) garantit que le contenu de ces données souvent sensibles est dans tous les cas enregistrés sous forme chiffrée sur le disque dur et donc protégé de manière optimale contre l'espionnage. C'est pourquoi l'utilisation d'un chiffrement du disque dur est recommandée comme protection de base importante et comme complément judicieux lors de l'utilisation de *u.trust LAN Crypt*.

Administration u.trust LAN Crypt et administration Windows

Un ordinateur d'administration séparé est utilisé pour configurer *u.trust LAN Crypt* et gérer les profils de chiffrement. Pour établir une distinction claire entre l'administration Windows et l'administration *u.trust LAN Crypt*, un responsable de la sécurité doit intervenir. Le responsable de la sécurité définit les profils de chiffrement dans les fichiers de stratégie pour déterminer quelles données chiffrées doivent être stockées dans des répertoires particuliers, et qui est autorisé à accéder à ces données. Après avoir créé les fichiers de stratégie sur le poste d'administration, le responsable de la sécurité les déploie.

Microsoft **M**anagement **C**onsole (MMC), outil Windows standard, est utilisé pour administrer *u.trust LAN Crypt*. L'interface utilisateur de l'administration *u.trust LAN Crypt* se compose de composants logiciels enfichables pour MMC. L'administration *u.trust LAN Crypt* stocke la plupart des objets à administrer (données utilisateur, clés, chemins de chiffrement, etc.) dans leur propre base de données.

Il y a deux avantages majeurs à utiliser cette approche de base de données plutôt que de simples outils Windows tels qu'Active Directory :

- L'administration du système et l'administration de la sécurité peuvent être strictement séparées. En effet, *u.trust LAN Crypt* utilise une base de données dédiée et est totalement indépendant de l'administration du système. Les clés de la base de données de l'administration *u.trust LAN Crypt* sont cryptées et donc protégées contre les accès non autorisés. En outre, cette base de données empêche le système d'*u.trust LAN Crypt* d'être modifié involontairement (par exemple si l'administrateur système supprime un objet de sécurité requis).
- D'autre part, il n'est souvent pas avisé de permettre aux personnes qui ne sont pas administrateurs système de changer la configuration du système. Il est évident qu'attribuer à l'administrateur système la permission d'écrire des données est un réel problème. C'est une autre bonne raison pour stocker les données spécifiques d'*u.trust LAN Crypt* dans une base de données séparée.

Pour fournir la meilleure protection possible, les fonctionnalités d'*u.trust LAN Crypt* sont divisées en deux parties :

- **Fonctionnalités d'utilisateur d'*u.trust LAN Crypt***

  Les fonctionnalités d'utilisateur d'*u.trust LAN Crypt* incluent les informations de chiffrement et de déchiffrement des données. Ces informations sont nécessaires pour les tâches quotidiennes qui s'appuient sur *u.trust LAN Crypt*. Une fois qu'un utilisateur est autorisé à accéder aux informations de chiffrement, les fichiers sont chiffrés et déchiffrés de manière transparente. Aucune autre interaction avec l'utilisateur n'est requise. En outre, *u.trust LAN Crypt* dispose d'une gamme de fonctions d'affichage qui permettent à l'utilisateur de visualiser « son » profil de chiffrement et les clés qui lui sont fournies.

- **Fonctionnalités du responsable de la sécurité d'*u.trust LAN Crypt***

  L'administration *u.trust LAN Crypt* propose des fonctions réservées à un responsable de la sécurité. Les règles de chiffrement ne peuvent être administrées que si vous possédez un certificat de responsable de la sécurité. C'est à ce moment qu'il est possible de créer de nouveaux profils de chiffrement ou de gérer des profils existants, par exemple.

Les deux composants peuvent être installés séparément.

1.3 Chiffrement transparent

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

- Chaque fichier pour lequel il existe une règle de chiffrement est chiffré automatiquement.
- Si les fichiers sont copiés ou déplacés vers un dossier chiffré, ils sont chiffrés conformément à la règle de chiffrement qui s'applique à ce dossier. Vous pouvez également définir différentes règles de chiffrement pour différentes extensions de fichiers ou de noms dans le même dossier. Le chiffrement n'est pas spécifique aux dossiers. Cela dépend entièrement des règles de chiffrement !
- Lorsque les fichiers chiffrés sont renommés, ils restent chiffrés (à condition qu'il n'y ait pas de règle de chiffrement différente, ou aucune règle de chiffrement pour le nouveau nom/extension de fichier).
- Si vous copiez ou déplacez des fichiers chiffrés vers un emplacement où la règle de chiffrement actuelle n'est plus valide, ils restent chiffrés, car le *chiffrement persistant* est activé par défaut.
- Si vous copiez ou déplacez des fichiers chiffrés vers un emplacement dans lequel la règle de chiffrement actuelle n'est plus valide, mais dans lequel une règle de chiffrement différente reste valide, ces fichiers sont d'abord déchiffrés, puis chiffrés à nouveau selon la nouvelle règle de chiffrement.
- Le *chiffrement transparent* s'applique à toutes les opérations de fichiers. L'utilisateur ne remarque aucunement ces processus lorsqu'il travaille avec des données chiffrées, car tous s'exécutent en arrière-plan.
- Le *chiffrement persistant* peut être utilisé pour empêcher un utilisateur de déchiffrer involontairement des fichiers lors de leur copie ou de leur déplacement vers un dossier qui ne comporte aucune règle de chiffrement.

1.3.1 Accès aux données chiffrées

Si l'utilisateur ne possède pas la clé appropriée, il n'est pas autorisé à accéder aux données chiffrées d'un dossier. L'utilisateur ne peut en aucun cas lire, copier, déplacer ou renommer les fichiers chiffrés de ce dossier, ni interagir d'une autre manière avec ceux-ci.

Si l'utilisateur dispose de la clé avec laquelle les fichiers ont été chiffrés, il peut ouvrir et travailler avec ces fichiers à tout moment, même si aucune règle de chiffrement ne fait référence à ces fichiers dans son profil de chiffrement.

1.3.2 Renommer ou déplacer des dossiers

Pour des raisons de performances, *u.trust LAN Crypt* ne modifie pas le statut du chiffrement lorsque des dossiers complets sont déplacés à l'aide de l'Explorateur Windows. Cela signifie qu'aucun chiffrement, déchiffrement ou rechiffrèrent n'est effectué lorsqu'un dossier est déplacé ou renommé.

Si les fichiers ont été chiffrés, ils restent chiffrés dans le nouveau dossier ou dans le nouvel emplacement de stockage. Si l'utilisateur possède la clé appropriée, il peut travailler avec ces fichiers comme d'habitude.

Remarque : Cependant, cela ne s'applique que s'il n'y a pas de règle de chiffrement pour le nouvel emplacement de stockage. Cependant, s'il y a une règle de chiffrement, les fichiers seront chiffrés selon la règle de chiffrement applicable au nouvel emplacement de stockage.

Déplacement sécurisé de fichiers et de dossiers : *u.trust LAN Crypt* permet également de déplacer des fichiers et des dossiers en toute sécurité. Les fichiers sont également chiffrés, déchiffrés ou rechiffrés selon les besoins, conformément aux règles de chiffrement applicables. Les fichiers sources sont supprimés (« effacés ») en toute sécurité après avoir été déplacés.

Cette fonction est disponible via l'entrée **Déplacement sécurisé** dans le menu contextuel de l'explorateur Windows sous l'élément ***u.trust LAN Crypt***. Une boîte de dialogue peut ensuite être utilisée pour sélectionner l'emplacement vers lequel les fichiers doivent être déplacés.

1.3.3 Déchiffrement explicite des fichiers

Si la fonction **Chiffrement persistant** est désactivée, un fichier à déchiffrer doit seulement être copié ou déplacé vers un emplacement ou un dossier pour lequel il n'y a pas de règle de chiffrement. Il sera alors automatiquement déchiffré.

Toutefois, ce n'est le cas que si

- un profil de chiffrement approprié a été chargé,
- l'utilisateur utilise 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 pour lequel vous possédez la clé.

Remarque : Supprimer des fichiers signifie que vous les déplacez vers la *Corbeille Windows*. Pour fournir le plus haut niveau de sécurité, les fichiers chiffrés par *u.trust LAN Crypt* restent chiffrés dans la *Corbeille*. Pour vider la *Corbeille*, aucune clé n'est nécessaire.

1.3.5 Fichiers/dossiers exclus du chiffrement

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

- Fichiers du dossier d'installation d'*u.trust LAN Crypt*.
- Fichiers dans les dossiers Programmes et Programmes (x86).
- Fichiers du dossier d'installation de Windows.
- Fichiers dans le dossier Windows.old.
- Cache du fichier de stratégie.

  L'emplacement est spécifié dans l'administration *u.trust LAN Crypt* et affiché dans l'onglet **Profil** de la boîte de dialogue **Statut**.
- Répertoire racine du lecteur système. Les sous-dossiers ne sont pas exclus.
- Emplacements indexés (search-ms).
- Fichiers dans des dossiers définis dans *u.trust LAN Crypt* avec une règle d'exclure, de bypass ou d'ignorer.

1.3.6 Chiffrement persistant

Les fichiers restent normalement chiffrés par *u.trust LAN Crypt* tant qu'ils sont soumis à une stratégie de chiffrement. Les fichiers seraient donc déchiffrés s'ils étaient copiés ou déplacés vers un dossier pour lequel aucune règle de chiffrement ne s'applique.

Si vous ne voulez pas que des copies indésirables en format texte brut de fichiers chiffrés soient créées, le **chiffrement persistant** peut empêcher cela. Avec le **chiffrement persistant**, vous pouvez vous assurer que les fichiers chiffrés ne sont pas déchiffrés lorsqu'ils sont déplacés ou copiés.

Les responsables de la sécurité ou les administrateurs système peuvent désactiver ce comportement dans la configuration de *u.trust LAN Crypt* via une stratégie de groupe (GPO) dans Windows. Par défaut, cette fonctionnalité est déjà activée dans *u.trust LAN Crypt*. Si le **chiffrement persistant** est désactivé, les fichiers chiffrés seront déchiffrés et stockés en format texte brut, lorsqu'ils sont copiés/déplacés vers un emplacement qui n'est pas défini dans la règle de chiffrement.

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

- Le pilote d'*u.trust LAN Crypt* conserve uniquement le nom du fichier, sans aucune information relative au chemin d'accès. Seul ce nom peut être utilisé à des fins de comparaison. Cela ne concerne donc que des situations dans lesquelles les fichiers source et cible ont un nom identique. Si le fichier est renommé pendant l'opération de copie, le nouveau fichier est considéré comme un fichier « différent » et n'est donc pas soumis au **chiffrement persistant**.

- Lorsqu'un utilisateur enregistre un fichier chiffré avec **Enregistrer sous** un nom de fichier différent dans un emplacement non couvert par une règle de chiffrement, le fichier sera en texte brut.
- Les informations relatives aux fichiers ne sont conservées que pendant une durée limitée. Si l'opération prend trop de temps (plus de 15 secondes), le fichier nouvellement créé est considéré comme un fichier différent et indépendant, et n'est donc pas soumis au **chiffrement persistant**.

1.3.6.1 Chiffrement persistant par rapport à la règle de chiffrement

Comme mentionné ci-dessus, le **chiffrement persistant** essaie de s'assurer qu'un fichier chiffré conserve son état de chiffrement, par exemple sa clé de chiffrement d'origine. Cela fonctionne parfaitement bien si le fichier est déplacé dans un dossier qui n'applique pas de stratégie de chiffrement. Mais si le fichier est copié ou déplacé vers un emplacement où une stratégie de chiffrement s'applique, la stratégie de chiffrement a une priorité plus élevée et annule donc le **chiffrement persistant**. Le fichier sera chiffré avec la clé définie dans la règle de chiffrement et non avec celle qui a été utilisée à l'origine.

1.3.6.2 Chiffrement persistant par rapport au paramètre Ignorer le chemin d'accès

Le paramètre **Ignorer le chemin d'accès** remplace également le **chiffrement persistant** et garantit ainsi que les fichiers chiffrés qui sont copiés dans un dossier avec le paramètre Ignorer le chemin d'accès sont stockés en texte brut !

Le paramètre **Ignorer ce chemin** est principalement utilisé pour les fichiers auxquels on accède très fréquemment, et pour les fichiers qui n'ont pas de raison particulière d'être chiffrés. Cela améliore les performances du système.

Remarque : Il n'y a pas de protection d'accès pour les fichiers dans les dossiers qui sont soumis au paramètre **Ignorer le chemin d'accès** si le mini-filtre est utilisé comme pilote de chiffrement.

1.3.6.3 Chiffrement persistant par rapport au paramètre Exclusions de chemin d'accès

Le paramètre **Exclure ce chemin** remplace également le **Chiffrement persistant** et garantit ainsi que les fichiers chiffrés qui sont copiés dans un dossier avec le paramètre Exclure ce chemin sont stockés en texte brut !

Remarque : Pour les fichiers dans les dossiers qui sont soumis au paramètre **Exclure ce chemin**, la protection d'accès existe toujours.

1.3.7 Limitations au chiffrement persistant

Pour des raisons techniques, le chiffrement persistant présente certaines limitations. Autrement dit, il est possible que le résultat réel du chiffrement persistant ne réponde pas toujours aux attentes de l'utilisateur.

Voici quelques scénarios courants dans lesquels le chiffrement persistant est insuffisant :

Les fichiers qui sont censés rester simples sont chiffrés.

- **Les fichiers SIMPLES sont copiés vers plusieurs emplacements avec et sans application de règles de chiffrement.**

  Si un fichier simple est copié de manière simultanée vers plusieurs emplacements, dont l'un a une règle de chiffrement appliquée, les autres copies de ce fichier peuvent être chiffrées également, et ce, bien que le fichier d'origine ne le soit pas. Si le fichier est copié vers un emplacement chiffré en premier lieu, il est ajouté à la liste interne des pilotes. Lorsque la deuxième copie est créée ailleurs, le pilote trouve le nom du fichier dans sa liste et chiffre donc la deuxième copie également.

- **Créez un fichier portant le même nom après avoir accédé à un fichier chiffré.**

  Si un fichier chiffré est ouvert (consulté) et qu'un nouveau fichier portant le même nom est créé peu de temps après, le fichier nouvellement créé est chiffré avec la même clé que le fichier qui a été ouvert en premier.

  Remarque : Cela ne s'applique que si le même thread/application est utilisé pour lire le fichier chiffré ainsi que pour créer le nouveau.

  Un exemple d'usage courant : Dans l'explorateur Windows, faites un clic droit dans un dossier avec la règle de chiffrement et cliquez sur **Nouveau > Document texte**. Faites immédiatement un clic droit sur un dossier sans règle de chiffrement et cliquez sur **Nouveau > Document texte**. Le second fichier sera également chiffré.

Les fichiers ne sont pas chiffrés.

- **Plusieurs copies d'un fichier sont créées.**

  Si des copies d'un fichier chiffré sont créées dans le même dossier que le fichier original, celles-ci ne sont pas chiffrées. Puisque les copies créées ont des noms de fichiers différents (par exemple doc.txt ou doc - Copy.txt), la correspondance du nom de fichier échoue. Elles ne sont donc pas chiffrées par le **chiffrement persistant**.

1.3.8 API client et étiquettes de chiffrement pour les produits DLP

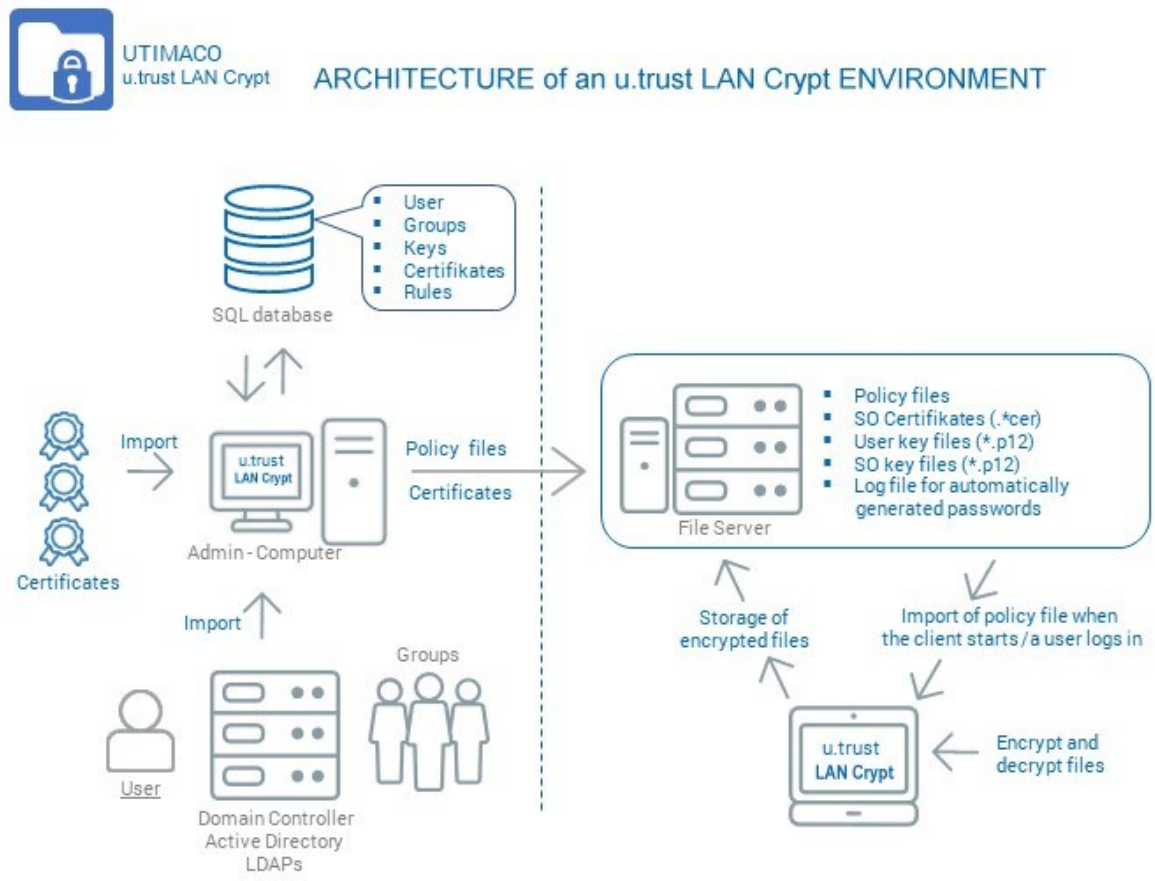
Si un produit DLP identifie des données qui doivent être chiffrées, il peut utiliser l'API client *u.trust LAN Crypt* pour chiffrer ces fichiers. Dans l'administration *u.trust LAN Crypt*, vous pouvez définir différentes balises de chiffrement qui spécifient la clé *u.trust LAN Crypt* à utiliser.

L'API client peut utiliser ces balises de chiffrement prédéfinies pour appliquer des clés spéciales selon les différents contenus. Par exemple, la balise de chiffrement `<CONFIDENTIEL>` peut être utilisée pour chiffrer tous les fichiers classés comme confidentiels par votre produit de protection contre la perte de données.

1.4 Architecture

u.trust LAN Crypt est constitué des deux composants suivants : L'administration *u.trust LAN Crypt* et le client *u.trust LAN Crypt*. Ces deux composants sont généralement installés sur les postes de travail standard dotés du système d'exploitation Windows 11. Les responsables de la sécurité utilisent l'administration *u.trust LAN Crypt* pour définir et distribuer des profils de chiffrement, puis les mettre à la disposition des utilisateurs.

La figure suivante illustre l'interaction entre les composants individuels et la méthode d'intégration d'*u.trust LAN Crypt* au réseau d'entreprise :



1.4.1 Administration u.trust LAN Crypt

Le composant administratif contient les outils nécessaires à l'administration centrale d'*u.trust LAN Crypt*. Il est utilisé par un ou plusieurs responsables de la sécurité. L'installation est généralement effectuée sur un ou plusieurs postes de travail avec Windows 11 comme système d'exploitation. L'installation sur un serveur système Windows pris en charge par *u.trust LAN Crypt* est également possible si l'administration centrale via Windows Terminal Services ou Citrix MetaFrame est nécessaire. Ceci est particulièrement recommandé dans les environnements plus grands et en particulier dans les emplacements distribués. L'administration *u.trust LAN Crypt* est ensuite accessible via le protocole RDP (Remote Desktop) ou ICA (Independent Computing Architecture). Pour plus d'informations sur les versions Windows prises en charge, veuillez-vous référer aux notes de publication d'*u.trust LAN Crypt*.

Étant donné que la sécurité et la confidentialité maximales des données à protéger ne peuvent être garanties que si le système d'administration et l'administration *u.trust LAN Crypt* sont indépendants l'un de l'autre, *u.trust LAN Crypt* a une administration séparée de l'utilisateur et du groupe. Pour faciliter les choses, les utilisateurs et les groupes gérés par *u.trust LAN Crypt* peut être importés à partir d'un Active Directory existant ou d'un autre répertoire LDAP.

L'administration *u.trust LAN Crypt* nécessite une base de données SQL pour stocker les données de configuration et gérer les utilisateurs et les groupes *u.trust LAN Crypt*. La base de données peut être installée localement sur le système d'administration si Microsoft SQL Server Express Edition est utilisé. Pour les grandes installations ayant plusieurs responsables de la sécurité, il est recommandé d'utiliser un système de base de données central sous la forme d'un serveur Microsoft SQL ou Oracle.

Les responsables de la sécurité sont chargés de définir la stratégie de sécurité utilisée dans leur organisation. Ils déterminent les stratégies et veillent à ce qu'elles soient implémentées, mises à jour et respectées correctement. Les petites entreprises font généralement appel à un seul responsable de la sécurité. Les grandes organisations ont souvent plusieurs responsables de la sécurité qui travaillent habituellement au niveau du département ou du site, et qui sont organisés en hiérarchie. *u.trust LAN Crypt* peut également indiquer et refléter les différents niveaux hiérarchiques impliqués dans cette situation.

Au sommet de la hiérarchie se trouve un ou plusieurs responsables principaux de la sécurité : ils doivent être présents lorsque la base de données d'*u.trust LAN Crypt* est générée. Ces responsables définissent les premières stratégies et décident si la règle des quatre yeux (deux responsables de la sécurité sont nécessaires à l'authentification) doit être appliquée pour prendre des mesures qui ont un impact sur les problèmes de sécurité. Chaque responsable de la sécurité se voit attribuer des autorisations administratives particulières qui définissent ses droits fondamentaux. Son domaine de responsabilité peut également être limité à quelques groupes d'utilisateurs par des listes de contrôle d'accès (ACL).

u.trust LAN Crypt utilise des clés de chiffrement à clé (KEK) pour administrer les droits d'accès des utilisateurs. Celles-ci sont chiffrées et stockées dans la base de données SQL et, comme tous les contenus de la base de données, elles sont protégées contre les modifications avec les valeurs MAC et de hachage. Les tâches administratives sont organisées de telle sorte qu'un responsable de la sécurité connaît seulement le nom d'une clé et non sa valeur réelle. Cela signifie qu'il peut travailler avec des objets de clé et créer des règles de chiffrement. La flexibilité des procédures de contrôle des autorisations permet de couvrir un large éventail de scénarios. Par exemple, un chef de section peut définir des clés et assigner des dossiers. À l'étape de travail suivante, un responsable de la sécurité centrale peut générer le profil de chiffrement. Par conséquent, les clés restent sous contrôle central.

u.trust LAN Crypt reconnaît deux types de clés générées automatiquement : les clés utilisateur et les clés de groupe. Les clés utilisateur sont générées pour des utilisateurs individuels et peuvent être utilisées pour des règles de chiffrement génériques, telles que le chiffrement de répertoires de base ou de dossiers locaux ou temporaires. Chaque utilisateur a précisément une clé utilisateur. Si des données protégées par une clé utilisateur doivent être récupérées en cas d'urgence, le responsable de la sécurité doit assigner cette clé spécifique à un autre utilisateur. Ce type de récupération nécessite une autorisation administrative spéciale et peut

être lié à une « règle à quatre yeux » (approbation par une deuxième personne) pour s'assurer qu'il n'est pas utilisé à mauvais escient. Un concept similaire est également disponible pour les groupes d'utilisateurs : il s'agit de la clé de groupe (voir « *Réattribuer des clés spécifiques* »).

Remarque : Pour plus d'informations sur la procédure de récupération d'urgence de l'administration *u.trust LAN Crypt*, par exemple si le certificat du responsable principal de la sécurité est endommagé, consultez le section 3.5.10 « *Onglet Clés de récupération* » à la page 74.

Les fichiers de stratégie comprennent toutes les règles, tous les droits d'accès et toutes les clés nécessaires au chiffrement transparent. Avant qu'un utilisateur puisse chiffrer/déchiffrer des données à l'aide du logiciel *u.trust LAN Crypt* installé sur le poste de travail client, il doit d'abord accéder aux informations de chiffrement stockées dans un fichier de stratégie. Dans ce cas, les fichiers de stratégie sont stockés soit sur un serveur de fichiers, soit dans le partage Net logon d'un contrôleur de domaine.

Remarque : Vous n'avez pas besoin d'installer les composants d'*u.trust LAN Crypt* sur les serveurs de fichiers ou les contrôleurs de domaine. Cependant, pour faciliter l'administration des groupes d'utilisateurs et des ordinateurs clients d'*u.trust LAN Crypt*, il peut être utile d'installer les fichiers modèles administratifs (Fichiers ADMX et ADML) fournis avec la console d'administration sur un poste de travail d'administration (RSAT). Ceux-ci permettent d'administrer simplement et clairement les paramètres les plus importants pour les clients d'*u.trust LAN Crypt*.

Le fichier de stratégie est protégé contre l'accès non autorisé par un certificat. Seul le propriétaire du certificat a accès à la clé privée qui appartient au certificat, et peut donc utiliser ce certificat pour accéder aux informations de chiffrement pertinentes. Si des certificats auto-signés sont utilisés, ils sont également stockés sur un serveur de fichiers et l'utilisateur aura besoin de droits d'accès en lecture pour pouvoir utiliser ces certificats. *u.trust LAN Crypt* prend également en charge l'utilisation de certificats stockés sur des cartes à puce, des jetons USB ou des cartes informatiques appropriées.

Remarque : Vous pouvez utiliser *u.trust LAN Crypt* sans avoir à utiliser de cartes à puce ou de jetons pour stocker des certificats.

Les chemins d'accès aux fichiers de stratégie (du point de vue de l'utilisateur) et aux autres paramètres d'*u.trust LAN Crypt* sont identifiés par des mécanismes dans le système d'exploitation.

Un groupe de confiance autour d'*u.trust LAN Crypt* se compose d'un certain nombre d'utilisateurs ayant le même profil de chiffrement. Les fichiers de stratégie de chaque utilisateur sont générés dans Administration. Tous les utilisateurs d'*u.trust LAN Crypt* qui ont le même profil stocké dans leur fichier de stratégie sont membres d'un groupe d'autorisation. Ils n'ont pas à se soucier du chiffrement ou de l'échange de clés. Il leur suffit d'accéder au fichier de stratégie pour que leurs données soient chiffrées ou déchiffrées de manière transparente, dès qu'ils les ferment où les ouvrent.

1.4.2 Client u.trust LAN Crypt

Le client *u.trust LAN Crypt* est installé sur les systèmes Windows (PC, postes de travail, ordinateurs portables, serveurs de terminaux) sur lesquels vous souhaitez que le chiffrement soit effectué. En plus du pilote de filtre requis pour le chiffrement et le déchiffrement, le composant Client dispose d'une gamme d'autres composants facultatifs :

- Les extensions de l'Explorateur pour le chiffrement initial et explicite.
- Une application utilisateur permettant de charger et supprimer des règles de chiffrement ainsi que d'activer et désactiver le chiffrement.
- Une application utilisateur permettant d'afficher tous les paramètres et les règles qui sont actifs sur le client. Cela est notamment important dans les cas de support.
- Une application utilisateur pour le chiffrement initial.
- La prise en charge des jetons afin que les certificats à base de jetons puissent être utilisés pour accéder aux informations de chiffrement stockées.
- Pilote de filtre réseau qui aide à améliorer les performances lors de l'accès au réseau.
- API client pour permettre à certaines applications (par exemple les produits DLP) d'accéder à la fonction de cryptage de fichiers *u.trust LAN Crypt*.

Une fois le client *u.trust LAN Crypt* démarré, il accède au dossier avec son conteneur PKCS#12 (fichier *.P12) et son fichier de stratégie via les mécanismes du système d'exploitation (paramètres de Registre, stratégies de groupe). Lors de son premier accès au conteneur PKCS#12, l'utilisateur doit saisir le code PIN qu'un responsable de la sécurité lui a fourni de manière sécurisée (voir section 3.5.6 « Fichier journal pour les mots de passe des fichiers clés » à la page 67). Le certificat utilisateur est ensuite stocké dans la mémoire de certificat locale du système d'exploitation, c'est-à-dire lié au profil Windows chargé. Le certificat permet d'accéder aux parties chiffrées du fichier de stratégie via la « **Clé** de **chiffrement** du **profil** - PEK ». Si le certificat est stocké sur un jeton matériel pris en charge par le composant client, aucune action de la part de l'utilisateur n'est requise pour les opérations de chiffrement et de déchiffrement une fois que le jeton a été déverrouillé.

Le client *u.trust LAN Crypt* charge ensuite le fichier de stratégie avec ses paramètres et ses clés.

2 Prise en main

2.1 Certificats

u.trust 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 propriétaire d'un certificat peut accéder à la clé privée qui appartient à ce certificat et peut donc l'utiliser pour accéder aux informations de chiffrement.

Remarque : N'utilisez pas de certificats valables plusieurs centaines, voire plus de mille ans !

Dans l'intérêt de la sécurité de l'information, la durée de validité des certificats ne doit pas, si possible, dépasser 5 ans. Pour les certificats CA (**C**ertificate **A**uthority), Utimaco recommande cependant une durée de validité maximale de 20 ans.

Certificats qui peuvent être utilisés et leur provenance :

- Toute société dispose de sa propre **i**nfrastructure **à c**lé **p**ublique (PKI) ou utilise un Centre de gestion de la confidentialité pour créer des certificats pour les utilisateurs. Dans ce cas, les certificats existants peuvent être utilisés.
- Le composant d'administration d'*u.trust LAN Crypt* peut également générer des certificats auto-signés. Ces certificats ne peuvent être utilisés que par *u.trust LAN Crypt* ! Les certificats possèdent également 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) conformes à la norme X.509.

Dans *u.trust LAN Crypt*, vous pouvez configurer l'ajout ou non d'une extension critique à un certificat nouvellement généré.

Remarque : Dans certaines situations, d'autres applications ignoreront ces extensions critiques sur les certificats *u.trust LAN Crypt*. Cela posera alors des problèmes avec ces certificats auto-signés. Dans ce cas, vous devez explicitement désactiver tous les domaines d'utilisation des certificats *u.trust LAN Crypt* avec le composant logiciel enfichable Certificat de Microsoft Management Console pour empêcher l'utilisation de ces certificats dans d'autres applications.

Remarque : Si vous avez choisi d'ajouter une extension critique aux certificats nouvellement générés, un tel certificat, lorsque vous consultez ses informations, affichera le statut : "Un certificat contient une extension inconnue marquée comme critique". Cependant, vous pouvez ignorer cette information en toute sécurité, car *u.trust LAN Crypt* connaît l'OID (object identifier) de ses propres certificats et les reconnaît donc comme valides.

Les certificats sont attribués aux utilisateurs dans le composant d'administration d'*u.trust LAN Crypt*.

Informations importantes sur l'utilisation des certificats :

- *u.trust LAN Crypt utilise uniquement l'API Microsoft Crypto pour les fonctionnalités de certificat.*
- *u.trust LAN Crypt version 13.0.1* prend en charge **K**ey **S**torage **P**rovider (KSP).
- *u.trust LAN Crypt* prend en charge tous les **C**ryptographic **S**ervice **P**rovider (CSP) qui respectent certaines normes (par exemple longueur de clé RSA d'au moins 2048 bits). Ils comprennent, entre autres, Microsoft Enhanced CSP.

  Remarque : Microsoft Standard CSP (Microsoft Base CSP) ne peut pas être utilisé pour les certificats auto-signés générés par *u.trust LAN Crypt*.

  Remarque : Veuillez également noter que les **C**ryptographic **S**ervice **P**rovider (CSP) pour les opérations clés de *u.trust LAN Crypt* ne sont désormais pris en charge qu'en association avec des shims qui les rendent accessibles en tant que **K**ey **S**torage **P**rovider (KSP).

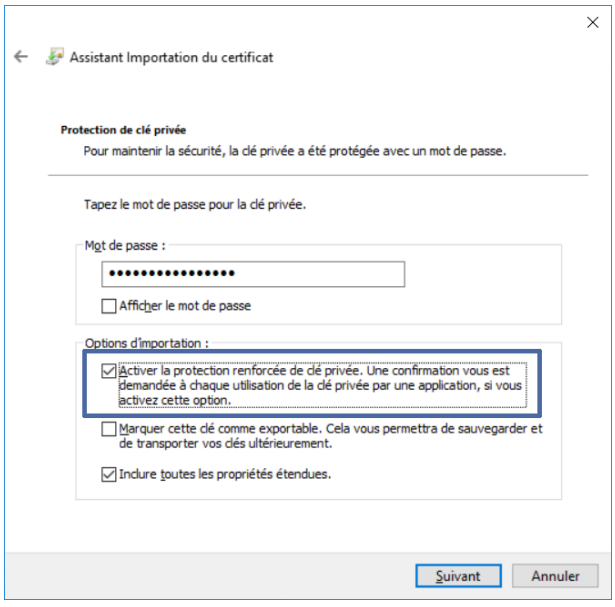
  Remarque : Veuillez également noter que l'algorithme de signature SHA-1 n'est plus pris en charge par Microsoft CSP car il n'est plus considéré comme sûr.

Si vous avez des questions sur la compatibilité d'autres CSP ou KSP, contactez l'équipe de support Utimaco (consultez la section *Support technique* sur la page 218).

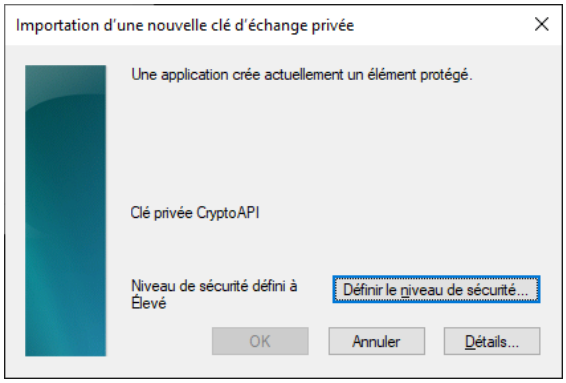
Remarque : Les certificats ECC (basés sur la cryptographie à courbe elliptique) ne sont actuellement pas pris en charge par *u.trust LAN Crypt*.

2.1.1 Niveaux de sécurité

Comme *u.trust LAN Crypt* vise à fournir le plus haut niveau de sécurité possible, nous recommandons de définir le niveau de sécurité sur « *Activer la protection renforcée de clé privée* » lors de l'importation d'un certificat à l'aide de l'assistant d'importation de certificats.



Après avoir cliqué sur **Terminer** dans l'*Assistant Importation du certificat*, la boîte de dialogue Importation d'une nouvelle clé d'échange privée s'affiche. Cliquez sur **Définir le niveau de sécurité** pour redéfinir le niveau de sécurité :



- **Élevé**

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

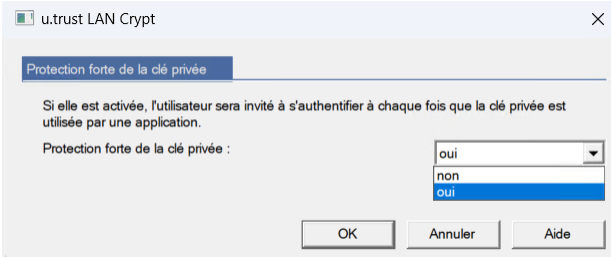
- **Moyen**

  Si vous sélectionnez *Moyen*, le système affiche une invite qui vous demande de confirmer l'utilisation d'une clé privée en cliquant sur **OK**.

Chaque fois que la clé privée est utilisée par une application, vous êtes invité à **saisir le mot de passe** (niveau de sécurité élevé) ou à cliquer sur **OK** (niveau de sécurité moyen), selon le niveau de sécurité choisi.

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

u.trust LAN Crypt vous permet d'importer des certificats automatiquement. Pour utiliser le niveau de sécurité moyen ou élevé avec les clés privées appartenant à ces certificats, vous devez définir l'option **Protection forte de clé privée** sur **oui** dans la configuration d'*u.trust LAN Crypt*.

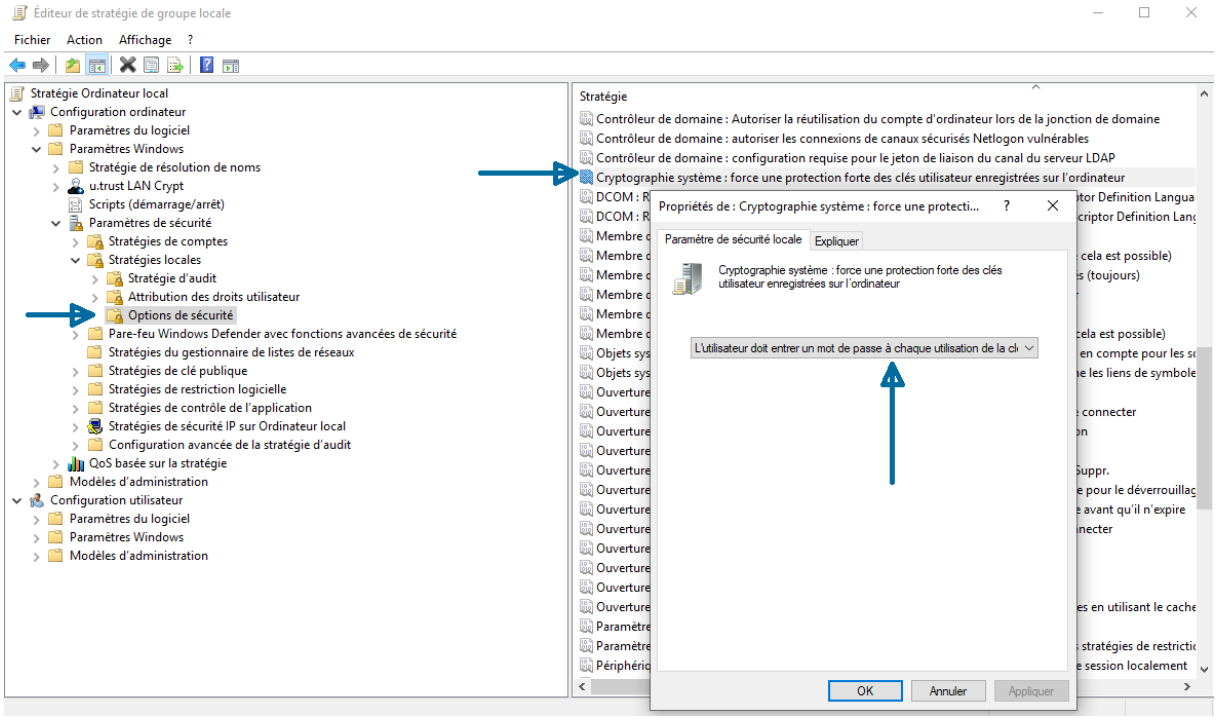


Si cette option n'est pas activée, le niveau de sécurité « **bas** » est automatiquement utilisé pour les certificats importés.

De cette façon, vous pouvez vous assurer que les certificats avec un niveau de sécurité élevé sont obligatoires et peuvent être mis en œuvre dans le cadre d'une politique de sécurité à l'échelle de l'entreprise.

Remarque : Si le niveau de sécurité le plus élevé est utilisé, les utilisateurs d'*u.trust LAN Crypt* doivent saisir le mot de passe de la clé privée une fois, à l'invite d'ouverture de session Windows, et à nouveau manuellement, chaque fois qu'une règle de chiffrement est chargée.

Activer également la stratégie de groupe Windows locale « *Cryptographie système* : *force une protection forte des clés utilisateur enregistrées sur l'ordinateur* » et sélectionner l'option « *L'utilisateur dot entrer un mot de passe à chaque utilisation de la clé* ».



Carte à puce :

Si des certificats stockés sur des cartes à puce sont utilisés, le mot de passe ne doit être saisi qu'une seule fois. Tant que la carte à puce reste dans le lecteur de cartes, il n'est pas nécessaire de saisir à nouveau le mot de passe.

Attention : nous recommandons d'activer la sécurité élevée pour la clé privée avant de démarrer l'administration *u.trust LAN Crypt* pour la première fois. Dans le cas contraire, le certificat du responsable principal de la sécurité initial est utilisé sans niveau de sécurité « élevé » lorsqu'il est créé par *u.trust LAN Crypt* et non, par exemple, importé à partir d'une carte à puce.

Attention : Par défaut, Windows met en cache les codes PIN pendant 24 heures. L'utilisation de certificats logiciels peut entraîner des problèmes de sécurité lors de la connexion à l'administration *u.trust LAN Crypt* et lorsque des autorisations supplémentaires sont fournies. Nous vous recommandons fortement de désactiver cette fonctionnalité.

Pour ce faire, définissez ces valeurs :

« `CachePrivateKeys` »=`dword:0x00000000`

« `PrivateKeyLifetimeSeconds` »=`dword:0x00000000`

« `PrivKeyCacheMaxItems` »=`dword:0x00000000`

« `PrivKeyCachePurgeIntervalSeconds` »=`dword:0x00000000`

Sous la clé :

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography
```

Ainsi que la valeur :

« `AllowCachePW` »=`dword:0x00000000`

Sous la clé :

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography\
Protect
```

Si vous faites cela, les codes PIN ne seront pas mis en cache.

Remarque : Si vous réglez « `CachePrivateKeys` » sur « `1` » et « `PrivateKeyLifetimeSeconds` » sur une valeur inférieure à « `5` », un **responsable de la sécurité (principal) pourrait devoir saisir son code PIN mot de passe à deux reprises** pour accéder à la clé privée, lorsque le paramètre « *Protection forte de clé privée* » est activé.

Conditions préalables à l'utilisation de certificats avec u.trust LAN Crypt

- Le certificat doit comporter une clé publique.
- La clé privée du certificat assigné doit être disponible avant qu'un utilisateur puisse accéder au profil de chiffrement.
- *u.trust LAN Crypt* répertorie uniquement les certificats stockés dans *Configuration utilisateur* dans les magasins de *Certificats personnels*, Autres personnes et Objet utilisateur Active Directory, ainsi que dans *Ordinateurs locaux* dans le magasin de certificats personnels. *u.trust LAN Crypt* ignore les certificats stockés à d'autres emplacements.

  Vous pouvez utiliser le *composant logiciel enfichable de la console Gestion des certificats* pour importer et organiser les certificats.
- Seule la clé publique est utilisée pour « associer » un certificat aux informations de chiffrement d'*u.trust LAN Crypt*. Vous n'avez pas besoin de connaître la clé privée. La clé privée reste la propriété du propriétaire du certificat, qui est la seule personne à pouvoir accéder aux informations de chiffrement.

Nous vous recommandons de disposer des certificats prêts à l'emploi avant de commencer à installer *u.trust LAN Crypt*. Les certificats apparaissent dans la boîte de dialogue Certificats immédiatement après l'installation d'*u.trust LAN Crypt*, et peuvent aussitôt être utilisés.

Remarque : *u.trust LAN Crypt* n'administre pas les certificats. Cependant, vous pouvez le faire en utilisant la propre infrastructure PKI de votre entreprise ou en utilisant des centres de gestion de la confidentialité.

2.1.2 Vérification des certificats

u.trust LAN Crypt effectue une vérification de certificat étendue. Cela signifie que les certificats ne sont acceptés qu'une fois leur chaîne de certificats complète (évaluation d'une **L**iste de **R**évocation de **C**ertificats) vérifiée.

Une vérification étendue de certificat est effectuée pour les certificats suivants :

- Pour les certificats fournis lors de la création d'un responsable principal de la sécurité. Seuls les certificats qui réussissent la vérification complète sont affichés.
- Pour les certificats créés après qu'une clé de récupération a été utilisée pour assigner un nouveau certificat à un responsable de la sécurité. Seuls les certificats qui réussissent la vérification complète sont affichés.
- Pour les certificats utilisés par les responsables de la sécurité pour se connecter à la base de données d'*u.trust LAN Crypt*. Si les certificats ne peuvent pas être vérifiés, l'accès est refusé.
- Pour les certificats utilisés pour des autorisations supplémentaires.

Voici les conditions préalables à la vérification étendue de certificat :

- Le certificat utilisé doit inclure une liste de révocation de certificats.

  Certaines PKI vous permettent de définir une liste de révocation de certificats dans le certificat lui-même. Si une liste de révocation de certificats a été définie, la liste est évaluée. Pour ce faire, vous devrez peut-être télécharger une liste de révocation de certificats de l'émetteur via le réseau. Si le certificat ne peut pas être vérifié, le profil de chiffrement n'est pas chargé.

- Une liste de révocation de certificats a été chargée dans le magasin de certificats local.

Remarque : Vous devez disposer d'une connexion réseau avant de pouvoir évaluer une liste de révocation de certificats. Dans le cas contraire, l'accès sera refusé, même si le certificat lui-même est valide.

2.1.3 Lecteurs de cartes à puce

Comme l'utilisation des certificats est gérée par les **C**ryptographic **S**ervice **P**roviders (CSPs) et les **K**ey **S**torage **P**roviders (KSPs), les lecteurs de cartes à puce sont automatiquement pris en charge lorsqu'un KSP pour cartes à puce est utilisé. Vous pouvez donc gérer l'accès aux informations de chiffrement en utilisant des certificats sur les cartes à puce.

Remarque : Si vous souhaitez utiliser des certificats sur des cartes à puce, assurez-vous que le lecteur de carte à puce, l'intergiciel associé et un **Fournisseur de service** ou de **stockage** (CSP ou KSP) correspondant sont correctement installés et opérationnels !

Remarque : Veuillez également noter que les **C**ryptographic **S**ervice **P**rovider (CSP) pour les opérations clés de *u.trust LAN Crypt* ne sont désormais pris en charge qu'en association avec des shims qui les rendent accessibles en tant que **K**ey **S**torage **P**rovider (KSP).

2.2 Installation

Remarque : Vous ne pouvez installer *u.trust LAN Crypt* que si vous disposez des privilèges d'administrateur Windows.

1. Accédez au répertoire d'installation de votre package d'installation décompressé et double-cliquez sur le fichier *LCAdmin.msi*.

   Un assistant d'installation vous guide lors de l'installation de l'administration *u.trust LAN Crypt*, qui est un processus très simple. Cliquez sur **Suivant**.

2. La boîte de dialogue *Contrat de licence* s'affiche.

   Dans cette boîte de dialogue Contrat de licence, sélectionnez **J'accepte le contrat de licence**. Si vous n'effectuez pas cette sélection, vous ne serez pas en mesure d'installer *u.trust LAN Crypt* ! Cliquez sur **Suivant**.

3. La boîte de dialogue *Dossier de destination* s'affiche.

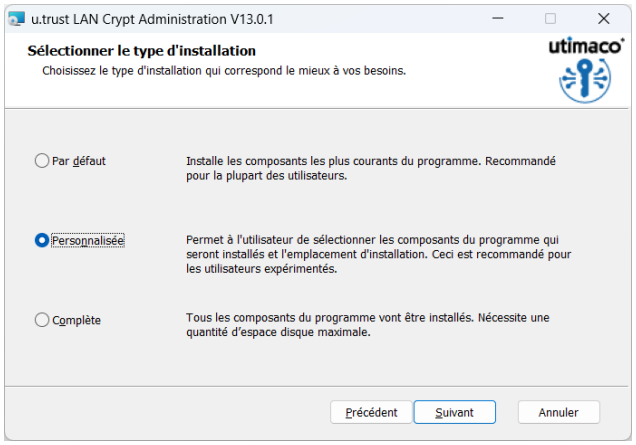
   Sélectionnez l'emplacement où vous souhaitez installer *u.trust LAN Crypt*. Si vous ne modifiez pas ce paramètre, l'installation est effectuée sous :

   ```
   <Lecteur système>:\Programmes (x86)\Utimaco\u.trust LAN Crypt\Administration
   ```

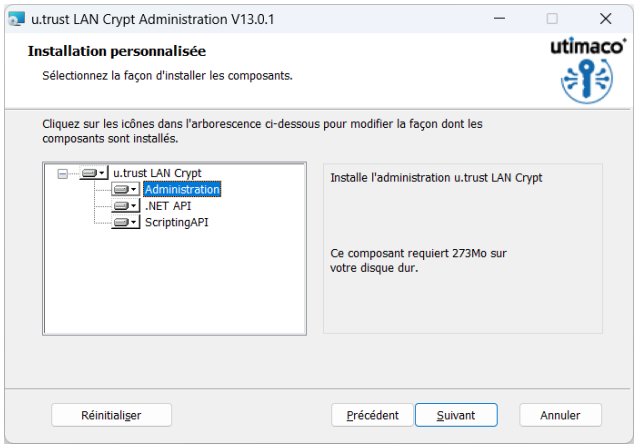
   Cliquez sur **Suivant**.

4. La boîte de dialogue Sélectionner le *type d'installation* s'affiche.

   Dans cette boîte de dialogue, vous pouvez sélectionner les composants *u.trust LAN Crypt* à installer.



Si vous choisissez **Personnalisée**, vous pouvez choisir les composants à installer :



- **Administration**

  Installe l'administration *u.trust LAN Crypt*.

- **ScriptingAPI**

  Installe le ScriptingAPI d'*u.trust LAN Crypt* requise pour utiliser les scripts afin d'administrer le produit.

  Remarque : Contrairement aux versions précédentes de *u.trust LAN Crypt* .NET API est désormais activée par défaut au lieu de ScriptingAPI lors d'une installation personnalisée.

- **.NET API**

  Installe le *u.trust LAN Crypt* .NET API nécessaire pour utiliser des scripts ou des applications basés sur .NET pour administrer le produit. De plus, des exemples de scripts sont également installés.

  Remarque : À partir de la version 13.0.0, vous pouvez installer le *u.trust LAN Crypt* .NET API sans aucune fonction ou composant supplémentaire.

  Remarque : Si vous recevez un message d'erreur lors de l'utilisation de *.NET API*, veuillez vérifier si la référence du paquet suivant est également incluse dans votre projet :

  ```
  <PackageReference Include="Microsoft.Win32.Registry" Version="5.0.0" />
  ```

Remarque : Si *u.trust LAN Crypt* Administration n'est pas installé via le paquet MSI inclus dans le dossier d'installation, mais via un installateur séparé, la clé de registre requise pour .NET API doit également être définie. Pour .NET API 32 bits, cela doit être défini comme suit :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\conpal\LAN Crypt\Admin\Setup]
"InstallDir"="C:\\Programmes (x86)\\Utimaco\\u.trust LAN Crypt\\Administration\\"
```

Pour .NET API 64 bits, cela doit être défini comme suit :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\conpal\LAN Crypt\Admin\Setup]
"InstallDir"="C:\\Programmes\\Utimaco\\u.trust LAN Crypt\\Administration\\"
```

Sous « `InstallDir` » vous devez entrer le chemin où se trouvent les DLLs de *u.trust LAN Crypt* Administration. Par défaut, il s'agit de l'un des chemins mentionnés ci-dessus.

Si vous n'avez **pas** installé *u.trust LAN Crypt* dans le chemin par défaut, veuillez noter : Si vous voulez utiliser les scripts d'exemple fournis, les chemins aux DLLs API dans les scripts doivent être ajustés de façon analogue au chemin d'installation modifié.

Remarque : Le .NET API est uniquement requis pour l'utilisation de scripts / projets cs, et non pour les scripts Powershell. Le programme d'exemple *StartFirstHere* est prédéfini par défaut pour *.NET Core 8.0*.

Remarque également : Veuillez également noter que si vous souhaitez utiliser la version **64 bits de .NET API**, une connexion **ODBC 64 bits à la base de données *LAN Crypt*** doit être établie où exister. Tous les fichiers de bibliothèque API associés (DLL) doivent être situés dans le même répertoire que l'application et doivent être trouvés via la variable d'environnement « `PATH` ».

Cela concerne les fichiers suivants :

- *LCAdminApiNetX64.dll*
- *LCNetApiX64.dll*
- *SGLCScriptApiV4.dll*
- *sglcapi.dll*
- *LCDA.dll*

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

Remarque : Si vous avez sélectionné l'option **Par défaut**, seule l'administration est installée. Si vous sélectionnez **Complète**, le *u.trust LAN Crypt* **ScriptingAPI** et le **.NET API** seront également installées.

6. Après avoir vérifié vos paramètres, cliquez sur **Installer** dans la boîte de dialogue Prêt à installer l'application. 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.

2.3 Installation sans surveillance

L'installation sans assistance signifie que vous pouvez installer *u.trust LAN Crypt* automatiquement sur un grand nombre d'ordinateurs.

Le dossier Installer contient le fichier LCAdmin.msi requis pour une installation sans surveillance.

2.3.1 Composants à installer

La liste suivante indique quels composants doivent être installés et la manière dont vous les spécifiez pour une installation sans surveillance.

Les mots-clés indiquent comment les composants individuels doivent être spécifiés sous `AddLocal=` si une installation est effectuée sans l'intervention de l'utilisateur. Les noms des mots-clés individuels pour les composants prennent en compte les majuscules et les minuscules !

`AddLocal=`**`Administration`**

Installe uniquement l'administration *u.trust LAN Crypt*.

`AddLocal=`**`Administration,ScriptApi`**

En plus de l'administration *u.trust LAN Crypt*, le ScriptingAPI est installée.

`AddLocal=`**`Aministration,AdminApiDotnet`**

En plus de l'administration *u.trust LAN Crypt*, l'AdminApi (.NET) est installée.

Exemple :

```
msiexec /i lcadmin.msi /qn AddLocal=Administration
```

Dans cet exemple, seule l'administration *u.trust LAN Crypt* est installée sans interaction utilisateur.

Remarque : Si vous ne spécifiez pas de composant, une installation complète est effectuée.

Remarque : L'installation le .NET API (AdminApiDotnet) entraîne également l'installation de scripts types. Par défaut, l'installation est effectuée pour la version 64 bits sous :

```
<Lecteur>:\Programmes\Utimaco\u.trust LAN Crypt\Administration\Admin API PowerShell Samples\
<Lecteur>:\Programmes\Utimaco\u.trust LAN Crypt\Administration\Admin API Dotnet Samples\
```

Et pour la version 32 bits sous :

```
<Lecteur>:\Programmes (x86)\Utimaco\u.trust LAN Crypt\Administration\Admin API PowerShell Samples\
<Lecteur>:\Programmes (x86)\Utimaco\u.trust LAN Crypt\Administration\Admin API Dotnet Samples\
```

Remarque : Voir également les notes complémentaires relatives à le .NET API à la page 26.

2.3.2 Syntaxe de ligne de commande

Pour effectuer une installation sans assistance, vous devez exécuter `msiexec` avec des paramètres spécifiques.

Paramètres obligatoires :

`/I`

Spécifie le package d'installation à installer.

`/QN`

Installation sans interaction utilisateur (installation sans assistance).

Nom du fichier *.msi : `lcadmin.msi`

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

Paramètres facultatifs :

`/L*xv <chemin + nom du fichier>`

Enregistre la procédure d'installation complète à l'emplacement spécifié sous <chemin + nom du fichier>.

Exemple :

`msiexec /i C:\Install\lcadmin.msi /qn /L*xv c:\Log\log.txt`

Cela effectue une installation complète d'*u.trust LAN Crypt*. Le programme est installé dans le répertoire d'installation par défaut

(`<Lecteur système>:\Programmes (x86)\Utimaco\u.trust LAN Crypt\Administration`).

Le fichier .msi se trouve dans le dossier d'*installation* du package d'installation d'*u.trust LAN Crypt*.

2.4 Mise à niveau

Pour effectuer la mise à jour de *LAN Crypt* version 4.2.0 vers la version actuelle de *u.trust LAN Crypt* Administration, vous devez d'abord passer par une mise à niveau intermédiaire vers *LAN Crypt* version 11.0.x, incluant l'installation du logiciel ainsi que la mise à jour de la base de données *LAN Crypt*. Ensuite, installez la version 13.0.1 de *u.trust LAN Crypt* Administration, puis mettez à jour la base de données existante à l'aide de l'outil en ligne de commande `CreateTables.exe`. Les étapes nécessaires à cette procédure sont expliquées plus en détail dans les pages suivantes.

Remarque : Si vous utilisez une version de *LAN Crypt* antérieure à la version 3.90, vous devez d'abord la mettre à jour vers la version 3.97, puis procéder à une mise à niveau vers la version 4.2.0 de *LAN Crypt*.

Remarque : La première connexion après la mise à niveau doit être effectuée par un responsable principal de la sécurité (MSO).

2.4.1 Mise à niveau vers la nouvelle version

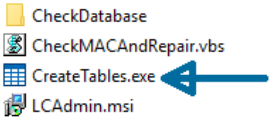
Installez la nouvelle version comme décrit précédemment.

Remarque : Assurez-vous que toutes les instances de l'administration *u.trust LAN Crypt* sont fermées avant d'installer la nouvelle version. Aucun autre responsable de la sécurité ne doit être connecté à la base de données *LAN Crypt* pendant la mise à niveau, car cela pourrait entraîner des incohérences dans la base de données !

Remarque : Veuillez noter **qu'après la mise à niveau de l'administration *LAN Crypt* à la version 13.0.0 ou supérieure, il n'est plus possible de procéder à un fonctionnement mixte avec des versions *LAN Crypt* antérieures !** Toutes les administrations *LAN Crypt* supplémentaires doivent être mises à jour en même temps. **L'accès à une base de données *LAN Crypt* antérieure n'est pas possible avec la version 13.0.x.** Une base de données antérieure doit impérativement être migrée vers la nouvelle version avant qu'un accès à celle-ci ne soit à nouveau possible avec l'administration *LAN Crypt*.

2.4.2 Mise à niveau de la structure existante de la base de données u.trust LAN Crypt

À l'aide de l'outil de ligne de commande `CreateTables.exe`, vous pouvez mettre à niveau la structure des tables dans votre base de données *u.trust LAN Crypt*. L'outil est disponible dans le dossier\Install de votre package d'installation.



Remarque : Faites une sauvegarde de votre base de données *LAN Crypt* avant la mise à niveau.

Pour la mise à niveau d'une structure de base de données *u.trust LAN Crypt* existante, Utimaco recommande de confier cette tâche à une **Administrateur informatique** ou à un **Administrateur de base de données**, car elle nécessite des autorisations avancées pour la base de données (rôle db : `db_ddladmin`). Lors de la mise à jour de la base de données par `CreateTables.exe`, de nouvelles tables doivent être créées dans la base de données de *u.trust LAN Crypt* et, entre autres, les déclencheurs DDL doivent être supprimés.

Remarque : La connexion à la base de données doit être effectuée avec des privilèges qui *permettent la création* et la *modification* du schéma de base de données. Pour les responsables de la sécurité, les rôles de base de données « `db_datareader` » et « `db_datawriter` » sont toutefois suffisants pour l'utilisation de la console d'administration *u.trust LAN Crypt*.

Remarque : Lors de la mise à niveau d'une base de données *LAN Crypt* à l'aide de l'outil en ligne de commande *`CreateTables.exe`* sur des bases de données SQL gérées par Oracle, les vues « *ADMLOGINVIEW* », « *USERGROUPVIEW* », « *GROUPRULEVIEW* » et « *ADMINLISTVIEW* » sont supprimées puis recréées. Les utilisateurs se connectant à la base de données *LAN Crypt* via ODBC peuvent alors ne plus disposer des privilèges SELECT nécessaires pour ces vues. Ces privilèges doivent ensuite être réattribués aux utilisateurs concernés par le propriétaire de la base de données ou un administrateur de base de données (DBA).

Remarque : Dans le contexte d'Oracle, lors de la réplication de la base de données *LAN Crypt* par l'administrateur, il est impératif de veiller à ce **qu'aucun trigger** ne soit exécuté dans la base de données cible. Pour ce faire, il est recommandé d'effectuer la réplication de la base de données avec *Oracle Golden Gate* et de configurer le paramètre *DBOPTIONS* avec le flag *SURPRESSTRIGGERS* (ce qui correspond au paramètre par défaut). Pour plus d'informations à ce sujet, consultez :

https://docs.oracle.com/en/middleware/goldengate/core/21.3/reference/dboptions.html#GUID-BA8C0CED-D87F-4106-862E-4AD22D910160

Syntaxe de ligne de commande :

```
CreateTables <Nom ODBC[.Nom du propriétaire]> <Dialecte SQL> <Actions>
```

CreateTables.exe fournit les paramètres suivants pour 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 soit correctement adressée, le propriétaire de la base de données doit être spécifié pour les bases de données Oracle. Le propriétaire doit être indiqué en MAJUSCULES. Si le schéma par défaut de votre serveur Microsoft SQL ne correspond pas à « *.dbo* », vous devez également indiquer le propriétaire de la base de données « *.dbo* » pour les bases de données Microsoft SQL.

Dialecte SQL :

m… Microsoft SQL Server 2022 ou 2025 (y compris Express)

o19 … Oracle version 19 ou plus récente

Actions :

u … Mise à jour de la structure de la base de données

Exemple 1 :

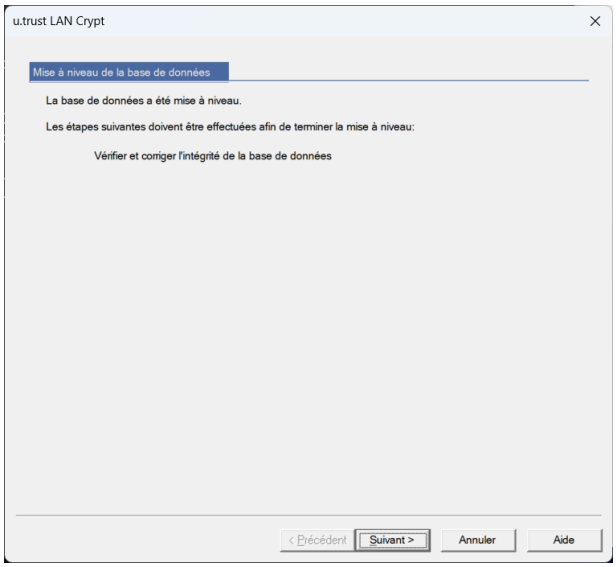
```
CreateTables SGLCSQLServer.dbo m u
```

Exemple 2 :

```
CreateTables SGLCSQLServer.SGLC o19 u
```

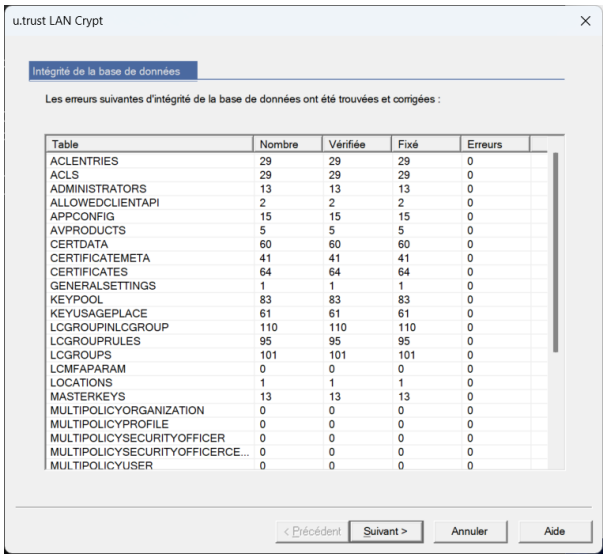
2.4.3 Assistant de mise à niveau

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.

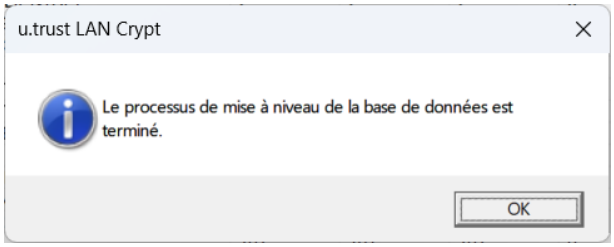


Remarque : Seul un responsable principal de la sécurité peut procéder à la première connexion après la mise à niveau de l'administration. Si vous ne possédez pas les droits appropriés, un message s'affiche.

L'assistant de mise à niveau vérifie l'intégrité de la base de données *LAN Crypt* et effectue les dépannages nécessaires. Il affiche ensuite des informations sur les erreurs corrigées et recommande des actions supplémentaires.

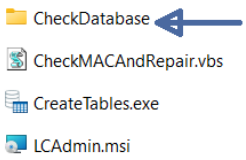


Une fois l'assistant terminé, vous pouvez utiliser l'administration.



2.4.4 Vérifier et réparer l'intégrité de la base de données

L'outil de ligne de commande `CheckDatabase.exe` vous permet de vérifier à tout moment l'intégrité de la base de données de *u.trust LAN Crypt* et, si nécessaire, de corriger les erreurs. Vous trouverez cet outil dans le dossier *\Install* de votre package d'installation *u.trust LAN Crypt*.



Remarque : Vous trouverez une description détaillée de l'outil de ligne de commande *CheckDatabase.exe* en anglais à l'adresse suivante : https://help.lancrypt.com/docs/admin/additional-documentation/CheckDatabaseTool/en/.

2.5 Paramètres de langue

L'administration *u.trust LAN Crypt* prend actuellement en charge les langues suivantes :

- Français
- Anglais
- Allemand
- Japonais

Le paramètre de langue de *u.trust LAN Crypt* dépend du paramètre de langue Windows actuellement défini. Si les langues ne sont pas prises en charge, *u.trust LAN Crypt* affiche les boîtes de dialogue en anglais par défaut.

Vous pouvez également définir vous-même la langue de *u.trust LAN Crypt*. Pour ce faire, apportez les modifications suivantes dans le registre de l'ordinateur sur lequel *u.trust LAN Crypt* Administration est installé dans la ruche mentionnée ci-dessous :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Utimaco\SGLANG]
```

```
"LCID"=dword:0x40C
```

pour la langue française

```
"LCID"=dword:0x0409
```

pour la langue anglaise (États-Unis)

```
"LCID"=dword:0x0407
```

pour la langue allemande

```
"LCID"=dword:0x0411
```

pour la langue japonaise

Après cela, redémarrez l'ordinateur.

La langue définie manuellement pour *u.trust LAN Crypt* est conservée, même si une langue différente est définie dans Windows ou si elle est modifiée.

2.6 Désinstallation

Remarque : Vous ne pouvez désinstaller *u.trust LAN Crypt* que si vous disposez des privilèges d'administrateur Windows.

1. Sélectionnez **Démarrer**, **Paramètres**, **Applications**.
2. Sélectionnez **Administration u.trust LAN Crypt** dans la liste des programmes installés.
3. Cliquez sur **Désinstaller** pour désinstaller l'administration *u.trust LAN Crypt*.
4. Si vous voulez vraiment désinstaller l'administration *u.trust LAN Crypt*, confirmez le message d'avertissement qui s'affiche en cliquant sur **OK**.
5. **Redémarrez** le système pour terminer le processus de désinstallation.

Remarque : Lors de la désinstallation d'*u.trust LAN Crypt*, le contenu de la base de données d'*u.trust LAN Crypt* est conservé. Si nécessaire, la base de données doit être supprimée séparément à l'aide des outils du système d'exploitation ou de l'outil d'administration de base de données. De plus, tous les paramètres spécifiques à l'utilisateur sont conservés sur le système (clés de Registre, paramètres de stratégie de groupe, etc.).

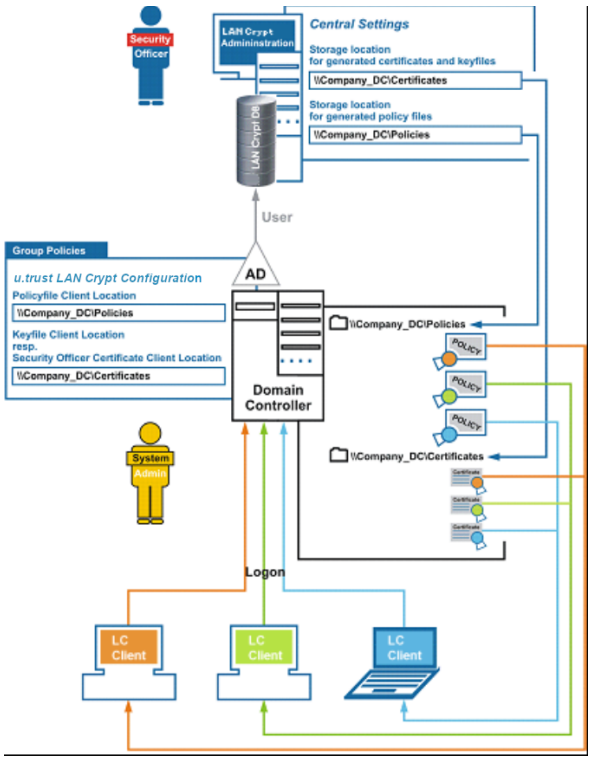
3 Administration

L'administration *u.trust LAN Crypt* s'intègre parfaitement dans la console de gestion (MMC) de Microsoft et offre à un responsable sécurité une interface utilisateur digne de confiance avec des fonctionnalités MMC typiques.

La console d'administration a été développée pour permettre aux utilisateurs de bénéficier des outils de réplication Windows existants. Cela permet non seulement d'atteindre des niveaux d'efficacité élevés, mais aussi de réduire les coûts totaux de possession (TCO). En effet, les clients qui possèdent un parc de stations de travail étendu ne souhaitent généralement implémenter qu'un seul système pour l'administrer.

La console d'administration d'*u.trust LAN Crypt* est généralement installée sur une machine séparée, à partir de laquelle les services d'annuaires requis et la base de données *u.trust LAN Crypt* sont accessibles.

u.trust LAN Crypt utilise le concept de responsables de la sécurité. Au départ, un responsable principal de la sécurité installe la console d'administration. Lors de l'installation, le responsable principal de la sécurité doit spécifier l'emplacement où seront enregistrés les certificats et fichiers clés (la partie publique du certificat du responsable de la sécurité et les fichiers *.p12 contenant les certificats utilisateur qui doivent être importés sur les machines clientes) générés pour les utilisateurs. Après l'installation, vous devez indiquer l'emplacement d'enregistrement des fichiers de stratégie générés pour les utilisateurs. Des fichiers de stratégie contenant les règles de chiffrement sont générés pour chaque utilisateur.



Les certificats, les fichiers *.p12 et les fichiers de stratégie sont automatiquement importés par les clients à partir de l'emplacement de stockage spécifié à un moment ultérieur.

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

Les clients peuvent utiliser des 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 de configuration *u.trust LAN Crypt*. *u.trust LAN Crypt* est configuré dans l'objet de stratégie de groupe valide pour les utilisateurs.

Les clients de *u.trust LAN Crypt* n'ont pas besoin de se connecter à la base de données *u.trust LAN Crypt*.

Les informations requises pour trouver des certificats, des fichiers *.p12 et des fichiers de stratégie peuvent être obtenues à l'ouverture de session dans les stratégies de groupe. Ces fichiers sont ensuite automatiquement transférés aux clients.

Pour importer son certificat, un utilisateur doit avoir un mot de passe. Dans le cas de certificats générés par *u.trust LAN Crypt*, le fichier *p12pwlog.csv* contient les mots de passe et peut être utilisé, par exemple, pour créer une lettre PIN (par exemple « *LCSendP12Password* »).

3.1 Étapes requises

Préparatifs :

- Facultatif : Installation du SGBD (Microsoft ou Oracle). Création d'une nouvelle base de données « *LANCRYPT* ». Les bases de données ajoutées au système de gestion de base de données (SGBD) ne doivent pas être utilisées pour *u.trust LAN Crypt* !
- Ajoutez une source de données (ODBC 32 bits) en tant que système DSN (consultez le section 3.2.2).
- Créez des tables de base de données avec `CreateTables` (ou étendez-les lors d'une mise à niveau).
- **Administrateur système** : Définissez les paramètres dans la console de configuration d'*u.trust LAN Crypt*.
- Créez le responsable sécurité principal initial.
- Définissez les emplacements de stockage dans la console d'administration :
  - pour les fichiers de clés d'utilisateur et les certificats de responsable de la sécurité générés par *u.trust LAN Crypt*
  - pour les fichiers de clés de responsable de la sécurité générés par *u.trust LAN Crypt*
  - pour le fichier journal des mots de passe des mots de passe générés automatiquement des fichiers de clés (uniquement si les certificats sont générés par *u.trust LAN Crypt*).
  - pour les fichiers de stratégie générés par *u.trust LAN Crypt* (veuillez contacter l'administrateur système pour mettre en œuvre ces étapes)

Remarque : Si vous utilisez une base de données Oracle et accédez à la base de données à partir de consoles d'administration sur différentes machines, vous devez maintenant également spécifier les paramètres de la page de code (voir « *Onglet Base de données* » à la page 78).

- Créer des responsables (principaux) de la sécurité supplémentaires
- Définir les droits des responsables de la sécurité
- Importer des objets (unités d'organisation, groupes, utilisateurs) à partir du service d'annuaire (par exemple Active Directory)
- Créer des groupes *u.trust LAN Crypt* et les remplir avec les objets importés depuis le service d'annuaire (utilisateurs, groupes)
- Assigner les groupes *u.trust LAN Crypt* et le responsable de la sécurité en charge aux différentes unités d'organisation ou régions, et définir leurs droits
- Créer des clés
- Créer des règles de chiffrement

  Remarque : Nous recommandons de définir des règles de chiffrement uniquement dans les groupes *u.trust LAN Crypt*. Les règles de chiffrement dans les objets répertoires directement importés représentent un risque de sécurité et sont également sujettes aux erreurs.
- Générer et attribuer des certificats pour les utilisateurs
- Générer des fichiers de stratégie pour les utilisateurs

3.2 Préparatifs pour l'administration d'u.trust LAN Crypt

Après l'installation, vous devez suivre les étapes suivantes avant de pouvoir commencer à administrer *u.trust LAN Crypt* :

- Facultatif : installer le système de gestion de base de données

Ceci n'est nécessaire que si votre système de base de données ne comprend pas une base de données que vous souhaitez utiliser pour administrer *u.trust LAN Crypt*.

u.trust LAN Crypt prend en charge les systèmes de base de données suivants :

- Microsoft SQL Server 2022 ou 2025 (y compris Express)
- Oracle 19 ou version plus récente

  Remarque : Si vous utilisez une base de données Oracle, vous devez installer le client Oracle avant de pouvoir utiliser l'administration *u.trust LAN Crypt*. Si vous sélectionnez la variante « runtime » du client Oracle, vous devez également installer le pilote Oracle ODBC.

  ***u.trust LAN Crypt* ne prend pas en charge Microsoft ODBC pour Oracle.**

  Assurez-vous de ne pas utiliser les mots-clés réservés par le fabricant lorsque vous générez des objets de base de données.

- Spécification d'une source de données (ODBC)

  Si vous souhaitez utiliser votre propre système de base de données, vous devez connaître les identifiants d'accès de la base de données que vous souhaitez utiliser afin de pouvoir spécifier la source de données.

- Création de tables de base de données

  Après avoir spécifié la source de données, vous devez créer les tables *u.trust LAN Crypt* dans la base de données à l'aide de l'outil fourni avec votre logiciel (`CreateTables.exe`).

  Dialecte SQL :

  m ... Microsoft SQL Server 2022 ou 2025 (y compris Express)

  o19 ... Oracle 19 ou version plus récente

  Actions :

  c ... Créer toutes les tables

  Exemple 1 :

  ```
  CreateTables SGLCSQLServer.dbo m c
  ```

  Exemple 2 :

  ```
  CreateTables SGLCSQLServer.SGLC o19 c
  ```

3.2.1 Installation du système de base de données

La description suivante se réfère à Microsoft SQL Server 2022 Express Edition. Pour cet exemple de description, les paramètres par défaut de cette version ont été utilisés autant que possible.

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

1. Téléchargez une version récente de Microsoft SQL Server Express (par exemple Microsoft SQL Server 2022 Express) à partir du site web de Microsoft. Ensuite, double-cliquez sur le fichier d'installation dans le dossier de téléchargement. Pour Microsoft SQL Server 2022 Express, il s'agit de *SQL2022-SSEI-Expr.exe*.
2. Acceptez le contrat de licence, puis 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 les paramètres par défaut.

   Paramètres par défaut : La description suivante des étapes préparatoires fait référence aux paramètres par défaut. Si vous apportez des modifications (méthode d'authentification, instance de base de données), vous devez en tenir compte lors de la spécification de la source de données et de la création des tables de base de données.

   Authentification de la base de données : Par défaut, Express Edition utilise l'authentification Windows. Une condition préalable à l'utilisation de l'authentification Windows est que l'utilisateur qui se connecte à la base de données dispose des droits d'administrateur Windows.

Base de données master : La base de données principale est utilisée par défaut au moment de spécifier la source de données. En général, nous vous recommandons de **ne PAS utiliser la base de données principale** car cela peut causer des problèmes lors de la mise à niveau de Express Edition ou de la version SQL Server.

Vous pouvez créer une base de données séparée pour *u.trust LAN Crypt* et la spécifier au moment d'ajouter la source de données. Pour Microsoft SQL Server 2022 Express Edition, vous pouvez créer une base de données en utilisant la commande suivante sur la ligne de commande :

```
osql -E -S .\SQLEXPRESS -Q "CRÉER BASE DE DONNÉES <nome_de_la_base_de_données>"
```

Une base de données avec le nom spécifié à l'aide de l'authentification Windows est créée.

Avec le paramètre `-U`, par exemple, vous pouvez spécifier un nom d'utilisateur pour l'authentification. Pour voir tous les paramètres, tapez `osql -?`.

Vous pouvez également utiliser une autre version de Microsoft SQL Server Express (*u.trust LAN Crypt* version 13.0.1 prend en charge Microsoft SQL Server Express à partir de la version 2022).

Vous pouvez également télécharger Microsoft SQL Server Management Studio Express, qui est disponible gratuitement, et l'utiliser pour créer une base de données séparée.

Au cours de l'étape suivante, une source de données doit être spécifiée afin *qu'u.trust LAN Crypt* puisse utiliser le système de base de données.

3.2.2 Ajouter une source de données (ODBC)

Remarque : La source de données doit être ajoutée avec l'administrateur de la source de données ODBC 32 bits, qui est également disponible sur les systèmes 64 bits. Démarrez l'administrateur de la source de données ODBC en cliquant sur *Démarrer\u.trust LAN Crypt Administration\ODBC Data Source Administrator (x86)*. Cela garantit que la bonne version est lancée.

Spécifiez une source de données afin qu'*u.trust LAN Crypt* puisse utiliser la base de données via le système de gestion des données. Pour ce faire, utilisez l'administrateur de la source de données ODBC.

ODBC (Open Database Connectivity) permet d'accéder aux données sur une grande variété de systèmes de gestion de bases de données. Par exemple, si vous disposez d'un programme pour accéder aux données d'une base de données SQL, ODBC vous permet d'utiliser le même programme pour accéder aux données d'une autre base de données. Pour ce faire, vous devez ajouter des « pilotes » au système. ODBC vous assiste lorsque vous ajoutez et configurez ces pilotes.

Pour ajouter une source de données :

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

2. Sélectionnez l'**onglet DSN système** et cliquez sur **Ajouter...**.

   Une liste apparaît, à laquelle vous pouvez ajouter des sources de données, chacune avec son propre système DSN (nom de la source de données système). Ces sources de données sont enregistrées localement sur un ordinateur mais ne sont pas attribuées à un utilisateur particulier : tout utilisateur disposant des droits appropriés peut utiliser un DSN système.

3. Sélectionnez **SQL Server** comme pilote pour lequel vous souhaitez créer la source de données et cliquez sur **Terminer**.

   Remarque : Si *SQL-Server Native Client* est disponible dans la liste, sélectionnez cette entrée. Pour sécuriser la connexion entre l'administration *u.trust LAN Crypt* et SQL Server, nous vous recommandons d'utiliser « *ODBC Driver 17 pour SQL-Server* » ou une version plus récente. Ce pilote permet le chiffrement de la connexion avec TLS 1.2 et offre ainsi une sécurité accrue. Un téléchargement est possible via : https://go.microsoft.com/fwlink/?linkid=2120137

4. Une boîte de dialogue apparaît. Saisissez-y le nom **SGLCSQLServer** pour référencer la source de données.

   Configurez le nom de référence de la source de données dans la configuration d'*u.trust LAN Crypt*. Le paramètre par défaut est **SGLCSQLServer**. Si vous souhaitez utiliser un nom différent, saisissez-le dans la configuration.

Remarque : Le nom de la source ODBC est sensible à la casse ! Ici, vous devez saisir les noms exactement de la même manière qu'ils ont été spécifiés dans la configuration d'*u.trust LAN Crypt*. Vous devez saisir les noms dans la configuration avant d'exécuter pour la première fois la console d'administration *u.trust LAN Crypt*.

5. Dans le champ *Serveur*, sélectionnez le serveur que vous souhaitez utiliser pour établir la connexion, puis cliquez sur **Suivant**.

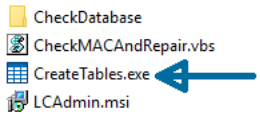
6. Acceptez les paramètres par défaut dans la boîte de dialogue suivante. Si vous acceptez l'option **Avec l'authentification Windows NT utilisant l'identificateur de connexion réseau**, vous spécifiez que les données utilisateur Windows doivent être utilisées pour vous connecter au système de base de données. Vous n'avez pas besoin de saisir de mot de passe. Cliquez sur **Suivant**.

7. Choisissez comme base de données par défaut (par exemple *LANCrypt*) celle que vous avez créée pour *u.trust LAN Crypt* et confirmez-la.

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

3.2.3 Créer des tables dans la base de données u.trust LAN Crypt

À l'aide de l'outil en ligne de commande `CreateTables.exe`, vous pouvez créer les tables requises dans votre base de données *u.trust LAN Crypt*. L'outil est disponible dans le répertoire « Install » de votre package d'installation décompressé.



Remarque : La connexion à la base de données doit être effectuée avec des privilèges qui permettent de créer et de modifier le schéma de la base de données.

Pour créer le tableau dans votre base de données, procédez comme suit :

1.) Saisissez ce qui suit sur la ligne de commande : `CreateTables SGLCSQLServer.dbo 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 l'administration *u.trust LAN Crypt*.

3.2.3.1 Syntaxe de la ligne de commande CreateTables

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

`CreateTables.exe` propose les paramètres suivants pour créer les tables dans différentes configurations :

Nom ODBC :

Le nom que vous avez utilisé pour la source de données ODBC.

Nom du propriétaire

Pour que la base de données soit correctement adressée, le propriétaire de la base de données doit être spécifié pour les bases de données Oracle. Le propriétaire doit être indiqué en MAJUSCULES. Si le schéma par défaut de votre serveur Microsoft SQL ne correspond pas à « *.dbo* », vous devez également indiquer le propriétaire de la base de données « *.dbo* » pour les bases de données Microsoft SQL.

Dialecte SQL :

m… Microsoft SQL Server

o19 … Oracle 19 ou version plus récente

Actions :

c ... Créer toutes les tables

Exemple 1 (uniquement pour une nouvelle installation) :

```
CreateTables SGLCSQLServer.dbo m c
CreateTables SGLCSQLServer.SGLC o19 c
```

Exemple 2 (uniquement en cas de mise à niveau) :

```
CreateTables SGLCSQLServer.dbo m u
CreateTables SGLCSQLServer.SGLC o19 u
```

3.3 Responsables de la sécurité principaux

u.trust LAN Crypt utilise le concept de responsables de la sécurité. Au départ, il y a un seul responsable de la sécurité principal. Celui-ci peut déléguer des tâches par la suite en créant des responsables de la sécurité supplémentaires et en leur attribuant des droits spécifiques pour l'administration *u.trust LAN Crypt*. Le tout premier responsable de la sécurité principal peut même créer des responsables de la sécurité principaux supplémentaires.

Les listes de contrôle d'accès permettent de définir les droits attribués aux responsables de la sécurité créés par un responsable de la sécurité principal. Les responsables sécurité peuvent ensuite être affectés à différentes unités d'organisation de l'administration centrale. Leurs droits s'appliquent alors exclusivement à l'unité d'organisation à laquelle ils ont été affectés. Ces droits sont hérités vers le bas dans la hiérarchie organisationnelle jusqu'à ce que d'autres droits soient attribués.

Une fois que vous avez configuré le système de base de données et la source de données, vous pouvez passer à l'étape suivante. Celle-ci consiste à créer un responsable sécurité principal initial lorsque la console d'administration d'*u.trust LAN Crypt* s'exécute pour la première fois.

Un responsable principal de la sécurité dispose toujours de tous les droits existants.

Remarque : Lors de la création du responsable principal de la sécurité initial, vous devez également définir l'emplacement de stockage des certificats et fichiers clés générées par *u.trust LAN Crypt*. La partie publique du certificat du responsable de la sécurité (*.cer), dont

les clients ont besoin, y est également stockée. Les certificats utilisateur (fichiers *.p12) sont également importés à partir de ce répertoire à un moment ultérieur. Le dossier que vous avez défini avec l'administrateur système doit déjà être disponible (partage réseau).

Tous les paramètres définis lors de la création du responsable principal de la sécurité initial peuvent être modifiés à un moment ultérieur sous **Paramètres centraux** dans la console d'administration d'*u.trust LAN Crypt*.

3.3.1 Responsable de la sécurité principal initial

Une fois la fonctionnalité Administration exécutée pour la première fois (*Démarrer, u.trust LAN Crypt, Administration*) et la connexion à la base de données effectuée, l'assistant de création du responsable de la sécurité principal initial apparaît.

Saisissez les données du responsable de la sécurité principal initial. Si vous utilisez des certificats générés par *u.trust LAN Crypt*, le nom que vous saisissez ici est utilisé comme nom courant dans le certificat. *L'adresse électronique* et les *commentaires* sont facultatifs. Cliquez sur **Suivant**.

Remarque : L'adresse électronique est ajoutée au *fichier journal du mot de passe* pour les certificats générés par *u.trust LAN Crypt*. Il peut par exemple être utilisé pour créer une lettre PIN par courriel (ex : avec « *LCSendP12Password* »).

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

- Les certificats générés (*.cer) et les fichiers clés (*.p12)
- Les certificats des responsables de la sécurité générés et
- Le fichier journal pour les mots de passe générés automatiquement des fichiers clés générés.

Emplacement de stockage pour les certificats et les fichiers clés générés

u.trust LAN Crypt peut générer des certificats auto-signés si nécessaire. Les fichiers clés (*.p12) générés pour les utilisateurs contiennent ainsi les clés privées et les certificats. Ceux-ci sont générés au moment d'attribuer des certificats aux utilisateurs. L'emplacement de stockage associé doit être spécifié dans la deuxième boîte de dialogue de l'assistant. En général, c'est via un partage de connexion que ces fichiers sont mis à la disposition des utilisateurs.

La partie publique du certificat du responsable de la sécurité (*.cer) est également enregistrée ici.

Les utilisateurs doivent recevoir leurs fichiers clés ou certificats (*.p12), les fichiers de stratégie et la partie publique du certificat (*.cer) du responsable de la sécurité qui a créé et signé les certificats utilisateur.

Ceci est fait pour configurer le client *u.trust LAN Crypt* en utilisant des stratégies de groupe ou des paramètres de registre (si aucun Active Directory n'est disponible ou ne doit pas être utilisé pour des raisons de sécurité). Avec ces paramètres, le client obtient les chemins d'accès appropriés. Nous recommandons l'utilisation de chemins UNC et de noms FQD (par exemple « \\fileserver1.lancrypt.intern\partage\lcpolicies »).

Si un fichier « *.cer » correspondant et qui contient la clé publique du certificat du responsable de la sécurité est trouvé, il est automatiquement importé.

Remarque : Pour utiliser la fonctionnalité décrite, les chemins correspondants doivent être définis dans la configuration d'*u.trust LAN Crypt*.

Les fichiers clés des utilisateurs et la partie publique du certificat du responsable de la sécurité peuvent également être distribués manuellement. Dans ce cas, assurez-vous que les deux sont importés par les clients.

Remarque : Le certificat public du responsable de la sécurité qui a créé les dossiers de stratégie doit toujours être importé par les clients.

Si vous modifiez le chemin d'accès sur lequel sont stockés les certificats publics (*.cer) des responsables de la sécurité et les fichiers clés (*.p12) des utilisateurs, par exemple après avoir créé des responsables de la sécurité supplémentaires, vous devez copier ces fichiers vers le nouvel emplacement. Dans le cas contraire, les clients *u.trust LAN Crypt* ne trouveront pas la partie publique des certificats des responsables de la sécurité. Les fichiers clés des utilisateurs doivent également être générés sous le nouveau chemin.

Emplacement de stockage pour les certificats générés des responsables de la sécurité

u.trust LAN Crypt stocke les certificats des responsables de la sécurité dans des fichiers *.p12, par exemple, en tant que sauvegardes. Ici, vous pouvez spécifier le dossier dans lequel ils sont enregistrés.

Remarque : Étant donné qu'ils contiennent des données sensibles, il est essentiel que vous les protégiez contre tout accès non autorisé.

Fichier pour le journal des mots de passe

L'emplacement de stockage et le nom du fichier journal des mots de passe des fichiers PKCS#12 générés peuvent être spécifiés ici (nom par défaut : *p12pwlog.csv*). Ce fichier contient les mots de passe des fichiers de clés PKCS#12 générés (*.p12). Cela peut également être utilisé pour créer, par exemple, une lettre PIN (ex : avec « *LCSendP12Password* »).

Remarque : Vous devez protéger ce fichier et en aucun cas l'enregistrer dans le même dossier que les fichiers de stratégie.

Grâce à *u.trust LAN Crypt*, vous pouvez facilement protéger le fichier journal des mots de passe. Pour ce faire, installez les composants Administration et Client sur le même ordinateur. Une fois que vous avez créé le responsable de la sécurité principal initial, créez une règle de chiffrement qui chiffre le fichier journal des mots de passe. Générez ensuite un profil pour le responsable de la sécurité principal initial et chargez-le. L'accès à la clé de chiffrement utilisée doit être réservé aux responsables de la sécurité principaux et aux responsables de la sécurité qui ont le droit de créer des certificats.

Remarque : Si vous installez les composants *Console d'administration* et *Application client* d'*u.trust LAN Crypt* sur le même ordinateur, ils doivent avoir la même version.

L'exécution de l'assistant de chiffrement initial chiffrera le fichier journal du mot de passe. Pour s'assurer que le mot de passe du responsable principal de la sécurité initial n'a pas été compromis alors que le fichier n'était pas chiffré, créez un nouveau certificat et attribuez-le au responsable principal de la sécurité initial.

Remarque : Si le responsable de la sécurité qui attribue les certificats n'a pas le droit du système de fichiers de modifier le fichier journal du mot de passe, *u.trust LAN Crypt* ne sera pas en mesure de générer des certificats.

Cliquez sur **Suivant**.

Validité du certificat

Dans la troisième boîte de dialogue de l'assistant, spécifiez la période de validité des certificats générés par *u.trust LAN Crypt* et attribuez un certificat existant, ou un certificat généré par *u.trust LAN Crypt*, au responsable de la sécurité.

Si vous utilisez un certificat généré par *u.trust LAN Crypt*, celui-ci est valide pour la période spécifiée. Tous les certificats générés après celui-ci ont également cette période de validité.

Le certificat initial du responsable de la sécurité

Vous devez sélectionner un certificat de chiffrement qui sera utilisé pour sécuriser les données du responsable de la sécurité. Vous pouvez également sélectionner un certificat de signature que le responsable de la sécurité peut utiliser pour s'authentifier auprès de l'administration *u.trust LAN Crypt*. Si vous ne spécifiez pas de certificat de signature, le certificat de chiffrement sera également utilisé comme moyen d'authentification.

Cliquez sur le bouton **Parcourir** (« **…** ») pour sélectionner un certificat existant ou pour qu'*u.trust LAN Crypt* en génère un nouveau. Dans la boîte de dialogue suivante, cliquez sur **Nouveau certificat**. Sélectionnez le nouveau certificat dans la liste et cliquez sur **OK**.

Remarque : Si vous souhaitez utiliser un certificat existant, ce certificat doit être disponible. Si vous utilisez un certificat logiciel, il doit être chargé dans le magasin de certificats. Si le certificat est enregistré sur un jeton, le jeton doit être attaché au système. Pour importer un certificat, cliquez sur **Importer un certificat**.

Cliquez sur **Suivant**.

Dans la quatrième boîte de dialogue de l'assistant, vous pouvez entrer une région avec le préfixe approprié. Lorsqu'*u.trust LAN Crypt* génère la clé, il joint 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 administrative la clé doit être utilisée. Dans les **Paramètres centraux** de la console d'administration, vous pouvez créer des régions supplémentaires, puis les affecter aux différents responsables de la sécurité. Cette procédure est particulièrement utile dans les environnements distribués.

Vous devez spécifier un emplacement. Dans les bases de données distribuées, l'emplacement est utilisé pour attribuer clairement les événements enregistrés dans la base de données *u.trust LAN Crypt*.

Vous devez spécifier l'emplacement même si vous n'utilisez pas de base de données distribuée. Cela garantit que les entrées peuvent être clairement attribuées lorsque la base de données sera distribuée plus tard.

Lorsque vous cliquez sur **Terminer**, *u.trust LAN Crypt* crée le fichier du responsable principal de la sécurité et affiche la boîte de dialogue de connexion pour l'administration *u.trust LAN Crypt*.

Plus tard, tous les responsables de la sécurité qui ont le droit de se connecter à la base de données de l'administration *u.trust LAN Crypt* seront affichés dans cette boîte de dialogue.

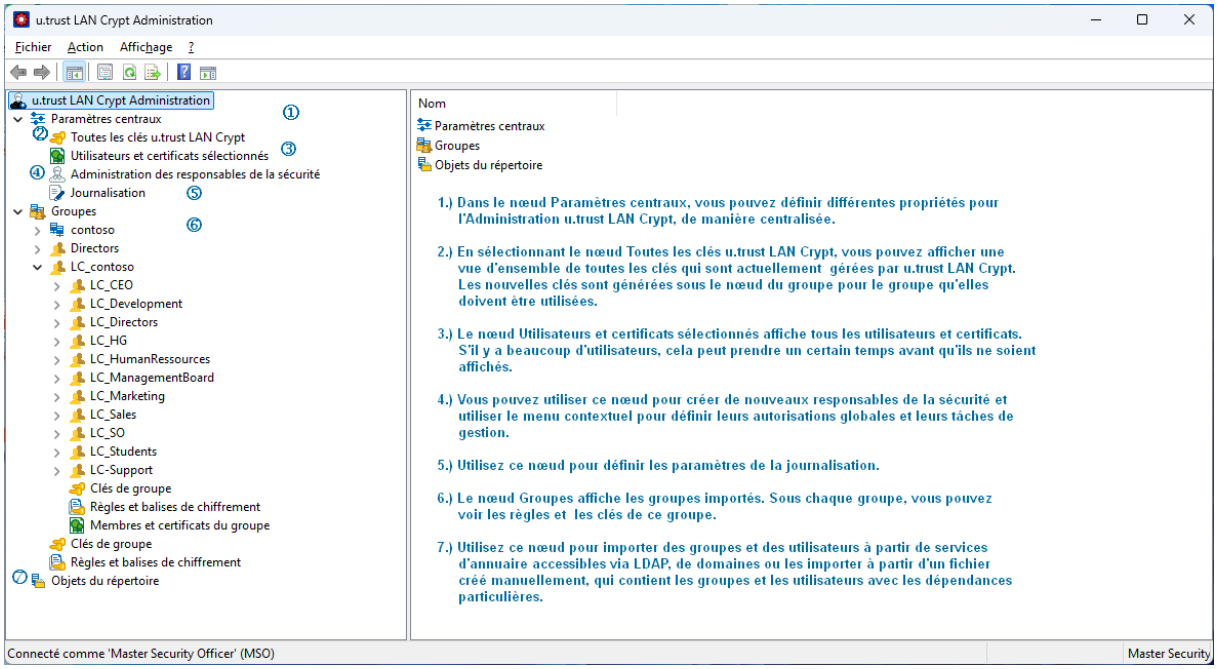
Dans cette boîte de dialogue, sélectionnez le responsable principal de la sécurité nouvellement créé et cliquez sur **OK**. La console d'administration d'*u.trust LAN Crypt* s'ouvre.

Remarque : Une fois que vous vous êtes connecté, une boîte de dialogue apparaît pour vous indiquer qu'une clé de récupération n'a pas encore été générée. Si vous n'avez pas de clé de récupération, il y a un risque que toutes vos données administratives et toutes les données chiffrées soient perdues en cas d'urgence (par exemple si vous perdez un certificat).

Cette boîte de dialogue apparaît chaque fois qu'un responsable principal de la sécurité se connecte, et ce, jusqu'à ce qu'une clé de récupération soit générée. Activez l'option **Ne plus afficher ce message** pour empêcher cette boîte de dialogue d'apparaître, même si aucune clé de récupération n'a été générée. **Pour éviter une éventuelle perte de données, vous devez générer une clé de récupération.**

3.4 Administration : vue d'ensemble

Une fois *u.trust LAN Crypt* installé, le fichier **SGLCAdmin.msc** est enregistré dans le dossier d'installation d'*u.trust LAN Crypt*. Cliquez sur cette entrée via le menu Démarrer de Windows (*Démarrer/u.trust LAN Crypt Administration/Administration*) pour ouvrir une fenêtre dans la console de gestion qui affiche uniquement les composants logiciels enfichables requis pour la console d'administration d'*u.trust LAN Crypt*.



Vous pouvez également ajouter le snap-in de la console d'administration d'*u.trust LAN Crypt* à la vue normale de la console de gestion (Fichier / Ajouter / Retirer le composant logiciel enfichable - Administration *u.trust LAN Crypt*). Même lorsque vous ajoutez le composant logiciel enfichable, vous avez toujours besoin du mot de passe pour la base de données de l'administration *u.trust LAN Crypt*.

Qui est connecté ?

La barre de statut indique quel responsable de la sécurité est actuellement connecté. Vous pouvez également voir s'il s'agit d'un responsable principal de la sécurité ou d'un responsable de la sécurité.

Barre d'outils de la console d'administration

De nombreuses fonctionnalités *u.trust LAN Crypt* apparaissent sous forme d'icônes dans la barre d'outils de la console d'administration. La fonctionnalité et le nombre d'icônes dans la barre d'outils dépendent de l'onglet sélectionné à un moment donné.

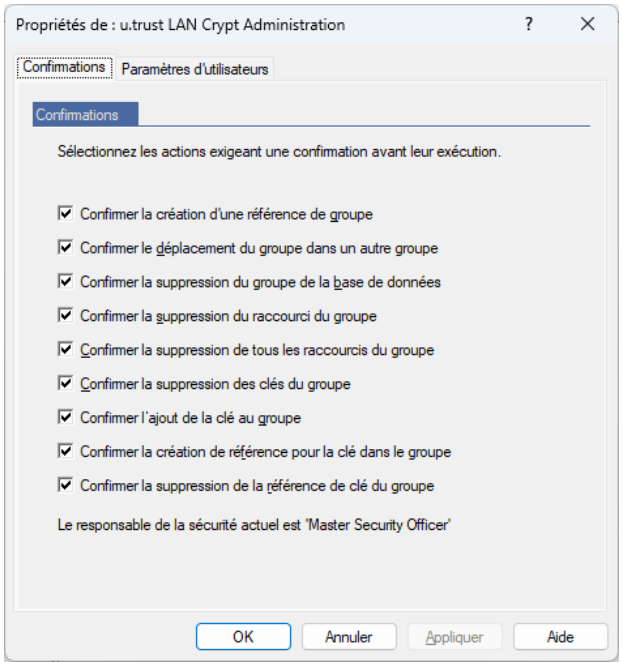
Vous pouvez également sélectionner toutes les fonctionnalités qui apparaissent sous la forme de ces icônes dans le menu contextuel correspondant.

Faites un clic droit sur l'onglet de **l'administration u.trust LAN Crypt** 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 d'administration d'*u.trust LAN Crypt*, vous pouvez spécifier les actions qui doivent être confirmées avant l'exécution. Pour ce faire, cliquez sur **Propriétés** dans le menu contextuel du nœud racine de l'administration **u.trust LAN Crypt**.

La boîte de dialogue suivante affiche ces actions :



Si vous sélectionnez une action, vous devez confirmer que vous souhaitez l'exécuter avant qu'elle ne soit exécutée. L'action n'est pas effectuée tant que vous ne l'avez pas confirmée.

Vous pouvez définir ce paramètre pour les actions suivantes :

- **Confirmer la création d'une référence à un groupe**

  La création d'une référence à un groupe existant doit être confirmée. Sélectionner groupe > clic droit > Copier > Sélectionner autre groupe > clic droit > Coller > Confirmation.

  Remarque : Toutes les opérations de Copier, Couper et Coller peuvent être effectuées soit en utilisant le menu contextuel, soit en utilisant la fonction *Glisser-Déposer* ou *Glisser-Déposer* + *CTRL*.

- **Confirmer le déplacement du groupe vers un autre groupe**

  Le déplacement d'un groupe vers un autre groupe doit être confirmé.

- **Confirmer la suppression du groupe de la base de données**

  La suppression d'un groupe doit être confirmée.

- **Confirmer la suppression du raccourci du groupe**

  La suppression d'une référence à un groupe doit être confirmée.

- **Confirmer la suppression de tous les raccourcis du groupe**

  S'il y a une référence à un groupe dans un autre groupe, par exemple dans les groupes 1 et 2, il y a un lien vers le groupe 3, la suppression de cette référence doit être confirmée (sélectionnez Groupe 3 > clic droit > **Supprimer les liens**).

- **Confirmer la suppression des clés du groupe**

  Il est nécessaire de confirmer la suppression de clés ayant été utilisées dans une règle de chiffrement et désactivées par la suite. Les clés utilisées sont marquées dans l'administration et résident également dans la base de données 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 elles sont supprimées d'un groupe.

- **Confirmer l'ajout de la clé au groupe**

  Les clés ayant été utilisées dans une règle de chiffrement et supprimées de tous les groupes résident dans la base de données et sont affichées sous le nœud **Paramètres centraux** / **Toutes les clés u.trust LAN Crypt**. De là, elles peuvent être réassignées à un groupe via *Glisser-Déposer*. Cette action doit être confirmée.

- **Confirmer la création de référence pour la clé dans le groupe**

  L'insertion d'un lien vers une clé dans un groupe (par exemple en la faisant glisser d'un groupe à un autre) doit être confirmée. Les clés sont toujours copiées, ou un lien redirigeant vers elles est inséré. Couper les clés n'est pas possible.

- **Confirmer la suppression de la référence de clé du groupe**

  La suppression d'un lien vers une clé d'un groupe doit être confirmée.

Quel est le responsable de la sécurité qui est connecté ?

Cette boîte de dialogue indique également quel responsable de la sécurité est actuellement connecté. Le nom du responsable de la sécurité s'affiche au bas de la boîte de dialogue. La barre de statut de l'administration *u.trust LAN Crypt* indique également quel est le responsable de la sécurité actuellement connecté.

3.4.2 Paramètres d'utilisateur

L'onglet **Paramètres d'utilisateur** vous permet d'influer sur la façon dont les informations apparaissent dans l'administration *u.trust LAN Crypt*.

Activer

- *Ajouter le nom du domaine à chaque nom de groupe* pour afficher la relation entre les groupes et domaines *u.trust LAN Crypt* dans l'administration *u.trust LAN Crypt*. Cette option est particulièrement utile si *u.trust LAN Crypt* doit être utilisé pour plusieurs domaines différents.
- *Afficher les utilisateurs et les certificats sélectionnés* pour afficher tous les utilisateurs (et leurs certificats) importés dans *u.trust LAN Crypt* sous le nœud Paramètres centraux.

  Remarque : Sachez qu'il faudra plusieurs minutes pour afficher tous les utilisateurs et certificats dans des installations plus grandes. Vous devez ensuite redémarrer l'administration *u.trust LAN Crypt* afin que les modifications apportées dans l'option *Afficher les utilisateurs et certificats sélectionnés* deviennent effectives.

- *Afficher les parents des utilisateurs* pour afficher le groupe parent d'un utilisateur particulier sous le nœud Membres et certificats du groupe. Cela vous permet de voir en un coup d'œil si la base de données *u.trust LAN Crypt* contient des utilisateurs qui ne sont assignés à aucun groupe. Vous devez ensuite redémarrer l'administration *u.trust LAN Crypt* pour que les modifications apportées à l'option Afficher les parents des utilisateurs deviennent effectives.
- Désactiver la mise en cache des listes utilisateur

  Pour améliorer les performances, *u.trust LAN Crypt* crée généralement des listes utilisateur en arrière-plan, et continue à les créer lorsqu'un utilisateur bascule vers un nœud différent dans Administration. Les résultats de ces listes sont mis en mémoire tampon de sorte qu'aucun accès à la base de données n'est nécessaire lorsque la liste est appelée à nouveau. Cela offre un gain de temps conséquent en cas de travail avec des listes volumineuses.

  Cependant, dans les environnements comportant plusieurs administrateurs *u.trust LAN Crypt* parallèles (serveurs Terminal Server), cela peut entraîner des besoins en mémoire accrus. Pour éviter cela, il suffit d'activer cette option. Il en résulte que les listes ne sont pas mises en mémoire tampon. La création de la liste ne se poursuit donc pas lorsque l'utilisateur quitte le nœud ou passe à un nœud différent. Nous vous recommandons de n'utiliser cette option que si vous rencontrez réellement des problèmes de capacité mémoire.

Les modifications apportées à la base de données au cours de la même session ne sont pas automatiquement transférées dans une liste.

Vous pouvez mettre à jour les modifications 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 enregistrés pour chaque utilisateur dans le composant logiciel enfichable Microsoft Management Console.

3.5 Paramètres centraux

Le nœud **Paramètres centraux** vous permet de définir différentes propriétés pour l'administration *u.trust LAN Crypt* de manière centralisée.

Pour ce faire, cliquez sur *Propriétés* dans le menu contextuel du nœud **Paramètres centraux**. Vous pouvez également sélectionner cela et cliquer sur l'icône « *Propriétés* » dans la barre d'outils de l'administration *u.trust LAN Crypt*. Vous pouvez ensuite afficher ces propriétés dans plusieurs onglets et les modifier si nécessaire.

Remarque : Seuls les responsables principaux de la sécurité peuvent afficher les onglets **Autorisation supplémentaire**, **Clé de récupération** et **Régions**. Seuls les responsables de la sécurité disposant de l'autorisation globale *Modifier la configuration* peuvent afficher les onglets **Serveur** et **Configuration**. L'autorisation globale *Modifier la configuration* est également requise pour modifier les chemins dans l'onglet **Répertoires**. Seuls les responsables principaux de la sécurité peuvent apporter des modifications dans les onglets **Algorithme**, **Certificats** et **Résolution des règles**.

3.5.1 Onglet Algorithme

u.trust LAN Crypt propose les algorithmes de chiffrement suivants :

- **AES-128**
- **AES-256**
- **3DES** (non recommandé)
- **DES** (non recommandé)
- **IDEA** (non recommandé)
- **XOR** (non recommandé)

Sélectionnez les algorithmes que vous souhaitez utiliser. Les algorithmes que vous sélectionnez ici peuvent être utilisés plus tard, lorsque vous générez des clés différentes.

Remarque : La modification ultérieure de ces paramètres (par exemple si 3DES est supprimé de la liste des algorithmes disponibles) n'affecte aucune des clés déjà générées ni aucune des données chiffrées avec elles. Un algorithme affecté n'est tout simplement pas disponible lors de la génération ultérieure d'une autre clé. Si vous sélectionnez des algorithmes qui ne sont plus considérés comme sécurisés, vous recevrez un avis de sécurité correspondant. Vous pouvez toujours choisir ces algorithmes.

Algorithme par défaut

Ici, vous sélectionnez l'algorithme par défaut à utiliser pour générer automatiquement des clés utilisateur et de groupe. **AES**, avec une **longueur de clé de 256** ou **128 bits**, est recommandé comme algorithme standard parce qu'il offre le niveau de sécurité le plus élevé.

3.5.2 Onglet Clés

Des problèmes avec des noms de clés internes dupliqués peuvent survenir lorsque plusieurs installations d'*u.trust LAN Crypt* sont combinées en une seule, par exemple en raison d'une fusion d'entreprise ou de département.

Pour cette raison, chaque clé est identifiée par son propre *identificateur global unique (GUID)*. Le GUID est habituellement généré de manière aléatoire par *u.trust LAN Crypt* et ne peut pas être modifié par la suite.

Cependant, si des fichiers ayant été chiffrés avec *u.trust LAN Crypt* doivent être échangés entre deux entreprises, vous aurez besoin d'une méthode qui vous permet de générer une clé commune.

C'est le seul moyen de s'assurer qu'un fichier chiffré avec, par exemple, la clé `CRYPTOKEY` de la société « A », peut être déchiffré par la société « B ». Pour que cela soit possible, la société « B » doit également générer une clé appelée `CRYPTOKEY`, dotée des mêmes paramètres que celle de la société « A ». Cela affecte également le GUID de la clé et l'algorithme de chiffrement.

Pour gérer cette situation, *u.trust LAN Crypt* dispose d'une option qui vous permet de saisir manuellement le GUID lorsque vous générez une nouvelle clé. Pour ce faire, il suffit d'activer l'option **Autoriser les responsables de la sécurité à définir le GUID des nouvelles clés (GUID aléatoire par défaut)**.

Remarque : d'autres possibilités de partage de clés existent également via *LC2Go* (voir section 3.15.1 « Importation de clés Lc2Go » à la page 138) ou via l'API *u.trust LAN Crypt* à l'aide de la nouvelle fonction « *Multi-policy support* ».

Remarque : Ce paramètre ne peut être modifié que par un responsable principal de la sécurité.

Valeur de la clé

En activant l'option **Autoriser les responsables de la sécurité à définir le GUID des nouvelles clés (GUID aléatoire par défaut)**, vous pouvez vous assurer que seuls les responsables de la sécurité dotés des autorisations globales *Créer des clés* et *Créer des profils* peuvent générer des clés (nom et valeur). Si le responsable de la sécurité n'assigne pas de valeur à la clé lors de sa création, la valeur est générée automatiquement lorsque la clé est enregistrée.

Si cette option est activée, les responsables de la sécurité ne disposant pas du droit *Créer des profils* ne peuvent pas générer de clés.

Ces responsables de la sécurité ne peuvent pas non plus utiliser de clés de groupe (<GROUPKEY>) dans les règles de chiffrement.

Remarque : Si un responsable de la sécurité ne doit générer que des clés, mais pas de profils, vous pouvez le configurer dans les autorisations des groupes respectifs (voir section 3.11.3 « *Accorder au responsable de la sécurité des autorisations pour traiter les groupes* » à la page 123.

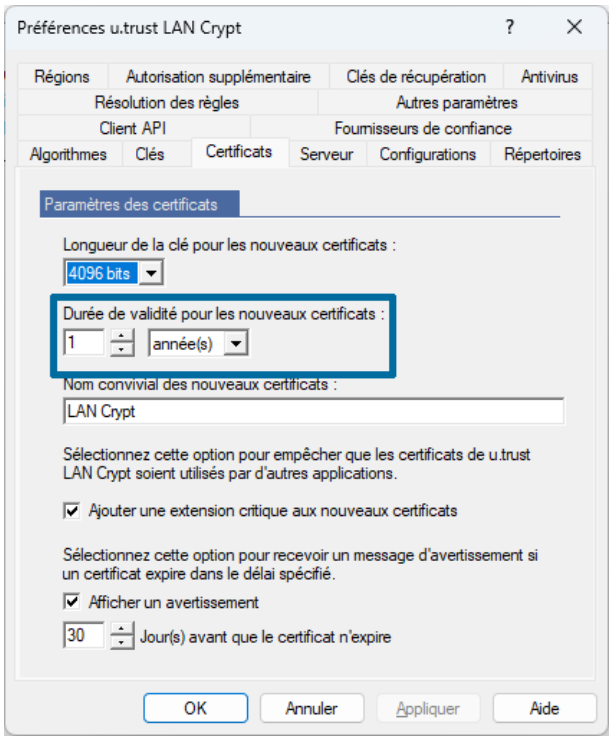
Concernant les clés de groupe, dont les valeurs sont générées lors de la génération de fichiers de stratégie, les valeurs sont également générées immédiatement lorsqu'elles sont utilisées pour créer une règle de chiffrement.

Remarque : L'option **Autoriser les responsables de la sécurité à définir le GUID des nouvelles clés (GUID aléatoire par défaut)** n'affecte pas l'utilisation des clés spécifiques à l'utilisateur (<USERKEY>) dans les règles de chiffrement.

Remarque : En principe, *u.trust LAN Crypt* offre également la possibilité de créer des clés sans valeur. De telles clés peuvent être utilisées dans l'administration sans restriction. Cependant, cela peut causer des problèmes avec les bases de données distribuées. La génération de fichiers de stratégie dans une fenêtre de délai de réplication à différents emplacements contenant des clés sans valeur (clés créées manuellement sans valeur, clé de groupe <GROUPKEY>) constitue un exemple d'utilisation d'une référence à une clé. Lors de la génération des fichiers de stratégie, une valeur de clé distincte est donc générée à chaque emplacement. Il en résulte donc une clé avec deux valeurs différentes.

3.5.3 Onglet Certificats

Ici, vous pouvez spécifier la longueur de clé (1 024, 2 048, 4 096 bits) et la validité des nouveaux certificats générés par *u.trust LAN Crypt*. Une durée de validité de 1 an est prédéfinie pour les certificats générés par u.trust LAN Crypt. Vous pouvez modifier cette valeur à tout moment.



Remarque : vous pouvez définir la durée de validité des certificats nouvellement créés entre 1 jour et 999 ans maximum. Dans l'intérêt de la sécurité de l'information, la durée de validité ne devrait toutefois pas dépasser 5 ans dans la mesure du possible. Pour les certificats CA (**C**ertificate **A**uthority), Utimaco recommande en revanche une durée de validité maximale de 20 ans.

Remarque : Pour les certificats attribués au responsable de la sécurité, la période de validité ne doit pas dépasser l'année 3100.

Sous *Nom convivial des nouveaux certificats*, vous pouvez indiquer un nom pour les certificats créés par *u.trust LAN Crypt*. Tous les certificats reçoivent ce nom et peuvent donc être facilement identifiés comme des *certificats* u.trust LAN Crypt.

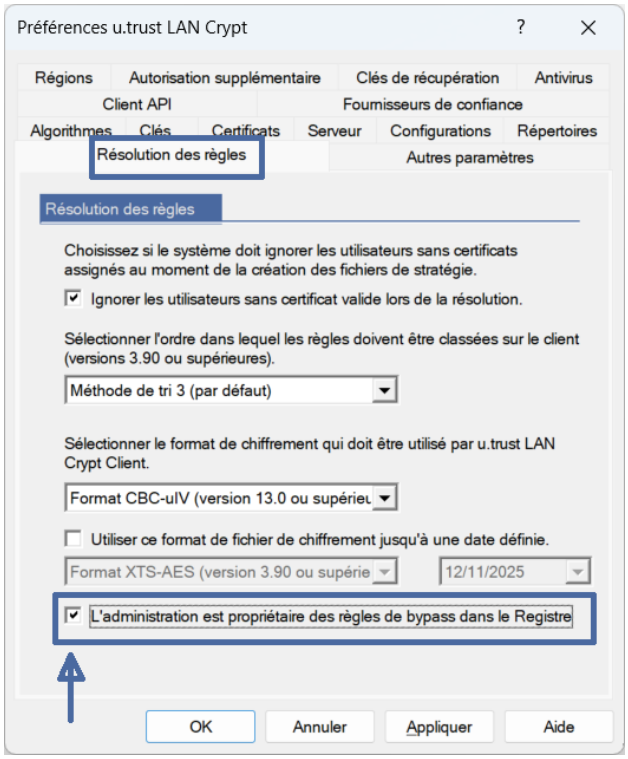
Si vous activez l'option **Ajouter des extensions critiques aux nouveaux certificats**, une extension critique indiquant à d'autres applications qu'elles ne doivent pas utiliser ces certificats est ajoutée aux nouveaux certificats.

Vous pouvez également spécifier une période d'avertissement, en jours, durant laquelle le système affiche un avertissement (si les règles sont annulées, ou en marquant les certificats en jaune dans la liste). Par exemple, si vous saisissez 30 jours ici, un message d'avertissement s'affiche environ un mois avant l'expiration du certificat. Ce message indique que le certificat ne sera bientôt plus valide et qu'il doit être renouvelé.

3.5.4 Onglet Résolution des règles

Ignorer les utilisateurs sans certificat valide lors de la résolution

Sélectionnez cette option si vous souhaitez que le système ignore les utilisateurs auxquels aucun certificat n'a été assigné lors de la génération des fichiers de stratégie. Par conséquent, aucun fichier de stratégie n'est généré pour ces utilisateurs.



Remarque : Si un utilisateur est créé, que cette option est sélectionnée et qu'aucun certificat n'a encore été assigné à l'utilisateur, le système n'affiche pas d'avertissement s'il n'est pas en mesure de créer des fichiers de stratégie pour cet utilisateur lors de la résolution (application) des règles de chiffrement.

Sélectionnez la méthode de tri des règles sur le client :

Remarque : Ce paramètre n'est appliqué qu'aux clients des versions 3.90 ou ultérieure.

Ici, vous pouvez choisir parmi trois méthodes de tri différentes. La *méthode de tri 3* est la méthode par défaut utilisée par les versions du client antérieures à la version 3.90. La méthode de tri ne pouvait pas être modifiée dans les versions précédentes de LAN Crypt, et correspondait à la méthode de tri 3. La méthode de tri 3 est donc considérée comme la méthode de tri par défaut.

Les méthodes de tri suivantes peuvent être définies :

- **Méthode de tri 1**

  1. Règles Ignorer
  2. Règles d'exclusion
  3. Règles de chiffrement

- **Méthode de tri 2**

  1. Règles Ignorer
  2. Règles d'exclusion
  3. Règles de chiffrement spécifiées comme chemins d'accès absolus sans caractères génériques
  4. Règles de chiffrement spécifiées comme chemins d'accès absolus avec caractères génériques excluant les sous-dossiers
  5. Règles de chiffrement spécifiées comme chemins d'accès absolus avec caractères génériques incluant les sous-dossiers
  6. Toutes les autres règles de chiffrement

  Un chemin d'accès absolu est soit un chemin UNC (qui commence par une double barre oblique inversée), soit une <lettre de lecteur>:\

  Exemples d'utilisation d'une référence à une clé :

  `\\server\share\*.*` ou

  `c:\confidential\*.*`

- **Méthode de tri 3 (par défaut)**

  La *méthode de tri 3* ne fait pas de distinction entre les règles Ignorer, d'exclusion et de chiffrement.

  Les règles sont classées dans l'ordre suivant :

  1. Tous les chemins d'accès absolus sans caractères génériques
  2. Tous les chemins d'accès absolus avec caractères génériques excluant les sous-dossiers
  3. Tous les chemins d'accès absolus avec caractères génériques incluant les sous-dossiers
  4. Toutes les autres règles

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

  L'ordre est le suivant :

  1. Chemins UNC.
  2. Chemins commençant par *<lettre de lecteur>:* Ici, la barre oblique inversée après la lettre de lecteur n'est pas prise en compte.
  3. Tous les autres chemins.

     En outre :

     - Les chemins avec plus de barres obliques inversées sont répertoriés avant les chemins qui en comportent moins.

     - Les chemins sans caractères génériques sont répertoriés avant les chemins contenant des caractères génériques *. et *.*.

Remarque : Les modifications apportées à cette option deviennent effectives sur les clients une fois les nouveaux profils générés et distribués.

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

Ici, vous pouvez configurer le mode de chiffrement de fichier utilisé par les clients. *u.trust LAN Crypt* prend en charge les modes de chiffrement suivants :

- Format CBC (version 3.50 ou supérieure)

  Ce format est utilisé par les versions 3.50 et supérieures des clients. Ces clients peuvent lire des fichiers chiffrés en mode OFB (format hérité). 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 supérieures des clients. Ces clients peuvent lire des fichiers chiffrés en mode OFB et CBC. Le mode de chiffrement des nouveaux fichiers est XTS-AES. Ce mode ne sera utilisé que pour les clés AES. Si un fichier est chiffré avec une clé utilisant un autre algorithme, le mode de chiffrement CBC est utilisé à la place.

- Format CBC-uIV (versions 13.0.0 ou supérieure)

  Ce format peut être utilisé par les clients *u.trust LAN Crypt* à partir de la version 13.0.0 ou supérieure. Ces clients peuvent lire les fichiers chiffrés en mode OFB, CBC et XTS-AES. Pour les nouveaux fichiers, le mode de chiffrement CBC-uIV est utilisé. Afin d'augmenter la sécurité de CBC, le format uIV (**u**npredictable **I**nitialization **V**ector) utilise un vecteur d'initialisation aléatoire et donc imprévisible.

Remarque : Vous pouvez vérifier quels fichiers ont déjà été chiffrés avec le nouveau format *CBC-uIV* à l'aide de l'outil en ligne de commande `encstatus.exe`. L'outil en ligne de commande est situé dans le dossier d'installation du paquet extrait *u.trust LAN Crypt* Admin.

Vous pouvez vérifier le mode de chiffrement à l'aide de la ligne de commande `encstatus.exe` comme suit :

Exemple : Si vous souhaitez vérifier, par exemple, si des fichiers du dossier « `HR` » sur le lecteur local « `C:` » sont déjà chiffrés avec le nouveau format *CBC-uIV*, ouvrez l'invite de commande sur votre ordinateur, accédez au dossier contenant l'outil en ligne de commande `encstatus.exe`, puis saisissez la commande suivante :

```
ENCSTATUS C:\HR /CNM /DCP /XM CBC-uIV /XM CBC /F /S
```

Remarque : Pour obtenir une description des différents paramètres de `encstatus.exe`, tapez `encstatus -h` dans la ligne de commande.

Pour les versions de clients antérieures à 3.90, seule la configuration suivante est valide :

Format CBC pour le chiffrement avec l'utilisation facultative de l'ancien format comme « ancien format de chiffrement ». Tous les autres paramètres sont ignorés par ces clients. Ils utilisent le format CBC ou le format hérité par défaut.

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

Au cours d'un processus de mise à niveau, un ancien mode de chiffrement peut être configuré. Cet ancien mode de chiffrement est actif jusqu'à une date spécifiée. À partir de cette date, tous les clients doivent être migrés pour prendre en charge le mode de chiffrage de fichier configuré. Sinon, les nouveaux clients créent des fichiers chiffrés en utilisant le mode configuré, mais ces fichiers ne peuvent pas être lus par les anciens clients.

Selon le paramètre du format de chiffrement à utiliser, les formats suivants peuvent être sélectionnés ici :

- **Format hérité (versions 2.x, 3.0x, 3.1x)**
- **Le format CBC (version 3.50 ou supérieure)** n'est disponible que si XTS-AES est configuré comme format de fichier de chiffrement. CBC exige une version client 3.50 ou supérieure.
- Le format **XTS-AES (versions 3.90 ou supérieures)** n'est disponible que si CBC-uIV est configuré comme format de chiffrement. XTS-AES requiert une version du client *LAN Crypt* supérieure ou égale à 3.90. Ce mode n'est utilisé que pour les clés AES.

  Les clients plus anciens évaluent le **format de fichier Utiliser ce chiffrement jusqu'à** un paramètre de date défini uniquement, si le format hérité est sélectionné.

  Vous devez spécifier la date jusqu'à laquelle l'ancien format est utilisé pour chiffrer les fichiers. Après cette date, ou si l'option est effacée, les fichiers sont écrits avec le nouveau format de chiffrement. Toute modification de cette option n'est effective sur les clients qu'après la génération et la distribution de nouveaux profils.

  Une fois que tous les clients ont été mis à jour, nous vous recommandons d'effectuer le chiffrement initial avec l'*outil de chiffrement initial*. Vous vous assurez ainsi que seul le nouveau format de chiffrement *u.trust LAN Crypt* est utilisé.

  Ce changement entre en vigueur la prochaine fois que les règles de chiffrement sont résolues.

  Remarque : Veuillez noter que tous les fichiers créés avec l'ancien mode de chiffrement OFB ne peuvent être lus qu'avec *LAN Crypt* version 4.0.0. Lors de l'enregistrement ou de l'écriture de nouveaux fichiers, le mode de chiffrement le plus récent est automatiquement utilisé. En général, Utimaco recommande d'encoder tous les fichiers qui sont encore chiffrés avec le mode de chiffrement OFB obsolète vers (AES) XTS en utilisant le chiffrement initial.

  Remarque : Les anciennes versions du client *LAN Crypt* ne prennent pas en charge le format CBC-uIV. Avant le chiffrement dans le nouveau format CBC-uIV, il est impératif de mettre à jour tous les anciens clients *LAN Crypt* vers la version actuelle. Les versions actuelles de *u.trust LAN Crypt* pour macOS, iOS et Android sont également compatibles avec le nouveau format CBC-uIV.

L'administration est propriétaire des règles de bypass dans le Registre

Les règles de *bypass* sont utilisées pour désactiver les fonctions essentielles de *u.trust LAN Crypt* dans des scénarios spéciaux (voir « *Bypass* » à la page 156). L'activation de cette fonction de bypass concerne tous les clients. La fonction de bypass n'est disponible pour les règles via le *u.trust LAN Crypt* Administration que si l'option **L'administration est propriétaire des règles de bypass dans le Registre** est activée.

AVERTISSEMENT : Veuillez noter qu'une extrême prudence est requise ici ! **Des réglages incorrects pourraient, entre autres, conduire à des fichiers endommagés (corrompus).** Par conséquent, la mise en œuvre de telles règles est critique et ne devrait être faite qu'en coordination avec le support de Utimaco.

Remarque : Ce paramètre ne peut être modifié que par un responsable principal de la sécurité.

Remarque : Si des règles de *bypass* étaient déjà définies par d'autres moyens via la stratégie de groupe ou le registre, cette nouvelle fonction les écraserait où les supprimerait.

Remarque : Les variables d'environnement ne sont pas prises en charge dans les règles de *bypass*.

Remarque : La désactivation de cette fonction ne peut être effectuée qu'après avoir supprimé toutes les règles de *bypass* de la configuration afin d'éviter tout conflit avec d'autres règles.

3.5.5 Onglet Serveur

Pour importer des groupes et des utilisateurs à partir d'un serveur, *u.trust LAN Crypt* nécessite les identifiants de connexion pour ce serveur. Vous devez saisir ces informations dans l'onglet **Serveur**. Cliquez sur **Ajouter** pour ouvrir une autre boîte de dialogue, qui comporte trois onglets : *Détails*, *Préférences* et *Certificats*.

Informations du serveur : Mot de passe de connexion

1. Entrez le *nom de domaine* ou de *serveur*, le *nom d'utilisateur* et le *mot de passe* approprié. Pour éviter les doublons, veuillez également saisir un autre nom en tant qu'*alias* pour le serveur dans le cas où plusieurs noms peuvent être utilisés pour accéder au même serveur.

   Si vous utilisez un **service d'annuaires Microsoft**, procédez comme suit :

   - Entrez le nom de domaine sous *nom de domaine ou de serveur*.
   - Entrez le *nom de l'utilisateur* comme nom d'utilisateur@domaine.

     Remarque : Le nom de l'utilisateur doit être entré dans la syntaxe LDAP (nom canonique) pour importer des objets à partir d'un service d'annuaire non Microsoft. Exemple : cn=admin,ou=techops

2. Spécifiez l'API à utiliser.

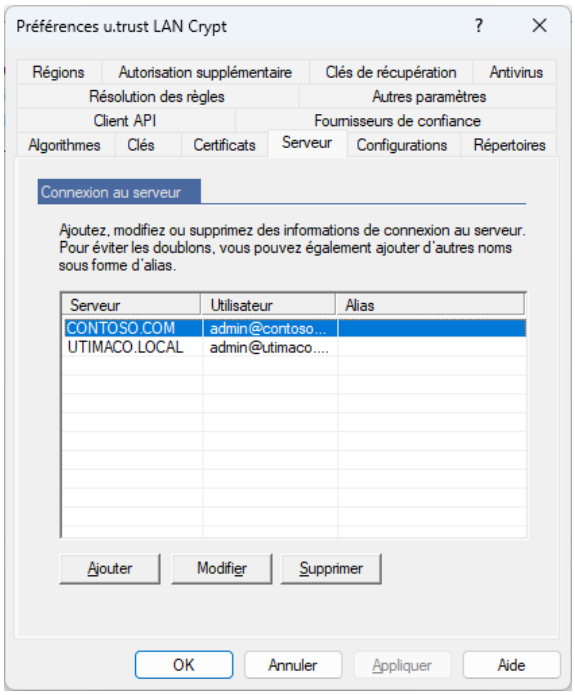
   Sélectionner *<Microsoft>* ou *<Novell>* dans la liste déroulante. L'espace réservé *<Novell>* correspond à toutes les API non Microsoft.

   Remarque : L'importation depuis le service d'annuaire de Novell n'est plus supportée depuis la version 3.90 de *LAN Crypt*. D'autres fonctionnalités de Novell ne sont plus supportées et ne sont pas fonctionnelles dans l'administration.

3. Spécifiez la méthode d'authentification LDAP à utiliser pour accéder au serveur. *u.trust LAN Crypt* propose les méthodes suivantes :
   - Mot de passe (LDAP)
   - Mot de passe (LDAP avec SSL)

4. Cliquez sur **OK**.

Le serveur est affiché dans le *tableau* de l'onglet **Serveur**.



Message d'erreur en cas d'échec de la connexion

Si *u.trust LAN Crypt* ne peut pas effectuer la connexion au serveur avec succès, un message d'erreur s'affichera dans l'administration *u.trust LAN Crypt*.

Informations du serveur : Connexion anonyme

1. Saisissez le *nom du serveur*. Pour éviter les doublons, veuillez également saisir un autre nom en tant qu'*alias* pour le serveur dans le cas où plusieurs noms peuvent être utilisés pour accéder au même serveur.

2. Spécifiez l'API à utiliser.

   Sélectionner *<Microsoft>* ou *<Novell>* dans la liste déroulante. L'espace réservé *<Novell>* correspond à toutes les API non Microsoft.

   Remarque : L'importation depuis le service d'annuaire de Novell n'est plus supportée depuis la version 3.90 de *LAN Crypt*. D'autres fonctionnalités de Novell ne sont plus supportées et ne sont pas fonctionnelles dans l'administration.

3. Spécifiez la méthode d'authentification LDAP à utiliser pour accéder au serveur. *u.trust LAN Crypt* propose ces méthodes pour une connexion anonyme :

   - Anonyme (LDAP)
   - Anonyme (LDAP avec SSL)

4. Cliquez sur **OK**.

Le serveur est affiché dans le tableau de l'onglet Serveur.

Message d'erreur en cas d'échec de la connexion

Si *u.trust LAN Crypt* ne peut pas effectuer la connexion au serveur avec succès, un message d'erreur s'affichera dans l'administration *u.trust LAN Crypt*.

Préférences

Identification d'un objet

u.trust LAN Crypt utilise un GUID (identificateur global unique) précis et immuable pour identifier les objets importés dans l'Active Directory. Ce GUID est également utilisé pour synchroniser la base de données et le service d'annuaire, car par exemple, les noms des objets individuels peuvent changer, pour s'assurer que les mises à jour dans l'Active Directory sont reflétées dans la base de données, et qu'aucun nouvel objet n'est généré dans la base de données en raison d'un changement de nom dans l'Active Directory.

Cependant, certains autres services d'annuaire n'utilisent pas ce type d'ID. Dans ce cas *u.trust LAN Crypt* propose une autre façon d'identifier les objets sans ambiguïté. *u.trust LAN Crypt* peut être configuré de sorte que certains attributs LDAP soient utilisés pour identifier les objets de manière unique. Vous configurez ces attributs dans l'administration *u.trust LAN Crypt*.

Les paramètres *<par défaut>* et *<autre>* sont toujours disponibles. De manière générale, le paramètre *<par défaut>* sera suffisant pour le serveur auquel le paramètre se réfère. Les attributs évalués par le paramètre *<par défaut>* apparaissent toujours en-dessous de *<par défaut>*. De cette façon, vous pouvez montrer quels attributs sont évalués dans le paramètre par défaut. Vous

pouvez également attribuer un attribut spécifique si tous ces attributs sont déjà présents dans le service d'annuaire concerné. Utiliser <*autre*> permet de spécifier un attribut autre que ceux qui sont déjà affichés.

Avertissement : Si vous entrez un attribut ici, assurez-vous qu'il contient des données qui identifieront l'objet sans ambiguïté.

- **GUID de l'objet**

  Ici, vous spécifiez quel attribut est utilisé pour l'identification. Si vous laissez le paramètre sur <*par défaut*>, les deux attributs, GUID et objectGUID sont évalués.

  Si vous souhaitez utiliser un autre attribut LDAP pour identifier les objets, sélectionnez <*autre*> sous objectGUID et saisissez le nom de l'attribut LDAP dans le champ de saisie à côté. Cet attribut doit contenir des données qui identifieront sans ambiguïté l'objet.

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

  Cette option n'affecte que la façon dont le GUID apparaît dans les boîtes de dialogue *Propriétés* de l'objet. Pour les afficher correctement, activez cette option si le GUID que vous utilisez à une valeur binaire. Si vous ne savez pas quoi faire, activez cette option.

Attributs pour les utilisateurs

- **Attribut le nom d'utilisateur :**

  Ce paramètre n'affecte que l'affichage des utilisateurs dans la console d'administration d'*u.trust LAN Crypt*. 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 l'un des attributs existants ou saisir un attribut LDAP en sélectionnant <*autre*>. <*par défaut*> évalue (CN et SN).

- **Attribut de nom de connexion :**

  Il s'agit d'une signification spéciale qui attachée à l'attribut pour l'*identifiant de connexion*. *u.trust LAN Crypt* nomme les fichiers de stratégie d'après l'*identifiant de connexion* de l'utilisateur. Un utilisateur ne peut se connecter que si son *identifiant de connexion* et le nom de son fichier de stratégie sont identiques.

  Ici, vous pouvez spécifier quel attribut LDAP est utilisé pour définir l'*identifiant de connexion* de l'utilisateur.

  <*par défaut*> évalue *nomComteSAM*, *utilisateurPrincipal* 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 d'ouverture de session de l'utilisateur.

  Sélectionnez <*autre*> pour spécifier un autre attribut de service d'annuaire qui contient le nom d'ouverture de session.

  Remarque : Si le nom dans l'attribut contient le caractère @, *u.trust LAN Crypt* coupe le nom à partir de là. Cela peut causer des problèmes, par exemple, si des adresses électroniques sont utilisées.

- **Attribut pour de courriel :**

  Cet attribut est ajouté aux certificats auto-générés.

- **Attribut pour commentaire :**

  Comme l' adresse électronique, cet attribut peut être utilisé pour identifier des objets utilisateur. Ceci est particulièrement utile si le nom de l'utilisateur et l'identifiant de connexion ne peuvent pas être utilisés par l'assistant pour identifier des objets lorsque des certificats sont attribués. À ce stade, vous pouvez saisir le nom de l'attribut que l'assistant doit utiliser pour identifier l'utilisateur correct lors de l'attribution des certificats.

  Remarque : Si des attributs vides sont importés pendant la synchronisation (par exemple en raison de la suppression d'un attribut dans l'AD), les commentaires d'*u.trust LAN Crypt* ne sont pas affectés. Les entrées existantes sont maintenues. Le nouveau contenu de l'attribut écrase les commentaires existants.

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

- **Certificats**

  Dans l'onglet **Certificats**, indiquez si les certificats qui ont été attribués à l'utilisateur dans le répertoire LDAP doivent être transférés lorsque l'utilisateur est importé dans la base de données *u.trust LAN Crypt*.

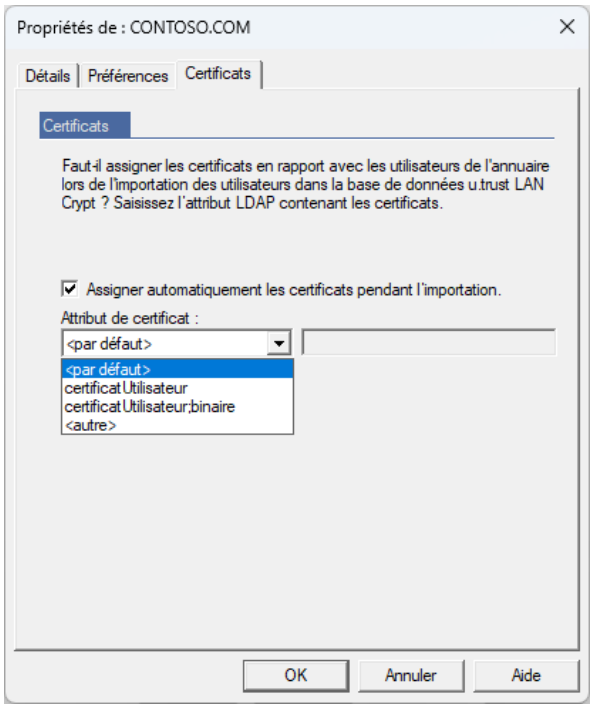
  Vous n'avez plus besoin d'assigner de certificats à ces utilisateurs dans la console d'administration d'*u.trust LAN Crypt*. Ici, vous pouvez également spécifier un attribut qui contient le certificat de l'utilisateur.

  Remarque : Les certificats attribués de cette façon ne sont pas vérifiés (heure d'expiration, sur une LCR, etc.) !

Activer le

Assigner automatiquement les certificats pendant l'importation

Si les certificats du répertoire LDAP doivent être automatiquement importés et attribués à l'utilisateur lorsqu'ils sont importés dans la base de données *u.trust LAN Crypt*.



<par défaut> évalue *certificatUtilisateur* et *certificatUtilisateur;binaire*.

Cliquez sur *<autre>* pour spécifier un autre attribut qui contient le certificat.

Lorsque vous cliquez sur **OK**, *u.trust LAN Crypt* transfère les informations de connexion vers la liste des serveurs. Vous pouvez également modifier ou supprimer ces informations dans cette liste.

3.5.6 Onglet Répertoires

Remarque : Les paramètres que vous effectuez ici sont toujours enregistrés dans la sauvegarde de configuration actuelle du responsable de la sécurité. Si aucune sauvegarde de configuration n'a encore été créée, le système utilise la sauvegarde de configuration *<DEFAULT CONFIGURATION>*.

Remarque : Dans le nœud **Paramètres centraux** de l'onglet **Répertoires**, les variables d'environnement telles que %LOGONSERVER% etc. ne peuvent pas être utilisées pour les spécifications de chemin.

Emplacement de stockage des fichiers de stratégie générés

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

Entrez l'emplacement de stockage (généralement un lecteur réseau qui a été partagé avec l'utilisateur) dans le champ de saisie.

Remarque : Vérifiez que l'utilisateur peut accéder à ce dossier, car les fichiers (de stratégie) générés sont chargés ou copiés à partir de celui-ci lorsque l'utilisateur se connecte.

Remarque : Vous devez également spécifier l'emplacement de stockage des fichiers de stratégie du point de vue du client. Vous trouverez ce paramètre sous *u.trust LAN Crypt Configuration* (voir « *Emplacement du fichier de stratégie client* » à la page 192.

Options de fichier de stratégie - Spécification du format de fichier de stratégie

Si vous utilisez différentes versions d'*u.trust LAN Crypt* Client, vous devez vous assurer que tous vos clients *u.trust LAN Crypt* peuvent lire les fichiers de stratégie générés.

Remarque : Depuis la version 4.0.0, *LAN Crypt* ne prend plus en charge les anciens formats de fichiers de stratégie (tels que *« *.pol.bz2»* ou « **.pol »*). Le format actuel des fichiers de stratégie est « **.xml.bz2* ». Ce format est pris en charge par *LAN Crypt* à partir de la version 3.90. Le fichier est un fichier XML compressé. Il contient toutes les règles assignées, les droits d'accès et les clés de l'utilisateur concerné, ainsi que la signature numérique de du responsable de la sécurité. Les clés contenues dans le fichier de politique sont chiffrées à l'aide du certificat public de l'utilisateur. Avant d'installer la version 13.0.1 du client *LAN Crypt*, les versions antérieures à la 3.90 doivent être mises à jour successivement vers les versions 3.97, 4.2.0, puis 11.0.x. **Veuillez également noter que le format des fichiers de stratégie est prédéfini et ne peut pas être modifié à partir de la version 4.0.0.**

Créer des fichiers de stratégie supplémentaires basés sur le nom Novell

Si vous activez cette option, *u.trust LAN Crypt* génère deux fichiers de stratégie pour chaque utilisateur. Un fichier a l'identifiant de connexion Novell et l'autre a le nom d'utilisateur Windows. Le contenu de ces fichiers est identique.

L'utilisation de l'identifiant de connexion Novell doit également être spécifiée dans **Configuration u.trust LAN Crypt / Paramètres client** avant que vous puissiez l'utiliser pour vous connecter.

Remarque : Cette fonction n'est plus prise en charge par la version 4 d'*u.trust LAN Crypt*.

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

u.trust LAN Crypt peut générer des certificats auto-signés (fichiers clés *.p12) et les attribuer aux utilisateurs si nécessaire. Ces certificats sont créés et attribués dans la console d'administration via le nœud **Utilisateurs et certificats sélectionnés**. Alternativement, cette fonctionnalité est également disponible via les nœuds **Groupes** / **Membres et certificats du groupe**.

Remarque : Si le nœud **Utilisateurs et certificats sélectionnés** n'est pas affiché dans la console d'administration, vérifiez sous le nœud **u.trust LAN Crypt Administration**, après avoir cliqué sur *Propriétés* dans le menu contextuel, si l'option *Afficher « Utilisateurs et certificats sélectionnés »* est affichée dans l'onglet **Paramètres utilisateur**.

Le chemin d'accès où ces fichiers doivent être stockés doit être spécifié dans la console d'administration dans le nœud **Paramètres centraux** de l'onglet **Répertoires**. Les clients reçoivent ce chemin d'accès soit via un paramètre dans la stratégie de groupe *u.trust LAN Crypt* (« *Emplacement du fichier clé client* ») soit via une entrée dans le registre, par exemple via un fichier de registre.

Le client *u.trust LAN Crypt* recherche d'abord un certificat correspondant dans le magasin de certificats local de l'ordinateur, puis (si aucun certificat n'a été trouvé) dans le chemin défini par GPO ou via le paramètre de registre. De plus, la partie publique du certificat du responsable de la sécurité (*.cer) est stockée par la console d'administration dans ce chemin (paramètre GPO « *Emplacement du certificat client du responsable de la sécurité* »).

Pour qu'u.trust LAN Crypt reconnaisse automatiquement les fichiers clés de l'utilisateur, les noms de fichiers doivent correspondre à l'identifiant de connexion de l'utilisateur (« Logonname.p12 »).

Lorsqu'*u.trust LAN Crypt* trouve le bon fichier, il affiche une boîte de dialogue PIN. Vous devez envoyer une lettre PIN pour indiquer à l'utilisateur ce code PIN (qui se trouve dans le fichier journal du mot de passe « p12pwlog.csv »). Le nouvel outil « *LCSendP12Password* », inclus dans le paquet d'installation, est également disponible à cet effet. Le certificat et la clé associée sont automatiquement importés après que l'utilisateur a saisi le code PIN.

Si *u.trust LAN Crypt* trouve un fichier « **.cer* » qui contient la partie publique du certificat du responsable de la sécurité, il l'importe automatiquement.

Vous pouvez également distribuer manuellement les fichiers clés pour les utilisateurs et la partie publique du certificat du responsable de la sécurité. Si vous faites cela, assurez-vous que les clients les importent tous 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 changez le chemin sur lequel les fichiers « **.cer* » des responsables de la sécurité et les fichiers « **.p12* » des utilisateurs sont stockés, après avoir créé les responsables de la sécurité, vous devez copier leurs fichiers « **.cer* » sur le nouvel emplacement. Sinon, les parties publiques des certificats des responsables de la sécurité ne seront pas trouvées.

Mot de passe par défaut pour les fichiers clés de l'utilisateur

Dans *u.trust LAN Crypt*, vous pouvez définir un mot de passe similaire pour tous les fichiers clés de l'utilisateur.

Pour ce faire, copiez un fichier qui contient le mot de passe que vous voulez (jusqu'à 60 caractères) dans le même répertoire qui contient le fichier journal du mot de passe (voir « *Fichier journal pour les mots de passe des fichiers clés* » à la page suivante).

Le fichier contenant le mot de passe doit avoir le même nom que le fichier journal du mot de passe correspondant (nom par défaut : p12pwlog.csv) mais doit avoir l'extension de fichier « **.pwd* » (similaire au nom par défaut du fichier journal du mot de passe : p12pwlog.pwd). Si le système trouve ce type de fichier, tous les fichiers clés de l'utilisateur générés auront ce mot de passe.

Remarque : Si vous utilisez un « *mot de passe par défaut pour les fichiers clés de l'utilisateur* », il ne doit pas y avoir plusieurs fichiers clés (« *.p12* ») du même utilisateur dans l'emplacement de stockage pour les certificats générés et les fichiers clés (.p12).

Dans ce fichier, si vous saisissez *logonname* comme mot clé, au lieu du mot de passe par défaut, l'identifiant de connexion actuel sera utilisé comme mot de passe.

Remarque : Les fichiers « **.p12* » pour les responsables de la sécurité reçoivent toujours un mot de passe aléatoire car ils ont une sécurité plus élevée.

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

u.trust LAN Crypt stocke les certificats des responsables de la sécurité dans les fichiers « **.p12* », par exemple, en tant que sauvegardes. Ici, vous pouvez spécifier le dossier dans lequel ils sont enregistrés.

Remarque : Étant donné qu'ils contiennent des données sensibles, il est essentiel que vous les protégiez contre tout accès non autorisé.

Fichier journal pour les mots de passe des fichiers clés

Ici, vous pouvez spécifier l'emplacement de stockage et le nom du fichier journal pour les fichiers PKCS#12 générés (nom par défaut : *p12pwlog.csv*). Ce fichier contient les mots de passe des fichiers PKCS#12 générés et peut être utilisé, par exemple, pour créer une lettre PIN.

Le fichier journal des mots de passe contient les informations suivantes (les mots-clés entre parenthèses représentent les en-têtes de colonne dans le fichier « **.csv* ») :

- Date de génération (CreateDate)
- Heure de génération (CreateTime)
- Date d'expiration (ExpirationDate)
- Heure exacte de fin de validité (ExpirationTime)
- Nom d'utilisateur (Name)
- Identifiant de connexion (Logonname)
- Adresse électronique (EMail)
- Mode de génération (Mode). Les valeurs possibles sont :

  <GUI> - Le certificat a été généré dans la boîte de dialogue Propriétés de l'utilisateur.

  <SO> - Le certificat du responsable de la sécurité. A été généré lors de la création du responsable de la sécurité.

  <WIZARD>- le certificat a été généré à l'aide de l'*Assistant d'attribution de certificat*.
- Nom du fichier (FileName)
- Mot de passe (Password)

Remarque : Vous devez protéger ce fichier et en aucun cas l'enregistrer dans le même dossier que les fichiers de stratégie.

Avec *u.trust LAN Crypt*, vous pouvez facilement protéger le fichier journal de mot de passe. Pour ce faire, installez la console d'administration et l'application client de *u.trust LAN Crypt* sur le même ordinateur. Après avoir créé le responsable principal de la sécurité initial, créez une règle de chiffrement pour chiffrer le fichier journal des mots de passe. Pour ce faire, créez un profil pour le premier responsable principal de la sécurité (MSO), puis chargez le profil. La clé de chiffrement utilisée ne doit être accessible qu'aux responsables principaux de la sécurité et aux responsables de la sécurité qui ont le droit de générer des certificats.

Remarque : Si vous installez les deux composants *u.trust LAN Crypt*, la console d'administration et l'application client sur le même ordinateur, ils doivent impérativement être de la même version !

En exécutant l'assistant de chiffrement initial, le fichier journal des mots de passe est chiffré et ne peut plus être consulté par des personnes non autorisées. Pour vous assurer que le mot de passe du responsable principal de la sécurité initial n'a pas été falsifié avant le chiffrement du fichier, créez un nouveau certificat et attribuez-le au responsable principal de la sécurité initial.

Remarque : Si le responsable de la sécurité qui attribue les certificats n'a pas le droit du système de fichiers de modifier le fichier journal du mot de passe, *u.trust LAN Crypt* ne sera pas en mesure de générer des certificats.

Définissez la longueur du mot de passe pour les fichiers clés

La longueur du mot de passe pour les fichiers clés (*.p12) est de 20 caractères par défaut. À partir de la version 13.0.0 de *u.trust LAN Crypt*, vous pouvez, en fonction de vos exigences de sécurité, définir de manière flexible la longueur du mot de passe pour les fichiers PKCS#12 générés par *u.trust LAN Crypt* (fichiers de clés contenant le certificat et la clé privée) entre 12 et 60 caractères.

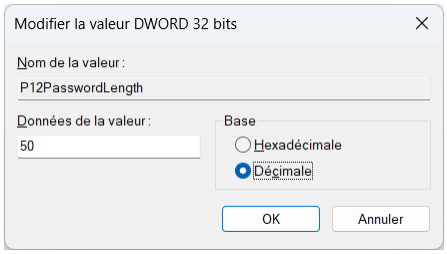
Pour ce faire, ajoutez la valeur DWORD nommée « P12PasswordLength » dans le registre Windows sous la clé

```
[HKLM\SOFTWARE\Policies\Utimaco\SGLANCrypt]
```

Saisissez une valeur (décimale) comprise entre « 12 » et « 60 » et cliquez sur **OK**.

Exemple :

```
"P12PasswordLength"=dword:0x00000032 (50)
```



Dans l'exemple ci-dessus, le mot de passe a été modifié pour atteindre une longueur de 50 caractères.

Remarque : il n'est pas nécessaire de redémarrer l'ordinateur après avoir modifié la valeur.

3.5.7 Onglet Régions

Dans *u.trust LAN Crypt*, vous pouvez configurer des régions pour rendre l'administration des clés plus facile et moins complexe. Chaque région est assignée à un responsable de la sécurité spécifique qui en est alors responsable. Lorsque ce responsable de la sécurité génère des clés, le système ajoute automatiquement le préfixe de cette région au début des noms des clés. Ainsi, vous pouvez toujours voir l'unité administrative pour laquelle chaque clé a été générée. Cette approche est particulièrement utile dans les environnements distribués.

Vous pouvez définir des régions en cliquant sur *Propriétés* dans le menu contextuel du nœud **Paramètres centraux** dans l'onglet **Régions**. Les régions affichées ici peuvent être attribuées aux responsables de la sécurité lors de leur création. Vous pouvez définir une nouvelle région en cliquant sur Ajouter. Dans le champ *Nom de la région*, saisissez un nom approprié (par exemple Grand Est) pour la région en question et dans le champ *Préfixe de cette région*, saisissez le préfixe correspondant à la région (par exemple NY). En cliquant sur le bouton **OK**, la nouvelle région est ajoutée à la liste des régions existantes.

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

Remarque : Vous ne pouvez supprimer une région que si elle n'est pas affectée à un responsable de la sécurité.

3.5.8 Onglet Configurations

À l'aide de l'onglet **Configurations** dans le nœud **Paramètres centraux**, des modèles de configuration individuels peuvent être créés pour chaque région. Un modèle de configuration défini de cette manière n'est alors valable que pour la région concernée. L'administration de chaque région peut être effectuée par des responsables de la sécurité sélectionnés, si vous les affectez à la région respective.

Les sauvegardes de configuration contiennent toutes les informations qui peuvent être saisies dans l'onglet **Répertoires** :

- l'emplacement de stockage des fichiers de stratégie générés
- l'emplacement de stockage pour les certificats générés et les fichiers clés de l'utilisateur
- l'emplacement de stockage des fichiers clés générés des responsables de la sécurité
- l'emplacement de stockage et le nom du fichier journal du mot de passe
- les options pour les fichiers de stratégie

Les sauvegardes de configuration sont toujours affectées à une région existante. De manière générale, un responsable de la sécurité affecté à une région ne peut utiliser que les sauvegardes de configuration qui ont été générées pour cette région. L'exception est la sauvegarde de configuration <DEFAULT CONFIGURATION> qui peut être utilisée dans toutes les régions.

En utilisant une configuration particulière pour une unité organisationnelle (région), vous vous assurez facilement que les chemins corrects peuvent être définis pour un ou plusieurs responsables de la sécurité, et que tous les responsables de la sécurité utilisent toujours les mêmes chemins pour enregistrer les fichiers générés (certificats, fichiers de stratégie, fichier journal de mot de passe).

Les modifications dans l'onglet **Répertoires** sont toujours enregistrées dans la sauvegarde de configuration actuellement attribuée.

Remarque : L'autorisation globale *Modifier la configuration* spécifie si un responsable de la sécurité est autorisé à modifier ses propres paramètres de configuration. Si un responsable de la sécurité n'a pas ce droit, il ne peut utiliser que les chemins sélectionnés.

Si un responsable de la sécurité modifie une sauvegarde de configuration existante, il modifie également la configuration de tous les responsables de la sécurité qui sont aussi affectés à cette configuration !

Générer une sauvegarde de configuration

Pour générer une sauvegarde de configuration, procédez comme suit :

1. Sélectionnez une région existante, pour laquelle vous souhaitez créer la sauvegarde de configuration, ou sélectionnez <no region> pour créer une sauvegarde de configuration à laquelle les responsables de la sécurité qui ne sont pas dans une région peuvent être affectés.

2. Dans *Nouveau nom*, entrez un nom pour la nouvelle sauvegarde de configuration (par exemple Grand Est).

3. Sélectionnez une sauvegarde de configuration existante dans la liste.

   Le système copie cet enregistrement de configuration et l'enregistre avec le nouveau nom. Cliquez sur **Copier**.

4. Si vous souhaitez modifier l'enregistrement de configuration, sélectionnez-le et cliquez sur **Modifier**.

5. Une boîte de dialogue s'affiche, qui est identique à la boîte de dialogue *Répertoires* dans *Propriétés*. Saisissez ici les chemins appropriés et définissez les options du fichier de stratégie. Cliquez sur **OK**.

6. Le système affiche maintenant le nouvel enregistrement de configuration dans la liste, dans la région appropriée, et vous pouvez l'utiliser pour créer d'autres responsables de la sécurité. Pour modifier la configuration (et la région) d'un enregistrement de configuration existant, sélectionnez l'onglet *Propriétés* en regard du responsable de la sécurité souhaité.

7. Vous pouvez créer autant d'enregistrements de configuration supplémentaires que vous le souhaitez.

3.5.9 Onglet Autorisation supplémentaire

Dans *u.trust LAN Crypt*, vous pouvez préciser que des actions particulières nécessitent une autorisation supplémentaire d'au moins un responsable de la sécurité supplémentaire. Une autorisation supplémentaire peut être requise pour les actions suivantes :

Actions	Autorisations nécessaires
Modifier les paramètres d'autorisation supplémentaires	Ne peut être effectué que par un responsable principal de la sécurité.
Modifier la clé de récupération	Ne peut être effectué que par un responsable principal de la sécurité.
Les actions suivantes ne peuvent être effectuées que par des responsables de la sécurité qui ont l'autorisation globale d'autoriser des opérations et ont le droit d'effectuer l'action. **IMPORTANT :** Veuillez noter qu'avoir seulement l'autorisation globale de fournir une autorisation supplémentaire peut ne pas être suffisant dans certaines situations. Le responsable de la sécurité qui fournit l'autorisation supplémentaire doit avoir le droit correspondant pour cet objet spécifique.	
Modification des paramètres globaux	Nécessite l'autorisation globale : *Changer la configuration*. Le système vous invite à demander une autorisation lorsque vous effectuez des modifications dans les onglets **Algorithmes**, **Certificats**, **Régions**, **Répertoires**, **Clés**, **Antivirus**, **Règles de résolution**, **Serveur**, **Configurations** et **Autres paramètres**. Seuls les responsables principaux de la sécurité peuvent autoriser des modifications aux onglets **Algorithmes**, **Certificats**, **Clés**, **Règles de résolution**, **Régions** et **Autres paramètres** !
Créer un responsable de la sécurité	Nécessite l'autorisation globale *Créer des responsables de la sécurité*.
Modifier les listes de contrôle d'accès	Nécessite l'autorisation globale : *Modifier les ACL* et les droits spécifiques de groupe ou SO correspondants.
Modifier les autorisations globales	Nécessite l'autorisation globale *Modifier les autorisations globales* et les droits spécifiques au groupe ou à l'OS correspondants.
Attribuer des certificats	Nécessite l'autorisation globale *Attribuer des certificats* et les droits spécifiques au groupe correspondants.

Actions	Autorisations nécessaires
Attribuer des certificats à tous les membres	Nécessite l'autorisation globale *Attribuer des certificats à tous les membres* et les droits spécifiques au groupe correspondant.
Utiliser des clés spécifiques à l'utilisateur ou au groupe	Nécessite l'autorisation globale *Utiliser des clés spécifiques*. Spécifier une autorisation supplémentaire pour l'utilisation de clés spécifiques n'affecte pas l'utilisation des espaces réservés <USERKEY> ou <GROUPKEY>. Cela limite uniquement la manipulation (**affichage / utilisation / édition**) d'une clé spécifique réelle.
Administrer les groupes	Nécessite l'autorisation globale *Administrer les groupes* et les droits spécifiques au groupe correspondant.
Administrer les utilisateurs	Nécessite l'autorisation globale *Administrer les utilisateurs* et les droits spécifiques au groupe correspondant.
Gérer l'enregistrement	Nécessite les autorisations globales *Lire les entrées de journalisation* et *Gérer la journalisation*
Créer des règles	Cela nécessite l'autorisation globale *Créer des règles* ainsi que le droit spécifique au groupe correspondant.
Créer ou déplacer des clés	Nécessite l'autorisation globale *Créer des clés* ainsi que le droit spécifique au groupe correspondant.
Créer des profils	Nécessite l'autorisation globale *Créer des profils* ainsi que l'autorisation spécifique au groupe correspondante.
Afficher la valeur de la clé	Nécessite l'autorisation globale *Lire la clé*. Une autorisation supplémentaire est requise lorsque vous cochez l'option Afficher la valeur de la clé dans la boîte de dialogue des propriétés d'une clé.

Remarque : Si une autorisation supplémentaire est nécessaire pour l'exécution de certaines actions, ce paramètre s'applique également aux actions étroitement liées.

Si une autorisation supplémentaire est nécessaire pour l'une de ces actions, vous devez spécifier le nombre de responsables de la sécurité requis pour l'action concernée.

Pour ce faire, sélectionnez cette action. Lorsque vous double-cliquez sur l'action sélectionnée, une boîte de dialogue s'ouvre. Celle-ci vous permet de spécifier le nombre de responsables de la sécurité requis. Lorsque vous cliquez sur **OK**, *u.trust LAN Crypt* met à jour la liste qui se trouve dans l'onglet **Autorisation supplémentaire** du nœud **Paramètres centraux**.

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

Remarque : Le système ne peut pas déterminer avec précision le nombre de responsables de la sécurité effectivement disponibles. Le nombre requis n'est peut-être pas disponible, même si le message n'apparaît pas. Par exemple, les droits d'un responsable de la sécurité peuvent avoir été modifiés après coup, ou un responsable de la sécurité peut avoir été supprimé.

Avertissement : Si vous êtes informé que les responsables de la sécurité requis ne sont pas disponibles et précisez qu'au moins un responsable supplémentaire est nécessaire lors de la définition du nombre requis, puis confirmez votre paramètre avec OK et fermez la boîte de dialogue, le paramètre sera néanmoins adopté pour des raisons techniques.

En résulte une situation où les actions nécessitant une autorisation supplémentaire ne peuvent plus être exécutées, car les responsables de la sécurité requis 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 ne peut être modifié qu'en générant une clé de récupération (voir « *Renonciation à une autorisation supplémentaire* à la page suivante).

Une situation similaire peut survenir suite à la suppression de responsables de la sécurité. En effet, le système ne vérifie pas si le nombre requis de responsables de la sécurité pour une autorisation supplémentaire est toujours disponible après la suppression de l'un d'eux. *u.trust LAN Crypt* garantit uniquement l'existence d'un responsable principal de la sécurité dans le système.

Remarque : Si vous n'utilisez pas de jetons pour obtenir une autorisation supplémentaire, nous vous recommandons de définir **Protection forte de la clé privée** sur **Oui**.

Fournir une autorisation supplémentaire

Si une autorisation supplémentaire a été spécifiée pour une action, l'assistant d'autorisation supplémentaire s'exécute lorsque cette action est sélectionnée. Cet assistant demande l'autorisation d'au moins un autre responsable principal de la sécurité. Vous pouvez sélectionner le responsable principal de la sécurité concerné dans une boîte de dialogue.

Si *u.trust LAN Crypt* authentifie avec succès ce responsable de la sécurité à l'aide de son certificat, l'action requise peut être effectuée.

Si plusieurs responsables de la sécurité ont le même certificat, celui-ci ne peut être utilisé qu'une seule fois dans une exécution d'autorisation. Tout autre responsable de la sécurité auquel ce certificat est assigné est retiré de la liste des responsables.

Remarque : La boîte de dialogue dans laquelle vous sélectionnez un responsable de la sécurité dispose d'une option qui vous permet de limiter l'affichage aux responsables de la sécurité dans une région particulière. Les responsables de la sécurité qui ne sont assignés à aucune région apparaissent toujours dans la liste.

Annulation d'une autorisation supplémentaire

Une autorisation supplémentaire d'action s'applique généralement pendant toute la durée d'une session d'administration *u.trust LAN Crypt*. Cliquez sur le bouton **Réinitialiser toutes les autorisations supplémentaires accordées** dans la barre d'outils d'administration pour

supprimer les informations pertinentes, de sorte qu'une autorisation supplémentaire soit requise la prochaine fois que l'action est exécutée dans la même session.

Renonciation à une autorisation supplémentaire

Si, en raison de la configuration, le nombre de responsables de la sécurité présents pour fournir une autorisation supplémentaire d'action est trop faible, vous pouvez utiliser la clé de récupération pour réinitialiser le nombre de responsables de la sécurité requis afin de modifier les paramètres d'autorisation supplémentaires sur « 0 ».

Pour ce faire, cliquez sur **Assigner le certificat** dans la boîte de dialogue de connexion. Cela exécute un assistant qui vous permet de réinitialiser le nombre de responsables de la sécurité supplémentaires requis sur « 0 ». Pour plus de détails, voir ci-dessous.

3.5.10 Onglet Clés de récupération

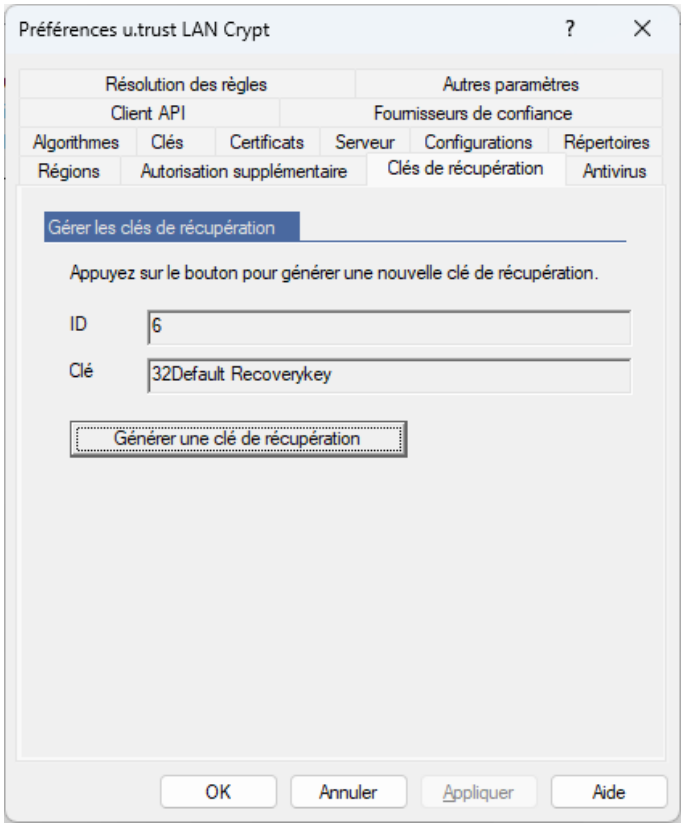
Vous pouvez générer une clé de récupération dans *u.trust LAN Crypt*. Vous pouvez utiliser cette clé pour assigner un nouveau certificat à un responsable de la sécurité lorsque celui-ci se connecte à la base de données *u.trust LAN Crypt* (cliquez sur le bouton « **Assigner le certificat** »). Cela est utile si, par exemple, son certificat est endommagé et ne peut plus être utilisé. À l'aide de la clé de récupération, vous pouvez également réinitialiser le nombre de responsables de la sécurité supplémentaires requis afin de modifier les paramètres d'autorisation supplémentaire sur « 0 ».

Une clé de récupération peut être divisée en plusieurs parties. Vous pouvez spécifier le nombre de parties nécessaires à l'assignation d'un nouveau certificat. Les différentes parties de la clé de récupération peuvent être distribuées à différents responsables de la sécurité. Le propriétaire de chaque partie doit être présent lorsque la clé de récupération est utilisée, et un assistant doit être utilisé pour présenter les parties de la clé. La clé de récupération (ou ses parties) peut être saisie manuellement ou chargée à partir d'un fichier.

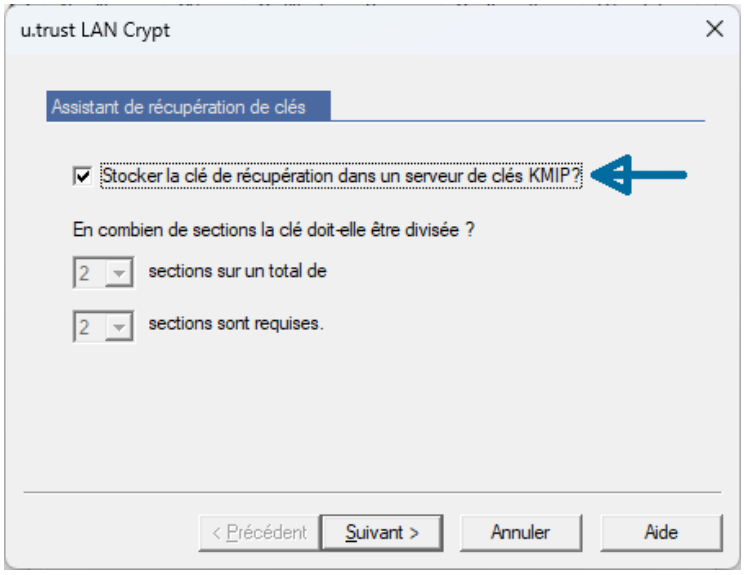
Alternativement (à partir de la version 4.1.0), vous pouvez également stocker la clé de récupération sur un **serveur de clés KMIP**.

Remarque : Vous pouvez utiliser un **serveur de clés KMIP** (facultatif) pour stocker la clé de récupération de manière particulièrement sécurisée. Veuillez noter que *u.trust LAN Crypt* ne prend actuellement en charge que l'Enterprise Secure Key Manager (ESKM) du fabricant Utimaco.

Pour générer une clé de récupération, ouvrez le menu contextuel dans le nœud **Paramètres centraux** de la console d'administration et cliquez sur *Propriétés*. Dans la boîte de dialogue qui apparaît, passez à l'onglet **Clé de récupération**.

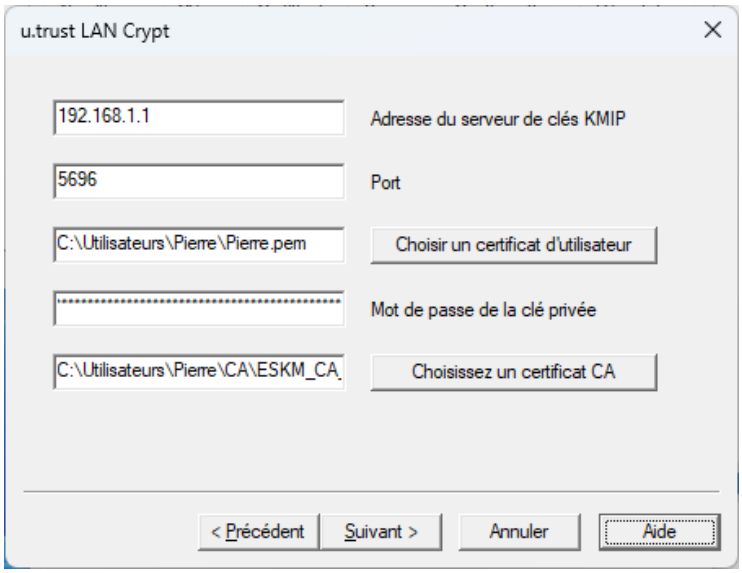


Cliquez sur le bouton **Générer une clé de récupération**.



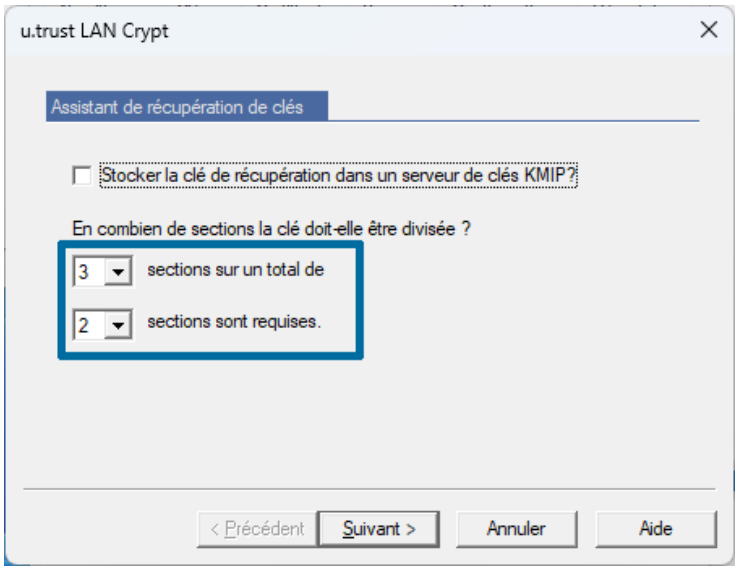
Sélectionnez l'option **Stocker la clé de récupération sur un serveur de clés KMIP ?** ou utilisez les menus déroulants, sélectionnez le nombre de parties que la clé doit contenir et combien d'entre elles sont nécessaires pour utiliser la clé de récupération.

Si vous sélectionnez **Stocker la clé de récupération sur un serveur de clés KMIP ?** puis cliquez sur Suivant, vous devez entrer les données de connexion pour le serveur de clés KMIP (adresse et port du serveur) ainsi que les informations de certificat requises et le mot de passe pour la clé privée dans les champs de saisie respectifs.



Cliquez ensuite sur **Suivant**. La connexion au **serveur de clés KMIP** ainsi que les détails du certificat sont vérifiés et, en cas de succès, la clé de récupération est stockée de manière sécurisée sur le **serveur de clés KMIP**.

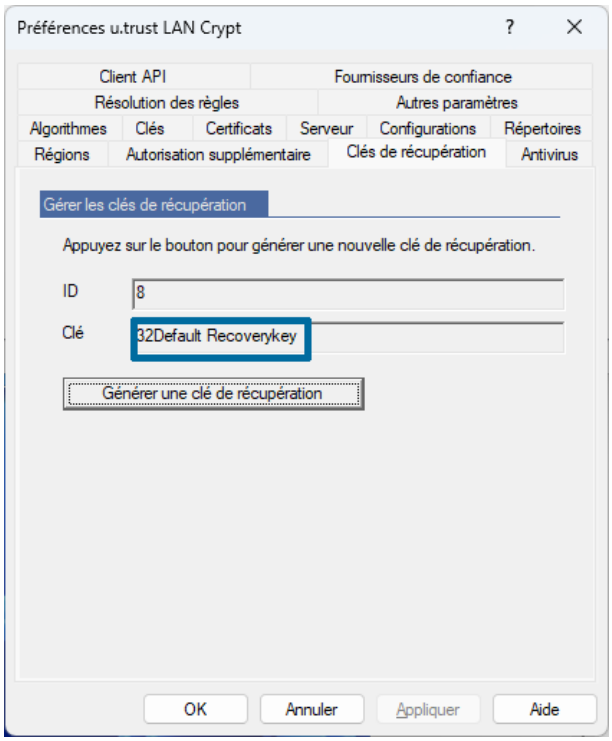
Dans notre exemple, la clé doit comporter trois parties, dont au moins deux sont nécessaires pour attribuer un nouveau certificat de responsable de la sécurité lors de la connexion.



À l'aide des menus déroulants, sélectionnez le nombre de parties que la clé doit contenir, et combien d'entre elles sont nécessaires pour utiliser la clé de récupération. Dans notre exemple, la clé sera constituée de trois parties, dont au moins deux seront nécessaires pour assigner un nouveau certificat au responsable de la sécurité lors de la connexion. Cliquez sur **Suivant**.

Pour chaque partie de la clé, l'assistant affiche une boîte de dialogue dans laquelle vous pouvez spécifier si la clé partielle est enregistrée dans un fichier ou affichée à l'écran afin que vous puissiez l'écrire. Une fois toutes les parties traitées, l'assistant se ferme.

Dans l'onglet **Clés de récupération** situé en bas du tableau, directement à gauche de l'entrée « *Clé de récupération par défaut* », vous pouvez voir le nombre de parties dont la clé se compose (dans l'exemple mentionné, 3 parties) et combien de ces parties sont nécessaires à son utilisation (dans l'exemple mentionné, 2).



Remarque : Lorsque vous générez et distribuez les parties de la clé de récupération, rappelez-vous qu'elles impliquent des données extrêmement sensibles. Il est essentiel de protéger la clé de récupération contre tout accès non autorisé.

Remarque : Vous ne pouvez utiliser que la clé de récupération la plus récente. Les clés de récupération générées précédemment ne sont plus valides et ne peuvent pas être utilisées pour assigner un certificat.

Utilisation de la clé de récupération

S'il n'est plus possible de se connecter à la base de données *u.trust LAN Crypt* (par exemple parce qu'un certificat a expiré), cliquez sur **Assigner le certificat** dans la boîte de dialogue de connexion pour démarrer l'*assistant de récupération de clés*.

Si une boîte de dialogue apparaît pour vous informer que le certificat ne peut pas être utilisé après la sélection d'un responsable de la sécurité, vous pouvez démarrer l'assistant à partir de cet emplacement.

Suivez les instructions à l'écran.

Selon le paramètre sélectionné pour la clé de récupération (classique ou via un **serveur de clés KMIP**), l'assistant affiche la boîte de dialogue correspondante nécessaire pour créer un nouveau certificat pour le responsable de la sécurité principale afin de lui permettre d'accéder à nouveau à l'administration du *u.trust LAN Crypt*.

Cet assistant contient une boîte de dialogue dans laquelle vous pouvez réinitialiser sur « 0 » le nombre de responsables de la sécurité nécessaires pour modifier les paramètres d'autorisation supplémentaire.

Cela garantit qu'aucune situation dans laquelle une autorisation supplémentaire n'est plus possible en raison de l'absence de responsables de la sécurité pouvant l'exécuter ne peut survenir.

Si vous activez cette option, un seul responsable de la sécurité peut modifier les paramètres pour une autorisation supplémentaire par la suite.

3.5.11 Onglet Base de données

Remarque : Ce paramètre n'est nécessaire que si vous utilisez une base de données Oracle, accessible via les consoles d'administration sur différentes machines. Seul un responsable principal de la sécurité peut effectuer ce réglage !

Le Support Linguistique National (NLS) 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 des différents jeux de caractères.

Exemple : WE8MSWIN1252: ü=FC00, AL16UTF16: ü=7C00.

L'ajout de texte à la base de données et son extraction à l'aide d'un jeu de caractères différent peut entraîner des erreurs lors du calcul de la somme de contrôle (MAC). Par exemple, si les caractères étaient convertis en binaire, les données binaires causeraient des problèmes pour le MAC.

Pour éviter ces erreurs, assurez-vous que les mêmes pages de code et jeux de caractères sont utilisés sur toutes les machines qui accèdent à la base de données via le client Oracle.

L'onglet **Base de données** vous permet de spécifier un jeu de caractères à utiliser sur toutes les machines à partir desquelles on accède à la base de données. Lors du démarrage de la console d'administration, *u.trust LAN Crypt* vérifie si les paramètres du client Oracle correspondent ou non aux paramètres de la base de données. Si ce n'est pas le cas, un avertissement apparaît et la console d'administration ne démarre pas.

Dans le champ d'édition, entrez le jeu de caractères à utiliser sur les clients Oracle pour permettre une connexion à la base de données. Sur un client Oracle, ce paramètre se trouve dans le registre sous la valeur *NLS_Lang (Language.Territory.CharacterSet*, par exemple : `GERMAN_GERMANY.WE8MSWIN1252`).

Le jeu de caractères de la machine actuelle est affiché sous INFO : dans l'onglet **Base de données**. En général, ce jeu de caractères doit également être utilisé par tous les autres clients qui accèdent à la base de données.

Remarque : Nous vous recommandons de n'utiliser qu'un seul jeu de caractères ! Si vous utilisez plus d'un jeu de caractères, des erreurs peuvent survenir lors du calcul de la somme de contrôle (MAC). Toutefois, il est généralement possible d'utiliser plusieurs jeux de caractères. Malgré cela, vous ne devez en utiliser plus d'un que si les jeux de caractères sont largement identiques et ne diffèrent que par quelques caractères. Vous devez identifier ces caractères et ne pas les utiliser pour les entrées de base de données !

Désactivation de cette vérification

u.trust LAN Crypt vous permet de désactiver la vérification des jeux de caractères. Si le champ d'édition est vide, aucune vérification n'est effectuée et il est toujours possible de se connecter à la console d'administration. Veuillez noter que cela peut entraîner des erreurs lors du calcul de la somme de contrôle (MAC).

Pour éviter les erreurs lors de la spécification d'un jeu de caractères (par exemple des erreurs de saisie), lesquelles peuvent empêcher le responsable principal de la sécurité ayant effectué le réglage de se connecter à la console d'administration, *u.trust LAN Crypt* vérifie les données saisies lorsque vous appuyez sur **Appliquer** ou **OK**. Si le jeu de caractères spécifié ne correspond pas à celui actuellement utilisé sur cette machine, un message apparaît et le jeu de caractères actuellement valide est ajouté au champ d'édition. L'onglet Base de données reste à l'écran pour permettre la vérification des données saisies. Si nécessaire, modifiez les paramètres et appuyez à nouveau sur **Appliquer** ou **OK**.

3.5.12 Onglet Antivirus

Vous devez spécifier les scanners antivirus ici pour que ces derniers puissent analyser les fichiers chiffrés avec *u.trust LAN Crypt*. Le logiciel antivirus saisi ici est donc explicitement autorisé à accéder aux fichiers chiffrés, et peut reconnaître les signatures de virus pendant le processus d'analyse, même dans les fichiers chiffrés *u.trust LAN Crypt*.

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

- Un nom pour le logiciel antivirus (ce nom est affiché dans l'onglet **Antivirus** sous-produit).
- Le nom du fichier exécutable qui effectue l'analyse antivirus.

Pour éviter que les scanners de antivirus ne retardent le chargement des règles de chiffrement du client *u.trust LAN Crypt*, configurez les processus antivirus pour qu'ils soient actifs lorsque les règles de chiffrement du client sont chargées, ou indiquez le chemin d'accès au fichier exécutable qui effectue l'analyse antivirus. Vous pouvez également utiliser des caractères génériques pour une partie du chemin.

Exemple :

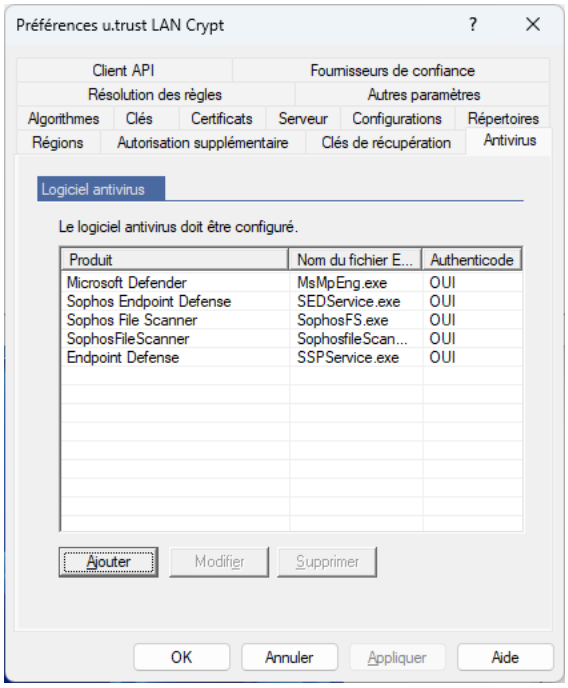
```
C:\ProgramData\Microsoft\Windows Defender\Platform\*\MsMpEng.exe
```

Remarque : Si vous n'incluez pas le chemin d'accès à ce stade, cela augmentera le temps de chargement du fichier de stratégie.

Activez l'option **Utiliser la vérification Authenticode**.

Remarque : Dans tous les cas, nous vous recommandons ici d'utiliser un scanner antivirus signé Authenticode pour spécifier le scanner et activer la vérification Authenticode. Seule cette vérification garantit que le fichier exécutable est vraiment celui nécessaire au scanner antivirus et que seules les applications fiables reçoivent l'accès explicitement souhaité aux fichiers chiffrés.

Après avoir cliqué sur **OK**, le logiciel antivirus s'affiche dans la liste. Vous pouvez ajouter d'autres scanners antivirus.



3.5.13 Onglet API client

u.trust LAN Crypt fournit une API client pour permettre aux applications de contrôler la fonctionnalité de chiffrement de fichiers via une ligne de commande simple ou une API de style COM. Pour plus de détails, veuillez consulter la documentation de l'API client (PDF) dans le dossier « `\api` » de votre package d'installation décompressé.

Remarque : L'API doit être sélectionnée lors de l'installation du client *u.trust LAN Crypt*. Si vous souhaitez que l'API client soit utilisée sur vos clients, assurez-vous qu'elle est correctement installée.

Dans l'onglet **API client**, spécifiez les paramètres de l'API client.

- Sélectionnez **Activer l'API client** pour rendre l'API disponible sur le client. Les applications peuvent désormais contrôler la fonctionnalité de fichier via l'API de style COM.
- Sélectionnez **Activer l'accès API pour l'outil de ligne de commande de chiffrement des fichiers LAN Crypt** afin de permettre le contrôle de la fonctionnalité de chiffrement de fichier via un outil de ligne de commande simple.

- **API de style COM uniquement** : par défaut, les règles de chiffrement définies dans l'administration *u.trust LAN Crypt* ont priorité sur les tâches de chiffrement effectuées via l'API client. Si vous voulez que les « règles API » aient la priorité, sélectionnez l'option **Les règles API ont la priorité sur les règles de chiffrement** dans les profils.

  Remarque : Les **règles Ignorer** et les **règles d'exclusion** d'*u.trust LAN Crypt* ont la priorité la plus élevée et ne peuvent pas être annulées par les règles API. En outre, les mêmes fichiers/dossiers sont automatiquement exclus du chiffrement (voir « *Fichiers/dossiers exclus du chiffrement* » à la page 10).

Comme l'accès API est limité aux applications autorisées, vous devez spécifier les applications autorisées à l'utiliser. Pour ce faire :

1. Cliquez sur **Ajouter** dans l'onglet **API client**.
2. Spécifiez le nom de l'application autorisée à utiliser l'API client.
3. Spécifiez le fichier exécutable qui accède à l'API client *u.trust LAN Crypt*.
4. Si vous souhaitez que seuls les fichiers exécutables signés Authenticode accèdent à l'API, sélectionnez l'option **Le fichier exécutable doit être signé Authenticode**.
5. Si vous souhaitez que seuls les fichiers exécutables signés par des fournisseurs de confiance soient utilisés, sélectionnez également l'option **Le fichier exécutable doit être signé Authenticode par un fournisseur de confiance**. Cela garantit que seuls les fichiers exécutables signés à l'aide du certificat qui est enregistré comme certificat de signature d'un fournisseur dans l'onglet **Fournisseurs de confiance** sont acceptés.
6. Saisissez éventuellement un commentaire.

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

3.5.14 Onglet Fournisseurs de confiance

L'onglet **Fournisseurs de confiance** vous permet d'enregistrer les fournisseurs qui peuvent signer un fichier exécutable Authenticode pour accéder à l'API client.

Pour ajouter un fournisseur de confiance

1. Cliquez sur **Ajouter** dans l'onglet **Fournisseurs de confiance**.
2. Entrez le nom du fournisseur.
3. Entrez le certificat de signature du fournisseur.

   Si elle est sélectionnée dans l'onglet **API client**, l'API n'acceptera que les exécutables signés Authenticode à l'aide de ce certificat.
4. Saisissez éventuellement un commentaire.

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

3.5.15 Onglet Autres paramètres

Options du responsable de la sécurité

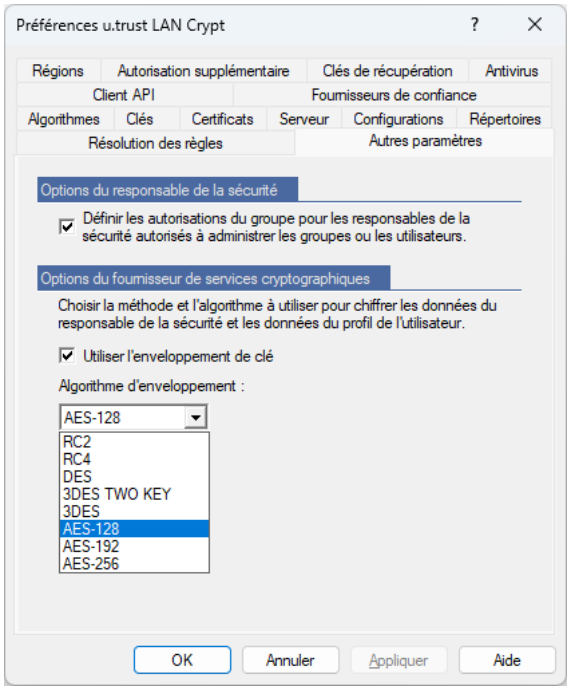
u.trust LAN Crypt peut être configuré pour créer automatiquement une ACL avec droit de visualisation du groupe racine pour un nouveau responsable de la sécurité. Cela nécessite que le responsable de la sécurité dispose de l'autorisation globale Administrer les groupes ou Administrer les utilisateurs. Le responsable de la sécurité a ainsi la garantie de pouvoir accéder (afficher et/ou modifier) à tous les groupes dont il est responsable.

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

Remarque : Si vous souhaitez ensuite retirer un responsable de la sécurité d'un groupe, vous ne pouvez le faire que dans le groupe racine, le nœud principal **Groupes**, car les autorisations sont « héritées » par tous les sous-groupes situés en dessous.

Options du fournisseur de services cryptographiques

Si l'option **Utiliser l'enveloppement de clé** (paramètre par défaut) est sélectionnée, les données du responsable de la sécurité et les données du profil utilisateur seront chiffrées à l'aide d'une clé de session aléatoire avec l'algorithme sélectionné (*AES-128* par défaut). Cette clé de session est à nouveau chiffrée RSA avec la clé publique du certificat.



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

Si vous désélectionnez cette option, les données sont chiffrées RSA sans clé de session. Notez que cette option peut ne pas être prise en charge par les cartes à puce ou les intergiciels.

Remarque : Si l'algorithme sélectionné n'est pas pris en charge, les utilisateurs reçoivent un message d'erreur lors du chargement du fichier de stratégie. Dans ce cas, modifiez l'algorithme ou sélectionnez un algorithme approprié qui est pris en charge par la carte à puce ou l'intergiciel que vous utilisez.

3.6 Affichage de toutes les clés u.trust LAN Crypt

En sélectionnant le nœud **Toutes les clés u.trust LAN Crypt**, vous pouvez afficher un aperçu de toutes les clés actuellement gérées par *u.trust LAN Crypt*. Vous pouvez consulter les informations suivantes ici :

- Nom de la clé longue.
- L'algorithme utilisé pour la clé.
- Informations indiquant si la clé est activée.
- Informations concernant qui a créé la clé (*Creator*).
- Informations indiquant si la clé doit être héritée.
- Informations sur le groupe pour lequel la clé a été créée.
- Informations indiquant si la clé est utilisée.
- Informations sur le champ Commentaire.

Dans la vue par défaut, toutes les clés créées des groupes respectifs sont affichées. En faisant un clic droit sur le nœud **Toutes les clés u.trust LAN Crypt**, vous pouvez utiliser le menu contextuel pour modifier la vue des clés dans la fenêtre de droite afin d'afficher toutes les clés spécifiques, telles que toutes les clés de groupe existantes (<GROUPKEY>) et les clés d'utilisateur (<USERKEY>).

Cliquez sur un en-tête de colonne pour trier le contenu de la table par ordre croissant ou décroissant, afin de trouver les informations dont vous avez besoin.

3.6.1 Recherche de clés

En plus de trier les informations clés, vous pouvez également rechercher une clé particulière. Pour ce faire, faites un clic droit sur le nœud **Toutes les clés u.trust LAN Crypt**, puis sélectionnez *Rechercher une clé* dans le menu contextuel.

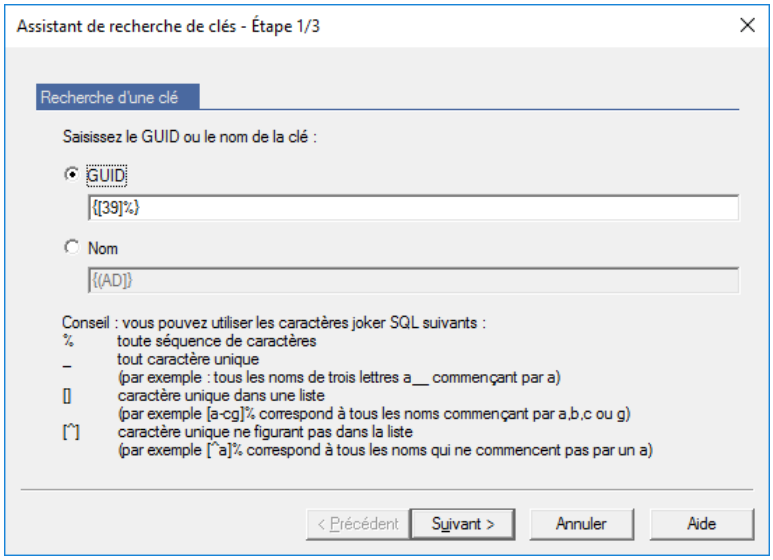
Remarque : La fonction **Rechercher une clé** est également disponible pour le nœud **Clés pour le groupe** dans chaque groupe. Pour ajouter une clé à un groupe, vous avez également besoin des bonnes *Clés de copie* pour le groupe dans lequel la clé se trouve ainsi que de la bonne clé de création pour le groupe auquel la clé doit être ajoutée.

Si une clé n'appartient à aucun groupe, elle ne sera pas affichée à un responsable de la sécurité à l'aide de la fonction **Trouver une clé**. Seul un responsable principal de la sécurité peut attribuer ce type de clé à un groupe.

Cela démarre un assistant qui vous aidera à trouver la clé que vous voulez. À l'étape 1, vous pouvez spécifier si vous souhaitez rechercher la clé en utilisant son GUID ou son nom. Vous pouvez utiliser certains espaces réservés SQL pour cela.

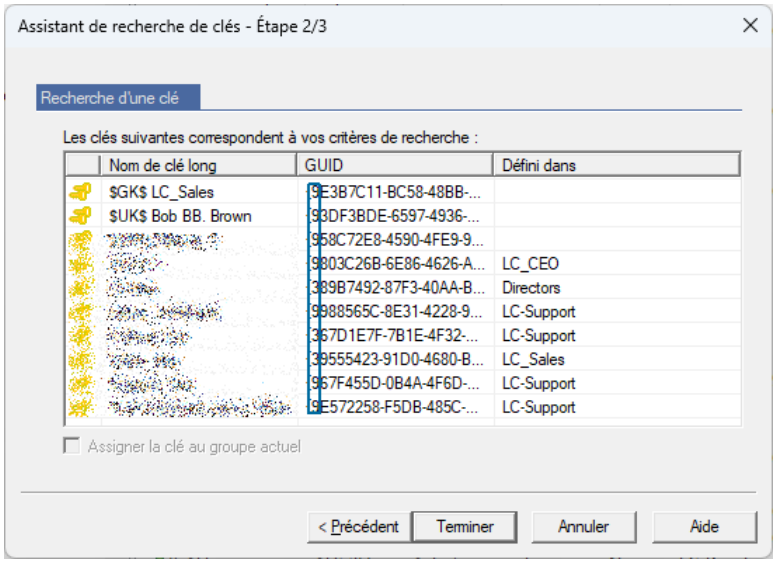
Exemple :

{[39]%} renvoie toutes les clés dont les GUID commencent par 3 ou 9.



Cliquez ensuite sur **Suivant** pour rechercher dans la base de données la clé dont vous avez besoin.

Si la clé est trouvée, l'étape 2 affiche le nom de la clé, son GUID et le groupe dans lequel elle a été générée.



Si vous avez appelé la fonction *Rechercher une clé* à partir d'un nœud de clé de groupe dans un groupe, activez l'option *Assigner la clé dans le groupe actuel* pour créer un lien vers la clé que vous avez trouvée. Vous pouvez ensuite utiliser une clé générée dans un autre groupe au sein du groupe actuellement sélectionné. Si vous activez cette option, cliquez sur **Suivant** puis sur **Fermer**

à l'étape 3, une icône de clé spéciale apparaît dans le nœud **Clés de groupe** du groupe actuel approprié. Vous pouvez maintenant utiliser cette clé dans les règles de chiffrement.

Remarque : Si vous sélectionnez l'option **Assigner la clé du groupe actuel**, celle-ci n'est effective que si vous avez appelé la fonction **Rechercher une clé** à partir du nœud **Clés de groupe** dans un groupe, et non à partir du nœud **Toutes les clés u.trust LAN Crypt**. En outre, des clés spécifiques peuvent être sélectionnées, mais elles ne seront pas assignées au groupe actuel. Si votre sélection contient une clé spécifique, un message correspondant s'affiche sur la dernière page de l'assistant.

3.7 Affichage des utilisateurs et des certificats sélectionnés

Le nœud **Utilisateurs et certificats sélectionnés** n'est disponible que si l'option *Afficher les « Utilisateurs et certificats sélectionnés »* est active dans les *paramètres utilisateur* de l'administration **u.trust LAN Crypt** (voir « *Paramètres utilisateur* » à la page 50).

Lorsque vous cliquez sur le nœud **Utilisateurs et certificats sélectionnés**, une boîte de dialogue s'affiche pour sélectionner les utilisateurs à afficher. Comme l'affichage de tous les utilisateurs peut prendre beaucoup de temps, *u.trust LAN Crypt* permet de définir des critères de recherche pour filtrer le processus de recherche.

Remarque : Si le système est configuré pour mettre en cache des listes d'utilisateurs, vous devez mettre à jour l'affichage via l'icône affichée dans la barre d'outils ou en appuyant d'abord sur **F5**, pour pouvoir entrer de nouveaux critères de recherche.

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

Les informations utilisateur suivantes seront extraites de la base de données *u.trust LAN Crypt* :

- Identifiant de connexion
- Nom d'utilisateur
- Affectation entre l'utilisateur et le certificat
- Demandeur du certificat
- Numéro de série du certificat
- Date à partir de laquelle le certificat est valide
- Date jusqu'à laquelle le certificat est valide
- Nom du groupe parent

Vous pouvez définir des critères de recherche en fonction de ces attributs. *u.trust LAN Crypt* recherche des chaînes de caractères définies dans les attributs utilisateur qui ont été récupérés.

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

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

Dans la liste déroulante sur le côté droit, vous pouvez entrer la chaîne de caractères d'*u.trust LAN Crypt* et chercher dans l'attribut défini.

Vous pouvez utiliser les caractères génériques SQL suivants pour saisir la chaîne de caractères :

%	toute séquence de caractères
_	caractère unique (par exemple, a__ signifie rechercher tous les noms contenant trois caractères et commençant par « a »)
[ ]	caractère unique d'une liste (par exemple, [a-cg]% signifie rechercher tous les noms commençant par « a », « b », « c » ou « g »)
[^]	caractère unique non contenu dans une liste (par exemple, [^a]% recherche tous les noms ne commençant pas par « a »)

Vous pouvez spécifier jusqu'à trois conditions pour le processus de recherche.

Si vous entrez plus d'une condition, vous pouvez définir comment ces conditions doivent être combinées (ET/OU).

Faites un clic droit sur **Utilisateurs sélectionnés et nœud de certificats** pour utiliser toutes les fonctions du composant logiciel enfichable de certificat disponibles pour chaque groupe individuel (voir « *Attribution de certificats* » à la page 163).

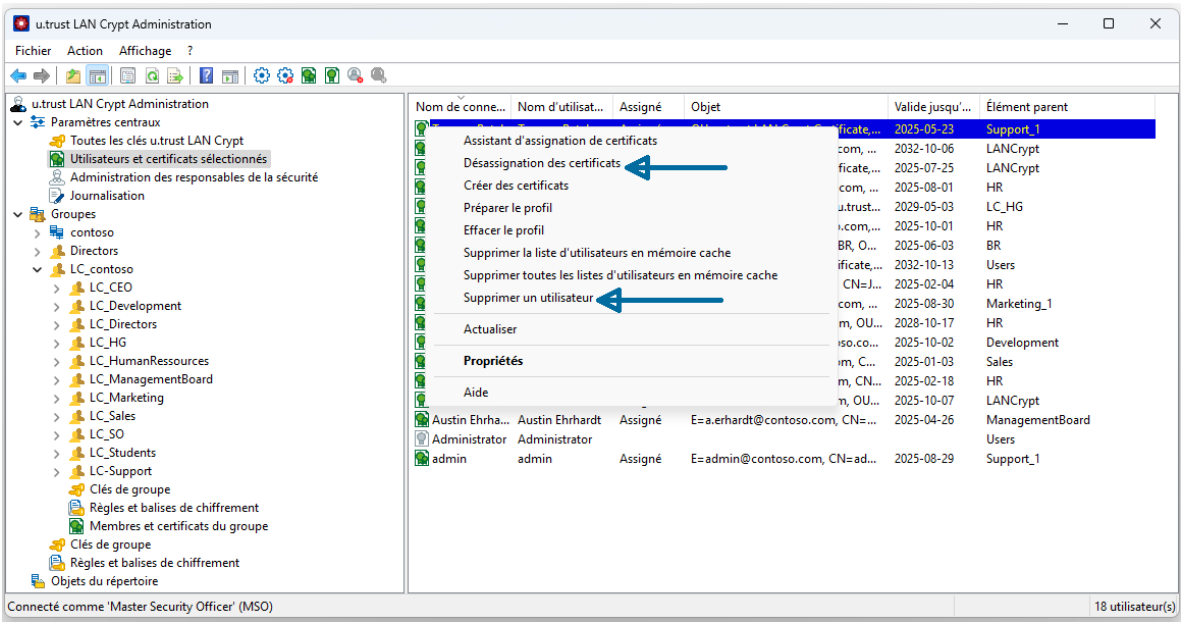
À ce stade, l'assistant d'attribution de certificat n'est disponible que pour les responsables principaux de la sécurité. Si un responsable de la sécurité dispose des autorisations appropriées, il peut utiliser le menu Propriétés pour attribuer un certificat à un utilisateur spécifique.

Cependant, si le responsable de la sécurité n'a aucune autorisation pour cet utilisateur, l'icône correspondante s'affiche.

3.7.1 Éléments de menu « Supprimer l'utilisateur » et « Supprimer » du menu contextuel

Pour les utilisateurs affichés dans la boîte de dialogue de droite dans le nœud **Utilisateurs et certificats sélectionnés**, les fonctions **Supprimer un utilisateur** et **Supprimer** sont disponibles via le menu contextuel si vous sélectionnez un ou plusieurs utilisateurs. Si un utilisateur n'a pas encore reçu de certificat, vous pouvez le reconnaître par son icône utilisateur

« grisée ». Les utilisateurs qui ont déjà un certificat valide peuvent être reconnus par le fait que leur icône d'utilisateur est affichée en « vert ».



Élément de menu « Désassignation des certificats » dans le menu contextuel

L'élément de menu **Désassignation des certificats** n'est disponible que pour les utilisateurs qui ont une icône d'utilisateur verte, jaune ou rouge. Avec **Désassignation des certificats**, vous pouvez supprimer l'affectation du certificat pour les utilisateurs précédemment marqués. Ensuite, la couleur de l'icône de l'utilisateur devient « grise » pour ceux-ci. Ces utilisateurs n'ont alors plus de certificat assigné.

Remarques : Un utilisateur peut également posséder plusieurs certificats. Avec **Désassignation des certificats**, tous les certificats attribués à l'utilisateur sont annulés. Avant de pouvoir fournir un nouveau profil à un tel utilisateur, vous devez d'abord lui attribuer un certificat.

Remarques : Si la couleur de l'icône de l'utilisateur est « rouge », cela signifie que le certificat de cet utilisateur a expiré. En revanche, si la couleur de l'icône de l'utilisateur est « jaune », cela signifie que le certificat de l'utilisateur affecté expirera bientôt (dans la période d'avertissement configurée).

Élément de menu « Supprimer un utilisateur » dans le menu contextuel

Avec la fonction **Supprimer un utilisateur**, vous pouvez supprimer un utilisateur existant dans la base de données *u.trust LAN Crypt*. Après avoir exécuté **Supprimer l'utilisateur**, l'utilisateur n'est plus affiché dans le nœud **Utilisateurs et certificats sélectionnés**.

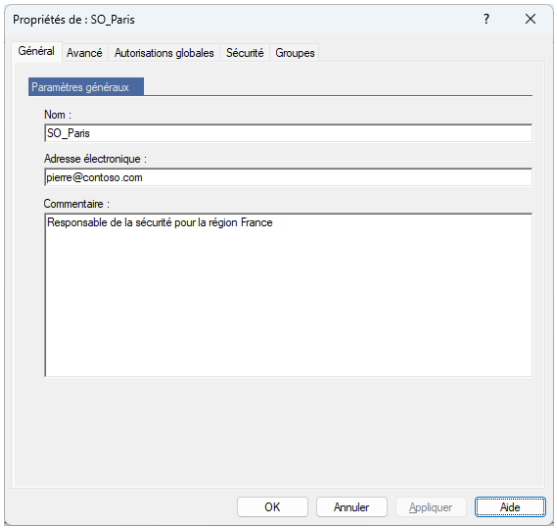
3.8 Créer un responsable de la sécurité

Les responsables principaux de la sécurité et les responsables de la sécurité habilités peuvent créer des responsables de la sécurité supplémentaires. Ces responsables de la sécurité peuvent ensuite être affectés à des unités administratives individuelles. Au départ, ils se voient accorder des droits globaux qui définissent précisément les tâches qu'ils peuvent accomplir. Une fois que les responsables de la sécurité ont été affectés à une unité organisationnelle (un objet dans l'administration *u.trust LAN Crypt*), les ACL peuvent être utilisées pour restreindre à nouveau leurs droits afin de répondre à cet objet particulier.

Remarque : Si les droits globaux d'un responsable de la sécurité ne lui permettent pas d'effectuer une action particulière, il n'est pas possible d'utiliser une ACL afin de lui accorder le droit pour cette action.

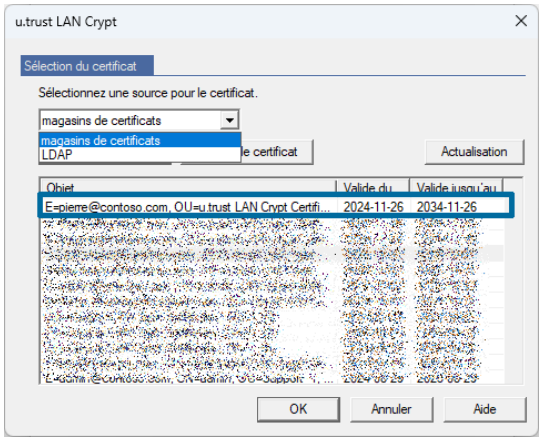
1. Pour créer un nouveau responsable de la sécurité (RS), sélectionnez le nœud **Administration des responsables de la sécurité**. Pour ouvrir la boîte de dialogue initiale afin de créer un responsable de la sécurité, cliquez sur **Ajouter un nouveau RS...** dans le menu contextuel de ce nœud, ou cliquez sur **Ajouter un nouveau RS...** dans le menu Action.

2. Dans cette boîte de dialogue, entrez un *nom* et, si nécessaire, une a*dresse électronique* et un *commentaire*. Cliquez ensuite sur **Suivant**.



Remarque : L'adresse électronique est ajoutée au fichier journal du mot de passe pour les certificats générés par *u.trust LAN Crypt*. Il peut par exemple être utilisé pour créer une lettre PIN par adresse électronique.

3. Maintenant, dans la boîte de dialogue, précisez si le nouveau responsable de la sécurité doit se voir accorder les droits d'un responsable principal de la sécurité. Un responsable principal de la sécurité a toujours tous les droits globaux existants. Cliquez sur le bouton **Parcourir** (« **…** ») pour sélectionner un certificat existant ou le faire générer par *u.trust LAN Crypt*.



Attribution de certificats à l'aide d'une source LDAP

u.trust LAN Crypt permet d'attribuer des certificats à partir de Microsoft Active Directory ou d'autres sources LDAP.

Pour ce faire, sélectionnez **LDAP** dans la liste déroulante de la boîte de dialogue Choisir un *certificat*.

Un champ d'édition s'affiche dans lequel 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_UO_1]*) représentent les UO dans la source LDAP. Pour afficher les certificats d'une UO, double-cliquez dessus.

Double-cliquez sur **[..]** pour monter d'un niveau dans la hiérarchie.

Sélectionnez un certificat et cliquez sur **OK**. Le certificat est maintenant attribué au responsable de la sécurité.

Remarque : Si le serveur LDAP n'autorise pas une connexion anonyme, vous devez entrer les identifiants du serveur dans l'onglet **Serveur** du nœud **Paramètres centraux**.

Remarque : Si vous utilisez *u.trust LAN Crypt* pour générer un certificat de chiffrement, ce responsable de la sécurité doit importer la clé privée sur son poste de travail à partir du fichier généré « *.p12 ».

Si le certificat de chiffrement a été attribué à partir d'un répertoire LDAP, la clé privée pertinente doit être présente sur le poste 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. Vous pouvez également cliquer sur le deuxième bouton **Parcourir** (« **…** ») pour sélectionner un certificat de signature existant ou demander à *u.trust LAN Crypt* d'en générer un nouveau pour vous.

Remarque : Si vous utilisez *u.trust LAN Crypt* pour générer un certificat de signature, ce responsable de la sécurité doit importer la clé privée sur son poste de travail à partir du fichier généré « *.p12 ».

Si le certificat de signature a été attribué à partir d'un répertoire LDAP, la clé privée pertinente doit déjà être présente sur le poste de travail du responsable de la sécurité. Le certificat de signature est utilisé pour la signature dans les profils générés et pour l'authentification lors de la connexion à l'API étendue.

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

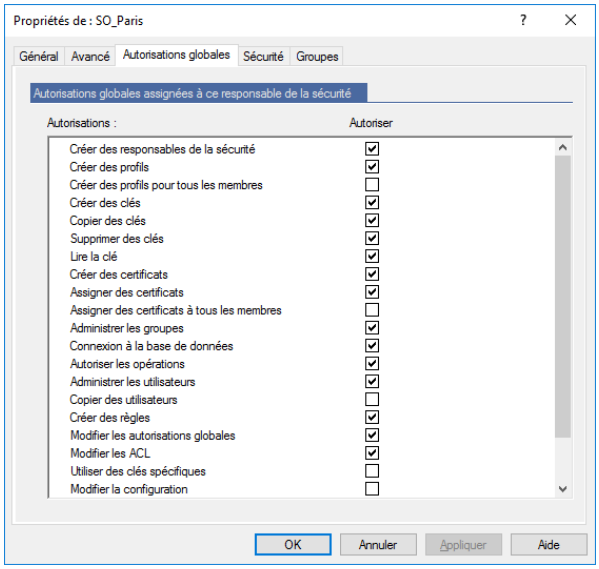
6. Si vous avez créé des sauvegardes de configuration individuelles pour les régions, vous pouvez maintenant en sélectionner une.

   Remarque : Le système affiche uniquement les configurations qui ont été générées pour la région sélectionnée.

7. Cliquez sur **Suivant**.

8. Dans la dernière boîte de dialogue de l'assistant, vous pouvez spécifier les actions que le responsable de la sécurité doit être en mesure d'effectuer. Toutes les autorisations globales requises pour les actions sélectionnées seront définies automatiquement.

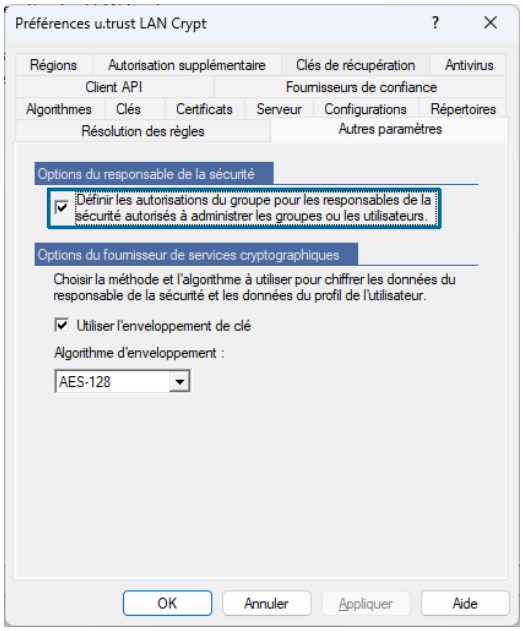
   Ces droits sont affichés dans les propriétés des responsables de la sécurité (double-cliquez sur un responsable de la sécurité pour les afficher) dans l'onglet **Autorisations globales**. Les autorisations globales peuvent être modifiées sur cette page.



Dans cette boîte de dialogue, si vous autorisez un responsable de la sécurité à effectuer une action spécifique, il se verra automatiquement accorder tous les droits nécessaires pour cette action.

Remarque : Pour qu'un agent de sécurité puisse traiter les groupes, des autorisations supplémentaires sont nécessaires (voir « *Accorder au responsable de la sécurité les autorisations pour traiter les groupes* » à la page 123.

Si un nouveau responsable de la sécurité reçoit l'autorisation globale *Administrer les groupes* ou *Administrer les utilisateurs* de cette manière, *u.trust LAN Crypt* crée automatiquement une ACL avec des droits d'affichage pour le groupe racine pour ce responsable de la sécurité, à condition que l'option *Définir les autorisations de groupe pour les responsables de la sécurité autorisés à administrer les groupes ou les utilisateurs* soit activée. Le responsable de la sécurité a ainsi la garantie de pouvoir accéder (afficher et/ou modifier) à tous les groupes dont il est responsable.



L'option *Définir les autorisations de groupe pour les responsables de la sécurité autorisés à administrer des groupes ou des utilisateurs* peut être activée dans l'onglet **Autres paramètres** du nœud **Paramètres centraux**.

9. Cliquez sur **Terminer**.

Le nouveau responsable de la sécurité est affiché dans l'administration *u.trust LAN Crypt*.

3.8.1 Octroi / modification des autorisations globales

Le responsable de la sécurité doit obtenir des droits globaux. Si le nœud **Administration des responsables de la sécurité** est sélectionné, tous les responsables de la sécurité existants sont affichés dans le volet de la console de droite. Double-cliquez sur un responsable de la sécurité pour ouvrir les onglets qui contiennent les propriétés qui leur sont attribuées.

Dans l'onglet **Autorisations globales**, vous accordez au responsable de la sécurité les « droits fondamentaux » nécessaires pour administrer *u.trust LAN Crypt*. Si, au moment de leur création, le responsable de la sécurité avait déjà le droit d'accomplir certaines actions, ces droits nécessaires sont déjà actifs.

Remarque : Veuillez noter qu'un responsable de la sécurité doit obtenir les autorisations pour le groupe, de la même manière que les Autorisations globales qui lui sont accordées, afin de pouvoir effectuer une certaine action (voir Section 3.11.3 « *Accorder au responsable de la sécurité les autorisations pour traiter les groupes* » à la page 123).

Exemple :

Pour qu'un responsable de la sécurité puisse importer des groupes et des utilisateurs, par exemple à partir de services d'annuaire, il doit disposer des droits de groupe « *Ajouter un groupe* » et « *Ajouter un utilisateur* » en plus des droits globaux « *Importer objets du répertoire* », « *Administrer les groupes* » et « *Administrer les utilisateurs* ».

Remarque : Un responsable principal de la sécurité a toujours toutes les autorisations globales existantes.

Un responsable de la sécurité peut se voir accorder les autorisations globales suivantes :

Remarque : Cliquez sur **Autoriser** pour sélectionner toutes les autorisations globales en même temps. Cliquez à nouveau pour désélectionner toutes les autorisations globales.

Autorisations	Description
Créer des responsables de la sécurité	Le responsable de la sécurité a la permission de créer plus de responsables de la sécurité.
Créer des profils	Le responsable de la sécurité a l'autorisation globale d'exécuter le résolveur de profil et de générer des fichiers de stratégie pour les utilisateurs individuels. Cette autorisation globale est la condition préalable pour définir l'autorisation *Créer des profils* pour un groupe spécifique pour un responsable de la sécurité. L'option *Créer des profils* permet au responsable de la sécurité de créer des profils pour les utilisateurs dans lesquels le responsable de la sécurité a le droit de *Créer des profils* pour le groupe parent de l'utilisateur (voir *« Groupe parent d'un utilisateur » à* la page 119*).* Cette autorisation est une condition préalable pour attribuer des valeurs aux clés. Un responsable de la sécurité qui n'a que l'autorisation de *Créer des clés* ne peut générer que des clés sans valeurs !
Créer des profils pour tous les membres	Cette autorisation nécessite que l'autorisation *Créer des profils* soit définie. Cette autorisation globale est la condition préalable pour définir l'autorisation *Créer des profils pour tous les membres* d'un groupe spécifique. L'option *Créer des profils pour tous les membres* permet à un responsable de la sécurité de créer des profils pour tous les utilisateurs dans lesquels le responsable de la sécurité a l'autorisation *Créer des profils* sur le groupe parent de l'utilisateur ou l'autorisation *Créer des profils pour tous les membres* sur l'un des groupes dont l'utilisateur est membre. **Remarque :** Comme l'autorisation globale *Créer des profils* est une condition préalable pour *Créer des profils pour tous les membres*, les éléments suivants s'appliquent : Si vous désactivez l'autorisation *Créer des profils*, l'autorisation *Créer des profils pour tous les membres* est automatiquement désactivée. Si vous activez l'autorisation *Créer des profils pour tous les membres*, l'autorisation *Créer des profils* est automatiquement activée.

Autorisations	Description
Créer des clés	Le responsable de la sécurité peut générer des clés dans les groupes individuels. Un responsable de la sécurité disposant de l'autorisation *Créer des clés* seul ne peut générer que des clés sans valeur ! Dans la console d'administration, des clés sans valeur peuvent être assignées aux règles de chiffrement. La valeur elle-même est générée lorsque des fichiers de stratégie sont générés. Pour générer des clés avec valeurs manuellement, le responsable de la sécurité doit avoir l'autorisation *Créer des profils*.
Copier des clés	Le responsable de la sécurité est autorisé à copier des clés.
Supprimer des clés	Le responsable de la sécurité peut supprimer des clés de groupes individuels.
Lire des clés	Le responsable de la sécurité peut voir les données des clés individuelles d'un groupe.
Créer des certificats	Le responsable de la sécurité peut générer des certificats pour les utilisateurs.
Attribuer des certificats	Le responsable de la sécurité est autorisé à assigner des certificats aux utilisateurs. Le responsable de la sécurité est autorisé à exécuter l'assistant permettant d'assigner des certificats. Cette autorisation globale est la condition préalable pour définir l'autorisation *Assigner des certificats* à un groupe spécifique pour un responsable de la sécurité. *Assigner des certificats* permet au responsable de la sécurité d'assigner des certificats aux utilisateurs lorsqu'il dispose du droit d'*assigner des certificats* pour le groupe parent de l'utilisateur (voir « *Groupe parent d'un utilisateur* » à la page 119).

Autorisations	Description
Assigner des certificats à tous les membres	Cette autorisation nécessite que l'autorisation *Assigner des certificats* soit définie. Cette autorisation globale est la condition préalable pour définir l'autorisation *Assigner des certificats à tous les membres* pour un groupe spécifique. *Assigner des certificats à tous les membres* permet à un responsable de la sécurité d'assigner des certificats à tous les utilisateurs lorsqu'il dispose du droit d'*assigner des certificats* pour le groupe parent de l'utilisateur ou d'*assigner des certificats à tous les membres* pour l'un des groupes dont l'utilisateur est membre. **Remarque :** Étant donné que l'autorisation globale *Assigner des certificats* est une condition préalable pour *Assigner des certificats à tous les membres*, ce qui suit s'applique : 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 à tous les membres*, l'autorisation *Assigner des certificats* est automatiquement activée.
Administrer les groupes	Le responsable de la sécurité peut apporter des modifications aux groupes. Ajout de sous-groupes, déplacement de groupes, synchronisation de groupes, suppression de groupes.
Connexion à la base de données	Le responsable de la sécurité peut se connecter à la base de données *u.trust LAN Crypt*. Le paramètre par défaut pour cette autorisation est Active. Avec cette autorisation, un responsable de la sécurité peut facilement apporter des modifications à la base de données *u.trust LAN Crypt* sans grande difficulté (par exemple, si le personnel quitte l'entreprise). Ce droit n'est pas accordé aux personnes qui ne sont autorisées à agir que si quelqu'un d'autre autorise leurs actions. Cela garantit que ces personnes ne peuvent autoriser que les actions qui nécessitent une confirmation, et n'ont aucun moyen d'apporter des modifications dans *u.trust LAN Crypt*.
Autoriser les opérations	Le responsable de la sécurité peut participer à des actions qui nécessitent une confirmation.

Autorisations	Description
Administrer les utilisateurs	Le responsable de la sécurité peut ajouter des utilisateurs à un groupe, les supprimer d'un groupe et synchroniser des groupes.
Copier des utilisateurs	Le responsable de la sécurité est autorisé à ajouter (copier) des utilisateurs à des groupes. Cette autorisation globale est la condition préalable pour définir l'autorisation *Copier les utilisateurs* pour un groupe spécifique pour un responsable de la sécurité. Pour ajouter un utilisateur à un groupe, le responsable de la sécurité doit disposer de l'autorisation *Copier les 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 accordés à un autre responsable de la sécurité.
Modifier les ACL	Le responsable de la sécurité peut modifier l'ACL d'un groupe.
Utiliser des clés spécifiques	Le responsable de la sécurité peut utiliser des clés spécifiques concrètes dans les règles de chiffrement. Il peut également afficher des clés spécifiques dans **Toutes les clés u.trust LAN Crypt**.
Modifier la configuration	Le responsable de la sécurité peut modifier la configuration (chemins). Cette autorisation est nécessaire pour afficher l'onglet **Configuration** dans les **Paramètres centraux**, et pour que le responsable de la sécurité puisse apporter des modifications dans l'onglet **Répertoires** s'il est connecté à la base de données.
Lire les entrées d'enregistrement	Le responsable de la sécurité peut afficher les paramètres utilisés pour l'enregistrement et les événements enregistrés.
Gérer l'enregistrement	Le responsable de la sécurité peut modifier les paramètres d'enregistrement. Il est autorisé à archiver, supprimer et vérifier les entrées.

Autorisations	Description
Importer des objets de répertoire	Le responsable de la sécurité peut importer des UO, des groupes et des utilisateurs à partir d'un service d'annuaire et les ajouter à la base de données *u.trust LAN Crypt*. Avant de pouvoir importer des objets du répertoire, le responsable de la sécurité a également besoin de l'autorisation *Administrer les groupes* et de l'autorisation *Administrer les utilisateurs*. Celles-ci sont définies automatiquement lorsque l'autorisation *Importer des objets du répertoire* est sélectionnée. Si un responsable de la sécurité n'a pas cette autorisation, le nœud **Objets du répertoire** (utilisé pour importer des UO, des groupes et des utilisateurs) n'est pas affiché dans la console d'administration.

Lors de l'octroi d'*autorisations globales*, veuillez noter les points suivants :

- Un responsable de la sécurité n'a pas d'autorisation globale, à moins que celle-ci ne lui ait été expressément accordée !
- Un responsable de la sécurité ne peut modifier que les autorisations qu'il possède personnellement.
- Un responsable de la sécurité ne peut pas modifier d'ACL décrivant ses propres autorisations.
- Certains droits ne peuvent être accordés que si vous disposez d'un autre droit. Lorsque vous sélectionnez ce type d'autorisation, l'autre autorisation est définie automatiquement.
- *u.trust LAN Crypt* peut être configuré pour créer automatiquement une ACL avec des droits d'affichage du groupe racine pour un nouveau responsable de la sécurité. Il est nécessaire que le responsable de la sécurité dispose de l'autorisation globale *Administrer le groupe* ou *Administrer les utilisateurs*. Cela garantit au responsable de la sécurité de pouvoir accéder (voir et/ou modifier) à tous les groupes dont il est en charge.

  Ce comportement doit être activé dans l'onglet **Autres paramètres** des **Paramètres centraux**.
- Si un responsable de la sécurité est modifié et reçoit l'autorisation globale *Administrer les groupes* ou *Administrer les utilisateurs* sans ACL pour le groupe racine, celle-ci est créée. L'ACL dispose de droits d'affichage pour le groupe. Les ACL existantes ne sont pas modifiées.

Sélectionnez les autorisations globales que vous souhaitez accorder au responsable de la sécurité et cliquez sur **Appliquer**.

Cliquez sur **OK** pour fermer la boîte de dialogue.

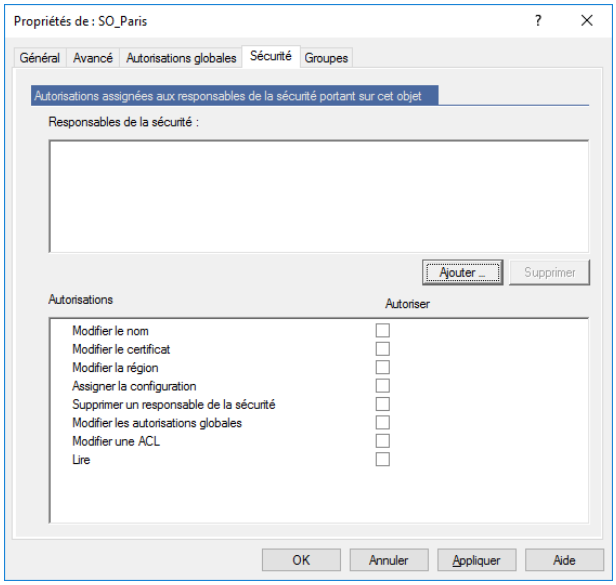
3.8.2 Autorisations de modification de paramètres pour un responsable de la sécurité

Les droits de modification des paramètres d'un responsable de la sécurité peuvent être transférés à d'autres responsables de la sécurité. Ce droit doit être expressément accordé à un responsable de la sécurité.

Remarque : Un responsable principal de la sécurité peut toujours modifier ces paramètres.

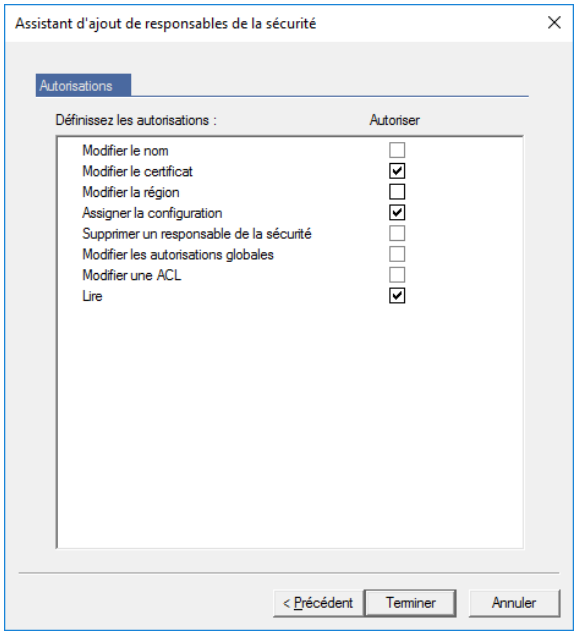
Les autorisations globales dont dispose un responsable de la sécurité particulier déterminent les autorisations qu'il peut modifier pour d'autres responsables de la sécurité. En outre, plusieurs autorisations peuvent être nécessaires pour effectuer une certaine fonction. Par exemple, si un responsable de la sécurité doit être autorisé à supprimer un autre responsable de la sécurité, ce responsable de la sécurité doit avoir la permission globale *Changer les ACL* et *Créer des responsables de la sécurité*.

Dans l'onglet **Sécurité**, vous pouvez définir les droits des autres responsables de la sécurité pour cet objet (= responsable de la sécurité). Dans la partie supérieure de la boîte de dialogue, vous pouvez voir les responsables de la sécurité qui ont le droit de modifier les paramètres de ce responsable de la sécurité.



1. Cliquez sur **Ajouter** pour exécuter un assistant afin d'ajouter un responsable de la sécurité. Sur la première page de l'assistant, sélectionnez le responsable de la sécurité dont vous avez besoin dans la liste des responsables de la sécurité existants.

2. Cliquez sur **Suivant** pour afficher la page sur laquelle vous spécifiez l'autorisation du responsable de la sécurité actuel de modifier cet objet (le responsable de la sécurité dont les paramètres sont en cours de traitement).

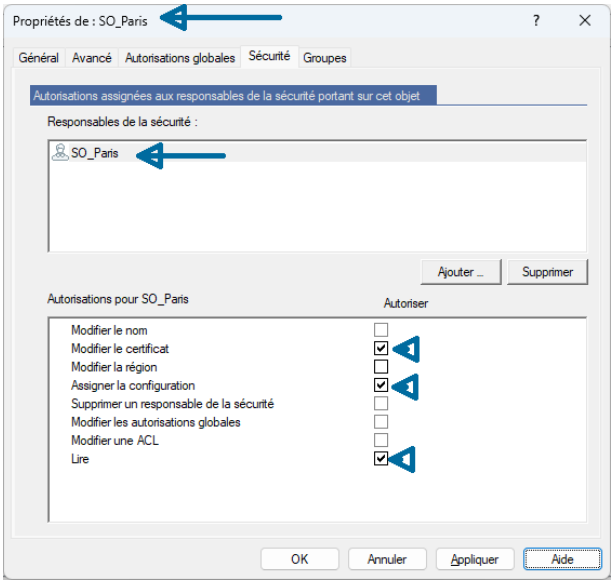


Remarque : Cliquez sur **Autoriser** pour sélectionner toutes les autorisations en même temps. Cliquez à nouveau pour désélectionner toutes les autorisations globales. Les paramètres d'autorisation globaux spécifient que les droits désactivés ne peuvent pas être accordés au responsable de la sécurité (voir « *Agrandissement / modification des autorisations globales* » à la page 92).

Autorisations	Description
Modifier le nom	Permet de modifier le nom du responsable de la sécurité auquel le propriétaire de l'autorisation est affecté.
Modifier le certificat	Permet de modifier le certificat du responsable de la sécurité à qui le propriétaire du droit est cédé.
Modifier de région	Permet de modifier le préfixe régional du responsable de la sécurité auquel le propriétaire du droit est affecté.
Assigner la configuration	Permet de modifier la configuration du responsable de la sécurité à qui le propriétaire du droit est attribué.
Supprimer le responsable de la sécurité	Permet de supprimer le responsable de la sécurité, à qui le propriétaire de l'autorisation est assigné.
Modifier les autorisations globales	Permet de modifier les autorisations globales du responsable de la sécurité auquel le propriétaire de l'autorisation est affecté.
Modifier une ACL	Permet de modifier les droits globaux de l'ACL à qui le propriétaire du droit est cédé.

Autorisations	Description
Lire	Affiche le responsable de la sécurité auquel le propriétaire de l'autorisation est affecté dans le nœud **Paramètres centraux** \ **Administration du responsable de la sécurité**. C'est la condition préalable à tous les droits qui permettent à ce responsable de la sécurité d'être traité. Ceci est défini automatiquement lorsqu'un droit de ce type est sélectionné.

Vous pouvez également accorder les autorisations **Modifier de certificat**, **Assigner la configuration** et **Lire** au responsable de la sécurité dont les propriétés sont définies ici. Avant que cela puisse se produire, ce responsable de la sécurité doit être présent sur la liste des responsables de la sécurité qui ont des droits sur cet objet (dans ce cas, ce responsable de la sécurité particulier).



Lire

Affiche le responsable de la sécurité spécifié dans le nœud **Paramètres centraux** \ **Administration du responsable de la sécurité**. Le responsable de la sécurité peut voir les autorisations qui lui ont été données.

Assigner la configuration

Permet au responsable de la sécurité de s'attribuer une configuration différente.

Modifier le certificat

La condition préalable à ce droit est d'obtenir l'autorisation **Lire**. Autorise le responsable de la sécurité à modifier son propre certificat.

Remarque : Les autorisations dont la case est grisée ne peuvent pas être accordées car le responsable de la sécurité sélectionné n'a pas les autorisations globales nécessaires pour le faire.

3. Accordez les droits appropriés au responsable de la sécurité en cliquant sur les cases à cocher, puis sur **Terminer**. Le système affiche désormais le responsable de la sécurité dans le volet supérieur de la page Sécurité. Dans le volet inférieur de la page, une ACL affiche les droits du responsable de la sécurité sélectionné.

3.8.3 Tous les droits pour les groupes / UO d'un responsable de la sécurité spécifique

Pour afficher les droits d'un responsable de la sécurité spécifique pour tous les groupes / UO pour lesquels le responsable de la sécurité a un droit, accédez au nœud **Administration du responsable de la sécurité** et double-cliquez sur le responsable de la sécurité concerné.

Dans la boîte de dialogue *Propriétés* des responsables de la sécurité, sélectionnez l'onglet **Groupes**. Cet onglet contient deux vues de liste :

- La vue de liste supérieure affiche tous les groupes / UO pour lesquels ce responsable de la sécurité a des autorisations.
- La deuxième vue de liste affiche les droits correspondants du responsable de la sécurité pour le groupe / l'UO sélectionnée.

De cette façon, vous pouvez facilement obtenir un aperçu de tous les droits d'un responsable de la sécurité spécifique pour les différents groupes de votre structure organisationnelle.

Remarque : Vous ne pouvez pas modifier les droits d'un responsable de la sécurité dans cette vue. La modification des droits n'est possible que dans la boîte de dialogue des propriétés d'un groupe.

Remarque : Seuls les groupes pour lesquels un responsable de la sécurité a des droits (**Autoriser** ou **Refuser**) sont affichés. Les groupes pour lesquels un responsable de la sécurité a hérité des droits ne sont pas affichés.

3.8.4 Modification ou renouvellement des certificats MSO ou SO

Les différentes façons de modifier ou de renouveler un certificat (M)SO sont décrites ci-dessous :

Variante 1 : Via l'administration des responsables de la sécurité

1. Démarrez l'administration *u.trust LAN Crypt* et connectez-vous en tant que responsable principal de la sécurité. Vous pouvez également vous connecter en tant que responsable de la sécurité si ce responsable de la sécurité a l'autorisation de modifier le certificat pour les responsables de la sécurité concernés. Cela peut également inclure le responsable de la sécurité lui-même, s'il a les autorisations appropriées et que son certificat est toujours valide.

2. Passez au nœud **Paramètres centraux** et allez ensuite au nœud **Administration des responsables de la sécurité**.

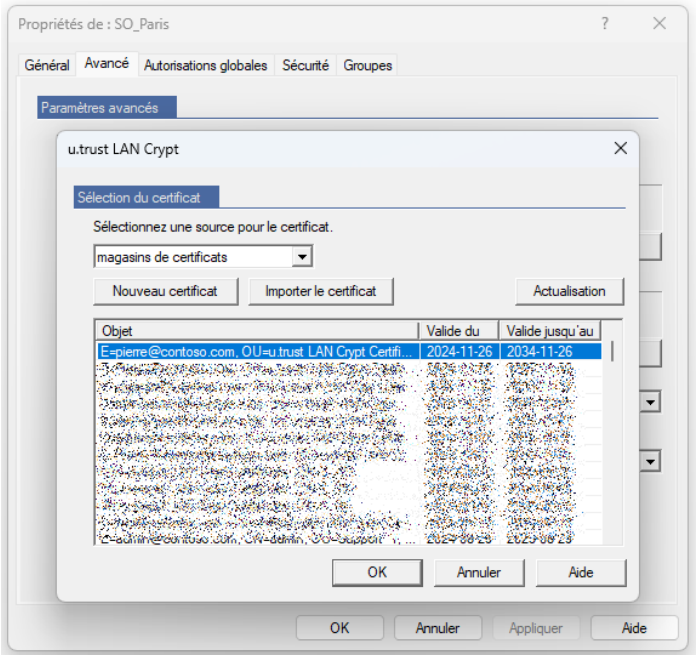
3. Faites un clic droit sur le responsable de la sécurité concerné et sélectionnez l'entrée *Propriétés* dans le menu contextuel.

4. Allez dans l'onglet **Avancé**.

5. Dans *Certificat de chiffrement*, cliquez sur le bouton **Parcourir** (« **…** ») pour sélectionner un nouveau certificat de chiffrement pour le responsable de la sécurité.

6. Vous pouvez également accéder au *Certificat de signature (facultatif)* et cliquer sur **Parcourir** (« **…** ») pour sélectionner un nouveau certificat de signature pour le responsable de la sécurité.

7. Sélectionnez le certificat préféré, sélectionnez ou créez un nouveau certificat. Vous pouvez également importer un certificat existant. Lorsque vous avez sélectionné le certificat pour le responsable de la sécurité, cliquez sur **OK**.



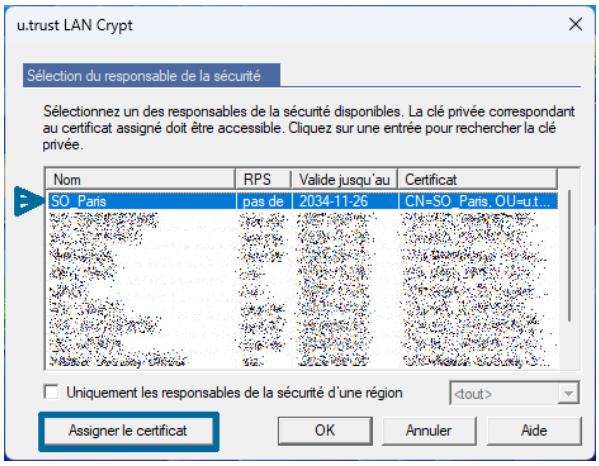
Remarque : Vous ne pouvez modifier les certificats de signature du responsable de la sécurité que dans la *variante 1* et non dans la *variante 2*.

Variante 2 : Utilisation de la clé de restauration

1. Démarrez l'administration *u.trust LAN Crypt*.

2. Dans la boîte de dialogue Responsable de la sécurité, sélectionnez le (M)SO dont vous avez besoin.

3. Cliquez sur le bouton **Assigner le certificat** et suivez les instructions de l'*Assistant de récupération de clés*.



En général, vous devez utiliser la *variante 1*. *La variante 2* est principalement destinée à être une méthode alternative et doit être utilisée dans les cas où aucun responsable de la sécurité disposant des autorisations appropriées n'est en mesure de se connecter à l'administration *u.trust LAN Crypt*.

Remarque : L'existence d'une clé de restauration est une condition préalable à la variante 2.

Quelle que soit la méthode utilisée, assurez-vous que le profil généré par le responsable de la sécurité est régénéré avant que l'ancien certificat n'atteigne sa date d'expiration. Sinon, les clients ne pourront plus charger le profil.

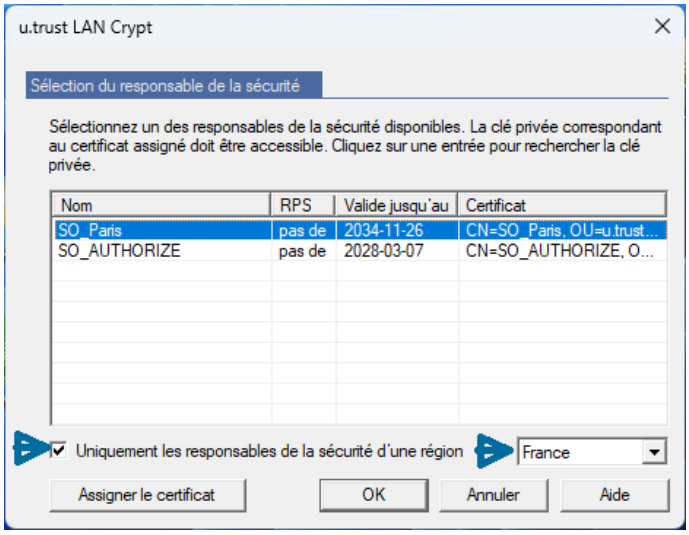
Cependant, vous pouvez autoriser l'assignation de certificats avec seulement une *autorisation supplémentaire*. Vous devez vous rappeler que ce type d'assignation prendra effet lors de la modification des certificats des responsables de la sécurité.

3.9 Connexion à l'administration

Pour se connecter à la console d'administration d'*u.trust LAN Crypt*, un responsable de la sécurité doit avoir l'autorisation globale de se *connecter à la base de données*. Les responsables principaux de la sécurité disposent toujours de cette autorisation, car ils bénéficient automatiquement de tous les droits disponibles.

Lorsque vous exécutez l'administration (*Démarrer/u.trust LAN Crypt Administration/Administration*), la boîte de dialogue de connexion s'affiche.

Tous les responsables de la sécurité autorisés sont affichés dans la liste. Si vous sélectionnez l'option **Uniquement les responsables de la sécurité d'une région** et sélectionnez cette région, seuls les responsables de la sécurité de cette région sont affichés.



Pour activer la connexion, le système doit accéder à la clé privée qui appartient au certificat (clé logicielle ou clé sur un jeton).

Après avoir sélectionné le responsable de la sécurité requis, cliquez sur **OK** pour ouvrir la console d'administration d'*u.trust LAN Crypt*.

Clé de récupération

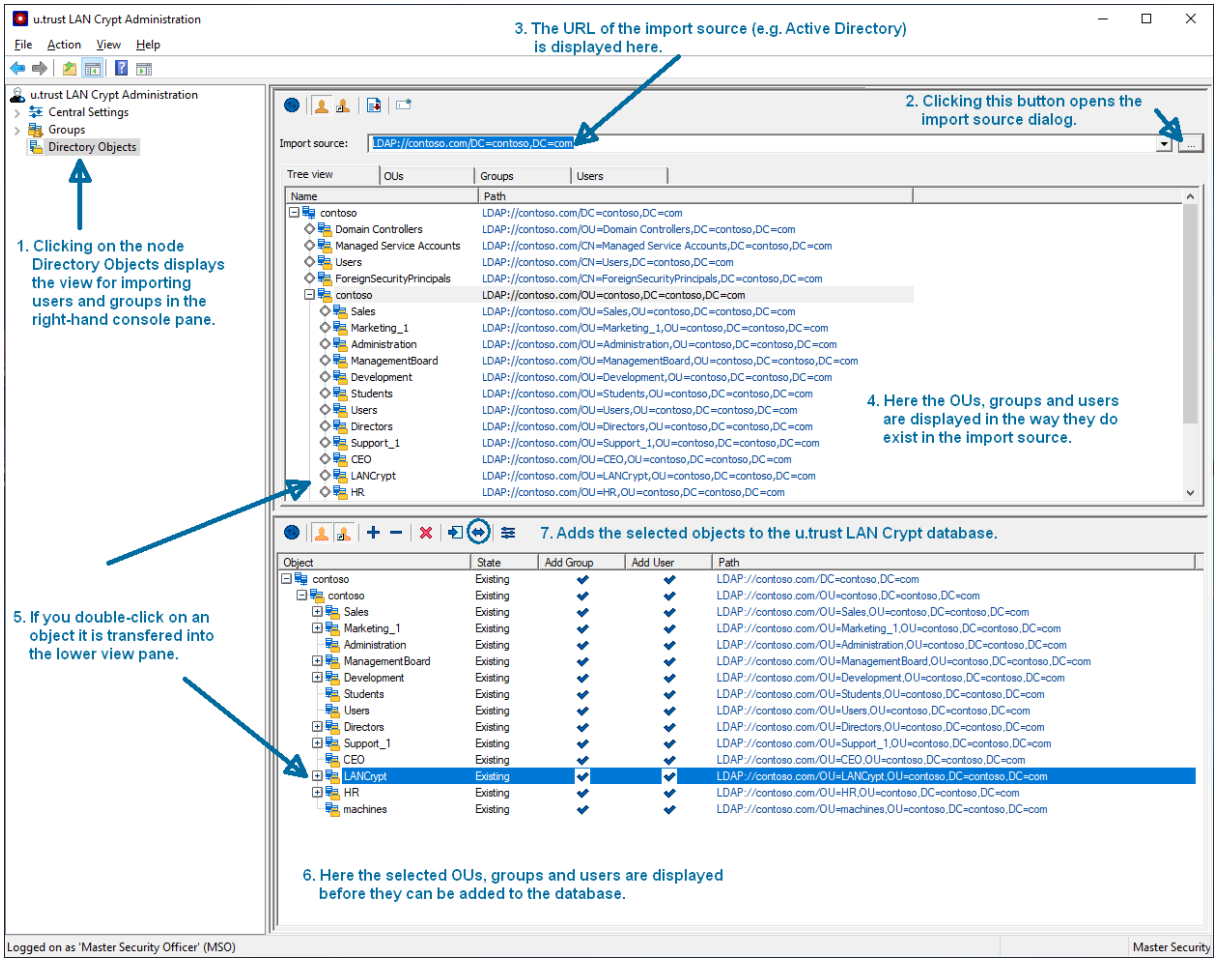
Si la clé appartenant au certificat d'un responsable de la sécurité a expiré, ou a été endommagée ou perdue, entrez une clé de récupération pour renouveler le certificat.

Remarque : Si un nouveau certificat est généré pendant le processus de récupération, ce certificat (et le mot de passe associé) est stocké dans le chemin configuré.

3.10 Importation de groupes et d'utilisateurs

Avec *u.trust LAN Crypt*, vous pouvez importer des groupes et des utilisateurs à partir de services d'annuaire accessibles via LDAP, à partir de domaines, ou les importer à partir d'un fichier créé manuellement qui contient les groupes et utilisateurs avec les dépendances particulières.

Cliquez sur **Objets du répertoire** pour afficher les boîtes de dialogue d'importation et d'assemblage des groupes à importer dans la base de données *u.trust LAN Crypt*, dans le volet droit de la console.



Remarque : Si un responsable de la sécurité connecté ne peut pas afficher le nœud **Objets du répertoire**, cela signifie qu'il n'a pas l'autorisation globale *Importer objets du répertoire*. Ce nœud n'apparaît dans la console d'administration que si ce responsable de la sécurité dispose de cette autorisation.

3.10.1 Importation de groupes et d'utilisateurs à partir d'un fichier

Les utilisateurs et les groupes peuvent être importés à partir d'un fichier créé manuellement qui contient les groupes et les utilisateurs avec des dépendances spécifiques. Les groupes et utilisateurs importés sont créés dans les nœuds **Groupes** et **Objets du répertoire** de la console d'administration d'*u.trust LAN Crypt*.

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** pour qu'u.trust LAN Crypt affiche une boîte de dialogue. Dans celle-ci, sélectionnez le fichier à partir duquel les utilisateurs et les groupes doivent être importés (voir « *Sélection de la source d'importation* » à la page 109).

Le fichier d'importation est un simple fichier texte sans extension de fichier spécifique (nous vous suggérons d'utiliser « **.lcg* » comme extension par défaut). Le contenu de ce fichier doit répondre à certaines exigences.

Format de fichier d'importation

Un fichier d'importation se compose de plusieurs sections. Les sections sont séparées par un nombre arbitraire de lignes vides.

Chaque section représente un utilisateur ou un groupe.

Chaque section se compose d'un en-tête et d'un nombre fixe de lignes, chacune commençant par un mot-clé. Les lignes doivent se terminer par un caractère de nouvelle ligne. Il peut n'y avoir aucune autre nouvelle ligne entre les lignes d'une section.

L'en-tête est le nom de la section entre crochets. Le nom de la section est utilisé pour définir l'affiliation des utilisateurs et des groupes.

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

Mots-clés	Description
type=	USER GROUP Définit si l'objet importé représente un utilisateur (USER) ou un groupe (GROUP).
name=	Définit le nom de connexion d'un utilisateur. Cela s'affiche sous *Nom de connexion* dans la console d'administration d'*u.trust LAN Crypt*.
display= facultatif	Permet de définir un nom d'utilisateur qui n'est pas identique au nom de connexion. Cela apparaît comme *Nom d'utilisateur* dans la console d'administration d'*u.trust LAN Crypt*. Si aucun nom n'est spécifié ici, le nom de connexion saisi sous *name=* apparaît sous *Nom d'utilisateur* dans la console d'administration d'*u.trust LAN Crypt*.
mail= facultatif	Permet de saisir l'adresse électronique de l'utilisateur. Cela apparaît dans l'onglet Détails des propriétés de l'utilisateur. **Remarque :** L'adresse électronique est ajoutée au fichier journal du mot de passe pour les certificats générés par *u.trust LAN Crypt*. Par exemple, il peut être utilisé pour créer une lettre PIN par courriel.

Mots-clés	Description
members=	Lorsque des groupes sont utilisés, cela définit quels utilisateurs et autres groupes sont membres d'un groupe particulier. Pour ajouter un membre, entrez le nom de la section qui identifie l'utilisateur ou le groupe (par exemple U_BKA,G_Utimaco). Entrez des virgules pour séparer le nom de chaque membre du groupe du suivant.

Remarque : Si vous tapez **//** au début d'une ligne, vous pouvez saisir un commentaire sur cette ligne n'importe où dans le fichier d'importation.

Remarque : Les entrées du fichier d'importation NE SONT PAS sensibles à la casse (ne faites pas de distinction entre les majuscules et les minuscules) !

Exemple :

```
[U_MB]
type=USER
name=MB
Display=Marie Bardot
Mail=mb@contoso.com
// mon commentaire…
[U_RS]
type=USER
name=RS
Mail=rs@contoso.com
[U_JG1]
type=USER
name=JG1
[U_RLU]
type=USER
name=RLU
[G_COMPANY]
type=GROUP
name=Groupe d'entreprises members=G_QA, G_PDM, U_JG1, U_MB
// mon commentaire… ...
[G_QA] type=GROUP name=QA members=U_RS, U_RLU, U_PW1
[G_HG] type=GROUP name=HG members=U_MB, U_PW1, U_RLU
```

3.10.2 Icônes du système d'administration

 Met à jour la vue dans la fenêtre actuelle.

 Affiche les utilisateurs dans des groupes particuliers.

 Affiche également les affiliations de groupes et d'utilisateurs dans des groupes particuliers.

Les affiliations dont l'objet n'est pas directement contenu dans le groupe sont grisées.

 Déplace l'objet sélectionné dans le volet inférieur. A le même effet que de double-cliquer sur l'objet sélectionné.

 Utiliser comme nouveau chemin.

Vous pouvez utiliser ce paramètre pour restreindre l'affichage de la structure. Si un nœud est sélectionné et que vous cliquez sur ce bouton, le système affiche uniquement la structure sous le nœud sélectionné. En outre, le chemin est ajouté à la liste déroulante afin que vous puissiez rapidement basculer à nouveau sur cet affichage.

 Affiche la structure arborescente.

 Ferme la structure arborescente.

 Supprime un objet sélectionné de la vue.

 Ajoute les objets affichés dans le volet inférieur droit à la base de données *u.trust LAN Crypt*.

 Synchronise les objets affichés dans le volet inférieur droit avec ceux déjà présents dans la base de données *u.trust LAN Crypt*.

 Ouvre la boîte de dialogue dans laquelle vous spécifiez les options de transfert.

Vous devez spécifier les options de transfert avant que les objets ne soient transférés à partir de la source d'importation.

3.10.3 Sélection de la source d'importation

Vous pouvez entrer l'URL du serveur à partir duquel les données doivent être importées directement dans le champ *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** pour qu'*u.trust LAN Crypt* affiche une boîte de dialogue dans laquelle vous pouvez sélectionner la source d'importation :

LDAP://

- **Domaine**

  Si l'ordinateur est membre d'un domaine Active Directory, cliquez sur ce bouton pour afficher la structure complète du domaine, tel qu'il est stocké sur le contrôleur de domaine.

  Remarque : Vous ne pouvez pas importer de groupes intégrés à partir d'Active Directory. Nous vous recommandons donc d'organiser les utilisateurs en UO (unités d'organisation) ou en groupes, et de les importer à la place.

- **Rechercher le conteneur**

  Si l'ordinateur est membre d'un domaine Active Directory, et que vous sélectionnez **Rechercher le conteneur…**, le système affiche le bouton **Parcourir** (« **…** »), sur lequel vous pouvez cliquer pour afficher une autre boîte de dialogue. Dans cette boîte de dialogue, vous pouvez ensuite sélectionner un nœud particulier dans la structure Active Directory.

WinNT://

- **Ordinateur**

  Affiche les groupes locaux et les utilisateurs de l'ordinateur sur lequel vous êtes actuellement connecté. De manière générale, ces groupes et utilisateurs ne sont utilisés qu'à des fins de test.

- **Domaine**

  Si l'ordinateur est membre d'un domaine Windows NT, cliquez sur ce bouton pour afficher la structure complète du domaine, tel qu'il est stocké sur le contrôleur de domaine.

  Remarque : Lors de l'utilisation du protocole WinNT, le système ne peut pas distinguer entre les utilisateurs renommés et les nouveaux utilisateurs pendant la synchronisation, car le protocole WinNT n'attribue pas de GUID uniques aux objets utilisateurs.

FICHIER://

- **Rechercher un fichier**

  Pour importer des utilisateurs et des groupes à partir d'un fichier, cliquez sur **Rechercher un fichier…** dans la boîte de dialogue *Importer la source*. Cliquez sur le bouton **Rechercher** pour sélectionner le fichier à partir duquel les utilisateurs et les groupes doivent être importés.

  Le fichier d'importation doit être d'un format spécifique pour vous permettre d'importer les utilisateurs et les groupes. Pour plus d'informations sur la création du fichier d'importation, voir « *Importation de groupes et d'utilisateurs à partir d'un fichier* » à la page 104).

  Une fois que vous avez sélectionné une source d'importation, cliquez sur le bouton **Transférer** pour afficher l'URL de la source, sous *Chemin*.

  Lorsque vous cliquez sur **OK**, *u.trust LAN Crypt* affiche les données sélectionnées dans le volet supérieur droit de la console. Dans cette vue, vous pouvez afficher les données sélectionnées dans une arborescence, organisée en UO, groupes et utilisateurs.

Uniquement pour le serveur LDAP

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

1. Sur la page **Serveur**, dans les **Paramètres centraux**, entrez le nom du serveur, ainsi que le nom et le mot de passe de l'utilisateur.
2. Pour LDAP ou SSL, précisez si l'implémentation <*Microsoft*> ou <*Novell*> est en cours d'utilisation.

   Remarque : L'importation depuis le service d'annuaire de Novell n'est plus supportée depuis la version 3.90 de LAN Crypt. D'autres fonctionnalités de Novell ne sont plus supportées et ne sont pas fonctionnelles dans l'administration.

3. Dans le champ d'entrée *Source d'importation*, saisissez l'adresse du serveur à partir duquel les données doivent être importées.

3.10.4 Préparation du transfert dans la base de données u.trust LAN Crypt

Dans le volet supérieur droit de la console, vous pouvez voir les UO, groupes et utilisateurs tels qu'ils sont stockés dans la source d'importation.

Ici, vous pouvez sélectionner lesquels de ces UO, groupes ou utilisateurs affichés doivent être importés dans la base de données *u.trust LAN Crypt*. Tout d'abord, déplacez les objets sélectionnés dans le volet d'affichage inférieur, où vous pouvez ensuite les traiter à nouveau.

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

3.10.4.1 Définition des paramètres de transfert de données

Pour optimiser les performances, vous pouvez définir des paramètres de transfert. Ces paramètres de transfert n'affectent que les transferts du volet d'affichage inférieur. Cela vous permet 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 comportant trois options :

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

  Ne s'applique que si des entrées sont déjà présentes dans la base de données, c'est-à-dire lorsque la base de données est en cours de synchronisation. Si cette option est sélectionnée, ce qui suit apparaît dans l'affichage inférieur de chaque objet :

  - S'il est déjà présent dans la base de données (dans la colonne *État*).
  - Si le responsable de la sécurité connecté dispose de l'autorisation de modifier un groupe (dans la colonne *Ajouter un groupe*). Une croix rouge indique que le responsable de la sécurité n'est pas autorisé à ajouter le groupe. Une coche verte signifie que le responsable de la sécurité est autorisé à *ajouter le groupe*.
  - Si le responsable de la sécurité connecté est autorisé à ajouter des utilisateurs (dans la colonne *Ajouter un utilisateur*). Une croix rouge indique que le responsable de la sécurité n'est pas autorisé à 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 affiche également les affiliations de groupe (groupes et utilisateurs qui ne sont pas membres directs des groupes individuels). Pour les distinguer des membres directs, ces éléments apparaissent sous forme d'icônes grisées.

  Remarque : Le système ne peut *calculer les affiliations* que jusqu'à leur transfert dans la base de données.

- **Trier les objets**

  Le tri alphabétique des entrées de groupes volumineux peut prendre un temps considérable. Par conséquent, les entrées ne sont généralement pas triées. Si vous souhaitez trier les objets par ordre alphabétique, sélectionnez cette option.

Mise à jour de l'affichage

Si aucune option n'a été définie pour le transfert, vous pouvez effectuer ces actions une fois celui-ci terminé, en cliquant sur le bouton **Actualiser**. Cliquez sur **Actualiser** pour ouvrir une boîte de dialogue comportant les mêmes options. La mise à jour n'affecte que les données du volet d'affichage inférieur.

3.10.4.2 Transfert d'objets dans le volet inférieur

Si vous double-cliquez sur un nœud, ou sélectionnez le nœud, puis cliquez sur le bouton **Transférer**, vous transférez les objets de la structure de la source d'importation vers le volet d'affichage inférieur.

Avant que les objets ne soient transférés, une boîte de dialogue apparaît. Celle-ci vous permet de spécifier la méthode de transfert des conteneurs et objets individuels.

- **Transférer uniquement cet objet**

  Ajoute l'objet sélectionné sans son contenu.

- **Transférer également les membres directs**

  Ajoute tous les objets présents dans le conteneur sélectionné.

- **Transférer les membres de manière récursive**

  Ajoute tous les objets qui sont présents dans ce conteneur ainsi que tous ceux qui sont membres et présents dans un autre conteneur. Les membres sont transférés avec toute leur hiérarchie.

Sélectionnez l'option requise et cliquez sur **OK** pour transférer les objets vers le volet d'affichage inférieur afin qu'ils soient prêts à être ajoutés à la base de données *u.trust LAN Crypt*.

Avant de les transférer dans la base de données, vous pouvez ajouter d'autres groupes à cette vue (par exemple, à partir d'autres sources), puis tout ajouter à la base de données en une seule étape.

3.10.4.3 Ajout de données à la base de données ou synchronisation des données

Les objets ne sont ajoutés à la base de données *u.trust LAN Crypt* qu'une fois regroupés dans le volet d'affichage inférieur et qu'une fois que vous avez cliqué sur le bouton **Ajouter dans la base de données** ou **Synchroniser**.

Remarque : Si vous ajoutez des objets à une structure existante, vous devez toujours commencer par les ajouter à la base de données. Pour ce faire, cliquez sur le bouton **Ajouter dans la base de données**.

La synchronisation n'est utilisée que si la seule modification concerne les relations entre les objets.

Lorsque vous cliquez sur **Ajouter dans la base de données**, le système ajoute les objets, puis lance le processus de synchronisation. Cela démarre avec une boîte de dialogue proposant trois options.

- **Synchroniser toute la base de données**

  Si vous sélectionnez cette option, le système synchronise toutes les entrées présentes dans la base de données *u.trust LAN Crypt* avec celles de la source d'importation. Les modifications apparaissent dans un autre écran qui s'affiche par la suite.

  Sélectionnez cette option si des objets ont été supprimés d'AD et qu'ils doivent également être supprimés de la base de données.

  Remarque : Si une structure complexe est impliquée, la synchronisation complète peut prendre beaucoup de temps.

- **Synchroniser uniquement les entrées visibles**

  Fait référence à la sélection dans le volet inférieur droit de la console d'administration.

- **Recalculer toutes les relations**

  Si vous sélectionnez cette option, le système recalcule toutes les affiliations en fonction de leur source d'importation, et les ajoute à nouveau dans la base de données. Les affiliations sont ajoutées même si elles ont été désactivées dans l'affichage du volet inférieur droit de la console (l'option **Calculer les affiliations** des paramètres de transfert a été désactivée).

- **Utiliser les relations visibles**

  Si vous sélectionnez cette option, seules les relations affichées dans le volet inférieur droit de la console sont ajoutées dans la base de données. Les « affiliations cachées » ne sont pas ajoutées dans la base de données (l'option **Calculer les affiliations** est désactivée dans les paramètres de transfert).

  Remarque : Si cette option est utilisée lors de la synchronisation et que les affiliations des objets présents dans la base de données n'apparaissent pas dans le volet inférieur droit de la console, toutes les affiliations présentes dans la base de données sont supprimées.

Lorsque vous sélectionnez une option et cliquez sur **OK**, le système affiche une boîte de dialogue qui documente la synchronisation. Vous devez confirmer les modifications dans cette boîte de dialogue.

- **Toutes les entrées**

  Affiche toutes les modifications d'une liste. Correspond au nombre total d'entrées sur les autres pages.

- **Objets supprimés**

  Affiche les objets qui ont été supprimés dans la source d'importation (serveur) depuis la dernière synchronisation, mais qui sont toujours présents dans la base de données *u.trust LAN Crypt*.

- **Nouvelles relations dans le répertoire**

  Affiche les objets et affiliations qui ont été ajoutés à la base de données *u.trust LAN Crypt*, ou les nouveaux 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 affiliations qui sont toujours présents dans la base de données mais qui ne se trouvent plus dans la source d'importation. Par exemple, les groupes peuvent avoir été supprimés ou les affiliations modifiées sur le serveur.

Remarque : L'exécution de la synchronisation n'évalue que les objets qui ont été importés au moins une fois d'une source d'importation vers la base de données.

Si des objets sont supprimés dans une source d'importation, ces modifications ne sont implémentées dans la base de données que si l'option *Synchroniser toute la base de données* est sélectionnée. Les groupes et utilisateurs ajoutés manuellement dans la console d'administration ne sont pas évalués lors de la synchronisation et n'apparaissent donc pas sur ces pages.

Vous pouvez annuler l'action pour chaque objet répertorié dans cette vue en cliquant sur l'action concernée (ce qui supprime la coche). Seules les actions sélectionnées (celles avec une coche) sont effectuées. Cliquez sur **OK** pour terminer l'exécution de la synchronisation des données.

Une fois les UO (unités d'organisation), groupes et utilisateurs importés, les responsables de la sécurité qui en ont la charge peuvent être assignés à chaque UO.

3.10.4.4 Ajout manuel de groupes

Pour ajouter un nouveau groupe manuellement, sélectionnez-le nœud/groupe auquel vous souhaitez ajouter le nouveau groupe, puis cliquez sur **Nouveau groupe** dans le menu contextuel.

Saisissez un nom pour le nouveau groupe dans le champ *Nom de groupe*, puis cliquez sur **OK**. Le système affiche désormais le groupe dans la console d'administration d'u.trust LAN Crypt.

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

Contrairement aux groupes importés, vous pouvez utiliser le glisser-déposer pour déplacer les groupes créés manuellement dans la hiérarchie du groupe.

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 groupe différent.

Un groupe inséré de cette façon apparaît sous forme de raccourci dans le groupe parent. En conséquence, les membres du groupe inséré héritent de toutes les clés et règles de chiffrement du groupe parent. La condition préalable pour hériter de clés est que celles-ci soient définies comme pouvant être héritées dans le groupe parent. Les droits d'édition du groupe ne sont PAS hérités.

Étant donné que ce groupe n'est inséré dans le nouvel emplacement qu'en tant que raccourci, les règles de chiffrement, les membres, les certificats et les clés ne sont pas affichés. Ces valeurs ne sont visibles que dans le groupe « réel » de la hiérarchie. Il est également possible d'y utiliser les clés héritées pour 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 également créer le raccourci en appuyant sur *Ctrl* et en effectuant un *glisser-déposer* du groupe sur le groupe cible.

3. Le système vous demandera de confirmer que vous souhaitez ajouter le groupe. Cliquez sur **OK** pour confirmer.

4. Le groupe apparaît désormais en tant que raccourci sous l'autre groupe.

De cette façon, vous pouvez facilement accorder à tous les membres d'un groupe tous les droits d'un groupe différent.

Par exemple : si vous souhaitez accorder aux membres de l'*équipe 1* les mêmes droits qu'aux membres de l'*équipe 2* pour une durée limitée (par exemple, pour que l'*équipe 1* puisse

assister l'*équipe 2* dans un projet), ajoutez simplement un raccourci au groupe de l'*équipe 1* dans le groupe de l'*équipe 2*. Générez ensuite de nouveaux fichiers de stratégie. Lors de leur prochaine connexion, les membres de l'*équipe 1* auront accès aux données de l'*équipe 2*.

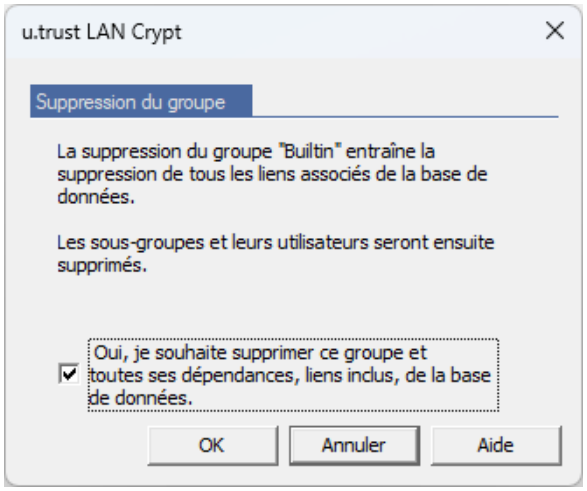
Lorsque l'*équipe 1* n'a plus besoin des droits supplémentaires, vous pouvez supprimer le raccourci du groupe de l'*équipe 2* et générer de nouveaux fichiers de stratégie. Les membres de l'*équipe 1* n'ont alors plus accès aux données de l'équipe 2.

3.10.5 Suppression de groupes

Vous pouvez supprimer des groupes/UO individuels ainsi que les raccourcis vers des groupes/UO dans la console d'administration d'*u.trust LAN Crypt*.

Pour **supprimer un groupe**, sélectionnez **Supprimer** dans le menu contextuel de ce groupe. Toutes les affiliations de sous-groupes et utilisateurs seront supprimées. Les utilisateurs eux-mêmes ne seront supprimés que si une UO est supprimée dans la console d'administration d'*u.trust LAN Crypt*. Dans ce cas, toutes les affiliations d'utilisateurs qui pourraient exister dans d'autres UO sont également supprimées. Les clés ne sont JAMAIS supprimées. Elles restent dans la base de données *u.trust LAN Crypt*.

Avant la suppression du groupe, une boîte de dialogue apparaît. Dans celle-ci, vous devez confirmer que vous souhaitez supprimer le groupe.



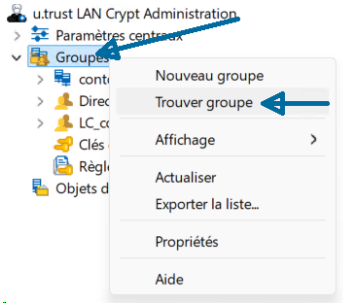
Pour **supprimer un raccourci** vers un groupe, cliquez sur **Supprimer** dans le menu contextuel du raccourci. Seul le raccourci est supprimé. Le groupe lui-même n'est pas affecté. Avant la suppression d'un raccourci, une boîte de dialogue s'affiche pour vous demander de confirmer cette action.

Le menu contextuel du groupe parent contient l'entrée **Supprimer les liens**, qui vous sert à supprimer un raccourci.

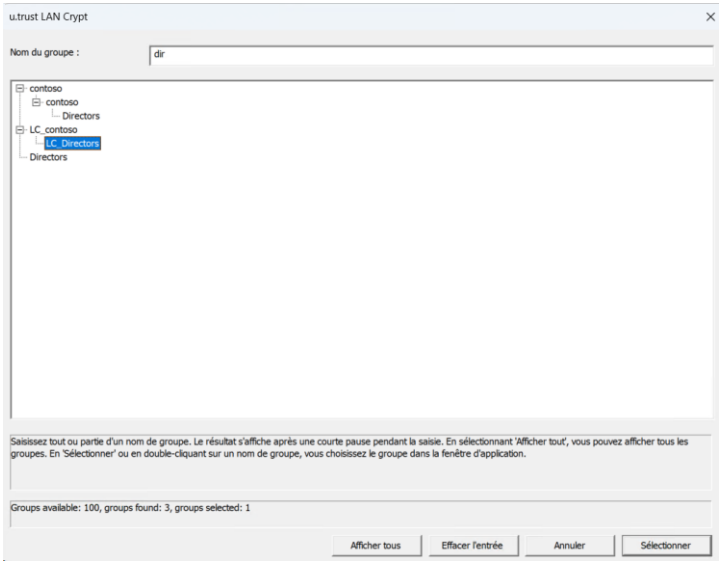
Cliquez sur **Supprimer les liens** pour supprimer tous les raccourcis vers ce groupe. Le groupe lui-même n'est pas affecté.

3.10.6 Trouver groupe

La fonction **Trouver groupe** vous permet de rechercher un groupe particulier. Cliquez avec le bouton droit de la souris sur le nœud **Groupes** et sélectionnez **Trouver groupe**.



Le dialogue suivant apparaît :



Saisissez tout ou partie d'un nom de groupe dans le champ de saisie supérieur. Le résultat s'affiche après une courte pause pendant la saisie. En sélectionnant **Afficher tous**, vous pouvez afficher tous les groupes. En **Sélectionner** ou en double-cliquant sur un nom de groupe, vous choisissez le groupe dans la fenêtre d'application.

Remarque : La fonction Trouver groupe est uniquement disponible dans le nœud principal du groupe. Cependant, cette fonction n'est pas affichée dans le menu contextuel des groupes qui lui sont inférieurs.

3.10.7 Icônes de groupe

Les UO et les groupes sont représentés par différentes icônes dans la console d'administration d'*u.trust LAN Crypt*, selon leur source d'importation :

 L'icône de serveur indique la source à partir de laquelle les UO et les groupes ont été importés.

 Icônes de raccourci vers le serveur (lien créé par copie).

 Icône d'UO importée à partir d'un serveur.

 Raccourci vers une UO importée.

 Icône de groupe importé à partir d'un serveur.

 Raccourci vers le groupe importé.

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

 Raccourci vers le fichier importé.

 Icône de groupe importé à partir d'un fichier.

 Raccourci vers le groupe importé.

 Groupe qui a été ajouté manuellement.

 Raccourci vers un groupe qui a été ajouté manuellement.

3.11 Assignation de responsables de la sécurité aux unités d'organisation

Une fois les UO, groupes et utilisateurs importés dans l'administration *u.trust LAN Crypt*, les responsables principaux de la sécurité peuvent assigner des responsables de la sécurité individuels aux différentes unités d'organisation.

Le responsable de la sécurité peut alors utiliser les droits qui lui ont été octroyés pour traiter les unités d'organisation auxquelles il a été assigné.

Pour s'assurer qu'un responsable de la sécurité peut uniquement modifier l'unité d'organisation dont il est en charge, le responsable principal de la sécurité peut lui « cacher » les autres nœuds. Cela signifie que le nœud est visible mais ne peut pas être modifié.

Si le responsable de la sécurité se connecte à l'administration u.trust LAN Crypt, il ne peut voir que la partie de la structure organisationnelle dont il est en charge.

3.11.1 Groupe parent d'un utilisateur

Dans *u.trust LAN Crypt*, un utilisateur peut être membre de plus d'un groupe, 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'UO à laquelle l'utilisateur appartient.
- Lors de l'importation de l'utilisateur via un fichier, le groupe parent est le groupe dont l'utilisateur est membre, tel que défini dans le fichier.
- Lors de la création d'un utilisateur via la boîte de dialogue des propriétés du groupe, le groupe parent est le groupe à partir duquel la boîte de dialogue des propriétés du groupe a été ouverte.

Dans la console d'administration d'*u.trust LAN Crypt*, le groupe parent est affiché en tant que colonne dans le nœud **Utilisateurs et certificats sélectionnés** ou dans le nœud **Membres et certificats du groupe** (lorsqu'il est configuré dans l'onglet **Paramètres d'utilisateur**, voir « *Paramètres d'utilisateur* » à la page 50).

Le groupe parent d'un utilisateur influe sur 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 lorsqu'ils disposent des droits 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 sous couvert qu'ils disposent de l'autorisation globale *Administrer les utilisateurs* et des autorisations *Ajouter un utilisateur* et Supprimer un utilisateur sur le groupe parent de l'utilisateur.

- Création de profils : Si Créer des profils est défini pour un groupe pour un responsable de la sécurité, ce dernier est autorisé à créer des profils pour tous les membres du groupe, à condition que le groupe est également l'objet parent du groupe. Ainsi, le responsable de la sécurité n'est pas autorisé à créer des profils pour les utilisateurs qui ne sont que des membres du groupe et qui ont un groupe parent différent. Pour ce faire, l'autorisation *Créer des profils pour tous les membres* est requise.

- Assigner des certificats : Si *Assigner des certificats* est défini pour un groupe, le responsable de la sécurité est autorisé à assigner des certificats à tous les membres du groupe, à condition que le groupe soit également l'objet parent du groupe. Ainsi, le responsable de la sécurité n'est pas autorisé à assigner des certificats aux utilisateurs qui ne sont que des membres du groupe et qui ont un groupe parent différent. Pour ce faire, l'autorisation *Assigner des certificats à tous les membres* est requise.

- Copier des utilisateurs : Lorsqu'un responsable de la sécurité souhaite ajouter un utilisateur à un groupe par le biais de la boîte de dialogue des propriétés d'un groupe (sous l'onglet **Membres**, via le bouton **Ajouter**), le responsable de la sécurité doit disposer de l'autorisation *Copier les utilisateurs* pour le groupe parent de l'utilisateur.

3.11.2 Permettre à un responsable de la sécurité de consulter et de modifier des groupes

1. Pour permettre à un responsable de la sécurité de consulter un nœud dans l'administration, vous devez d'abord définir le droit **Visible** dans le nœud de base dans la structure de l'organisation.

2. Pour ce faire, sélectionnez le nœud de base dans la structure et cliquez sur **Propriétés** dans le menu contextuel afin d'ouvrir la boîte de dialogue *Propriétés* de ce nœud.

3. Accédez à l'onglet **Sécurité**, puis cliquez sur **Ajouter**.

   Cet onglet permet de sélectionner le responsable de la sécurité que vous souhaitez assigner au traitement des groupes.

   Remarque : Plusieurs responsables de la sécurité peuvent être assignés au même groupe.

4. Cliquez sur **Suivant** pour afficher la boîte de dialogue *Autorisations* de ce responsable de la sécurité. Sélectionnez l'autorisation *Visible*, puis cliquez sur **Terminer**. Cette autorisation est héritée vers le bas dans la hiérarchie des groupes, ce qui signifie que le responsable de la sécurité peut désormais visualiser tous les groupes.

   Si le responsable de la sécurité se connecte à la base de données avec ces paramètres, il peut voir toute la structure d'administration, mais ne peut pas la modifier.

5. Dans l'étape suivante, vous pouvez maintenant masquer (supprimer) les groupes dans la console d'administration que vous ne voulez pas que le responsable de la sécurité voie parce qu'il n'a aucun droit d'accès.

6. Pour ce faire, sélectionnez ces groupes, ouvrez leurs boîtes de dialogue *Propriétés* et sélectionnez l'onglet **Sécurité**.

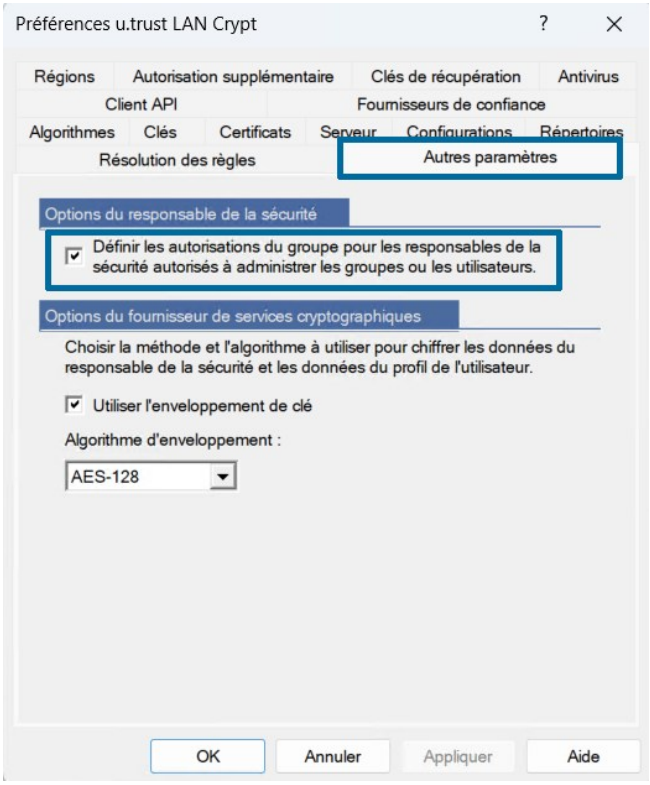
7. Ici, choisissez **Visible** pour **Refuser** les groupes qui doivent être cachés au responsable de la sécurité.

Remarque : Si un responsable de la sécurité s'est vu explicitement refuser un droit à un groupe hiérarchiquement supérieur, ce droit ne peut pas être attribué à un groupe subordonné. Nous vous recommandons donc d'assigner uniquement les autorisations **Lecture** et **Affichage** du responsable de la sécurité à un groupe hiérarchiquement supérieur afin qu'il puisse assigner des droits à des groupes subordonnés sans causer de problèmes.

Remarque : *u.trust LAN Crypt* peut être configuré pour créer automatiquement une ACL contenant la droite visible sur le groupe racine pour un responsable de la sécurité nouvellement créé. Il est nécessaire que le responsable de la sécurité dispose de l'autorisation globale *Administrer les groupes* ou *Administrer les utilisateurs*. Cela garantit que le responsable de la sécurité peut accéder (voir et/ou modifier) à tous les groupes dont il est responsable.

Ce comportement doit être activé dans l'onglet **Autres paramètres** du nœud **Paramètres centraux**.

Exemple (Responsable principal de la sécurité) :



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

Seuls les groupes pour lesquels le responsable de la sécurité a l'autorisation **Visible** sont affichés. Ces groupes sont grisés parce que, pour l'instant, le responsable de la sécurité n'a pas le droit de les traiter.

Si l'autorisation **Visible** et l'autorisation **Lecture** ont été attribuées au responsable de la sécurité en même temps, le système afficherait également les composants logiciels

enfichables pour les *Règles de chiffrement*, les *Membres et les certificats pour le groupe* et les *Clés de groupe* sous les groupes. Le responsable de la sécurité peut voir le contenu des composants logiciels enfichables, mais ne peut pas les modifier.

Vous pouvez utiliser l'autorisation **Lecture** pour donner à un responsable de la sécurité des informations sur d'autres groupes sans lui permettre de modifier ces groupes : le système inclut simplement ces informations dans la vue du responsable de la sécurité.

Remarque : Si le responsable de la sécurité a également obtenu l'autorisation **Lecture**, vous devez spécifiquement le refuser à nouveau pour cacher les groupes une nouvelle fois. Il ne suffit pas de refuser simplement l'autorisation **Visible**.

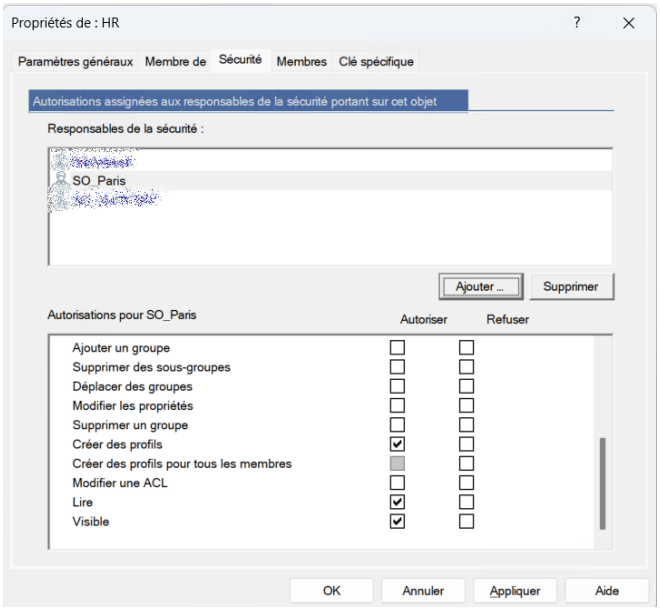
3.11.3 Accorder au responsable de la sécurité les autorisations pour traiter les groupes

Une fois que vous avez configuré le responsable sécurité pour qu'il voie les groupes qu'il doit modifier, vous pouvez lui attribuer les autorisations appropriées.

Ces autorisations sont héritées vers le bas dans la hiérarchie de l'organisation et vous pouvez les refuser à un autre endroit, plus bas dans la hiérarchie.

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

2. Sous Responsables sécurité, vous voyez tous les responsables de la sécurité qui sont affectés à ce groupe. 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 marquées d'une coche grise. Les cases à cocher complètement grisées signalent des autorisations qui ne peuvent être accordées, en raison des paramètres des droits globaux.

Remarque : Les paramètres des autorisations globales définissent les autorisations qui peuvent être attribuées à un responsable de la sécurité particulier. Les droits globaux sont définis lors de la création du responsable de la sécurité.

Remarque : Cliquez sur **Autoriser / Refuser** pour autoriser ou refuser toutes les autorisations. Cliquez à nouveau pour désélectionner toutes les autorisations globales. Si tous les droits sont sélectionnés, vous pouvez les sélectionner/désélectionner ultérieurement si nécessaire. Les paramètres d'autorisation globale définissent que les droits désactivés ne peuvent pas être accordés au responsable de la sécurité.

Vous pouvez attribuer les autorisations suivantes :

Autorisations	Description
Créer une clé	Le responsable sécurité est autorisé à générer des clés dans le groupe.
Copier des clés	Le responsable de la sécurité est autorisé à copier des clés.
Supprimer la clé	Le responsable de la sécurité est autorisé à supprimer des clés.
Créer des règles	Le responsable de la sécurité est autorisé à générer des règles de chiffrement pour les utilisateurs.
Attribuer des certificats	Le responsable de la sécurité est autorisé à assigner des certificats aux utilisateurs. Le responsable de la sécurité est autorisé à exécuter l'*assistant permettant d'attribuer des certificats*. Cette autorisation permet au responsable de la sécurité d'assigner des certificats aux utilisateurs du groupe là où le groupe est également le groupe parent.
Attribuer des certificats à tous les membres	Cette autorisation nécessite que l'autorisation *Assigner des certificats* soit définie. *Assigner des certificats à tous les membres* permet au responsable de la sécurité d'assigner des certificats à tous les utilisateurs du groupe : les utilisateurs dont le groupe est le groupe parent ainsi que ceux qui sont membres du groupe et ont un groupe parent différent. **Remarque :** Si vous définissez *Assigner des certificats à tous les membres* sur **Autoriser**, l'autorisation *Assigner des certificats* est automatiquement définie sur **Autoriser**. Si vous définissez *Assigner des certificats* sur **Refuser**, l'autorisation *Assigner des certificats à tous les membres* est automatiquement définie sur **Refuser**.

Autorisations	Description
Ajouter un utilisateur	Le responsable de la sécurité est autorisé à ajouter manuellement des utilisateurs au groupe. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Copier des utilisateurs	Le responsable de la sécurité a l'autorisation d'ajouter des utilisateurs de ce groupe à un autre groupe. Cela n'est autorisé que pour les membres dont ce groupe est également l'objet parent.
Supprimer un utilisateur	Les responsables de la sécurité sont autorisés à utiliser le composant logiciel enfichable des *membres et certificats de groupe* pour supprimer des utilisateurs. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des 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 des utilisateurs.
Supprimer des sous-groupes	Le responsable de la sécurité est autorisé à supprimer les sous-groupes de ce groupe. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Déplacer des groupes	Le responsable de la sécurité est autorisé à déplacer des groupes créés manuellement dans l'administration (avec une action de *glisser-déposer*). Les groupes importés ne peuvent pas être déplacés. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Modifier les propriétés	Le responsable de la sécurité est autorisé à modifier les propriétés d'un groupe.

Autorisations	Description
Supprimer un groupe	Le responsable de la sécurité est autorisé à supprimer des groupes. Cela suppose que le responsable de la sécurité a supprimé l'autorisation « *Supprimer des sous-groupes* » dans le groupe du dessus. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Créer des profils	Le responsable de la sécurité a l'autorisation d'exécuter le résolveur de profil 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, là où le groupe est également le groupe parent.
Créer des profils pour tous les membres	Cette autorisation nécessite que l'autorisation *Créer des profils* soit définie. *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 également les utilisateurs qui sont membres du groupe et ont un groupe parent différent. **Remarque :** Si vous définissez *Créer des profils pour tous les membres* sur **Autoriser**, l'autorisation *Créer des profils* est automatiquement définie sur **Autoriser**. Si vous définissez *Créer des profils* sur **Refuser**, l'autorisation *Créer des profils pour tous les membres* est automatiquement définie sur **Refuser**.
Modifier une ACL	Le responsable de la sécurité est autorisé à modifier la liste de contrôle d'accès du groupe (par exemple, en ajoutant un autre responsable de la sécurité).
Lire	Le responsable de la sécurité dispose de droits de lecture sur ce groupe et peut consulter le contenu des composants logiciels enfichables. Est défini automatiquement si les autorisations de modification sont accordées.
Visible	Le responsable sécurité peut consulter le groupe. Est défini dans le nœud de base et hérité vers le bas. Si le responsable de la sécurité n'est pas autorisé à consulter le groupe, ce dernier est alors masqué (« *Lecture* » doit également être défini sur **Refuser**).

3. Sélectionnez les autorisations que vous souhaitez assigner au responsable de la sécurité. Cliquez sur **Appliquer** pour stocker les paramètres dans la base de données.

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

Remarque : Les modifications apportées aux autorisations d'un responsable de la sécurité pour un groupe ne deviennent effectives qu'après que le responsable de la sécurité concerné s'est de nouveau connecté à l'administration *u.trust LAN Crypt*.

3.12 Propriétés des groupes

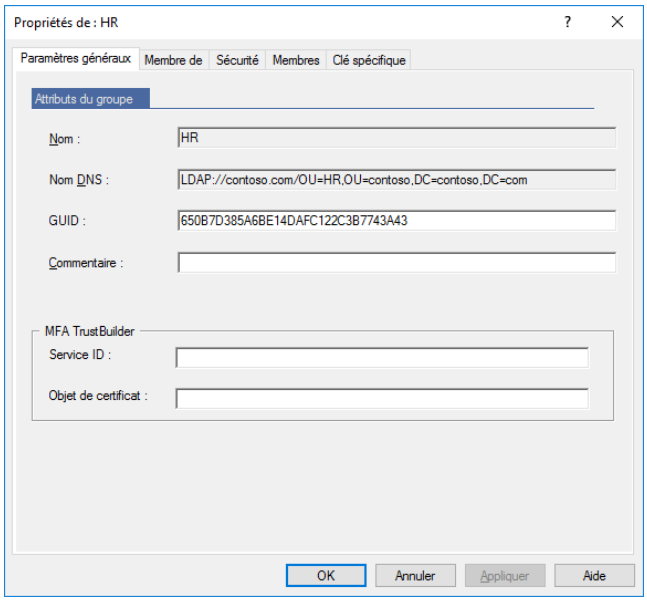
La boîte de dialogue des *Propriétés* d'un groupe (<Groupe>/Menu contextuel/Propriétés) se compose de quatre onglets dans lesquels vous pouvez modifier les propriétés d'un groupe.

3.12.1 Onglet Propriétés

L'onglet **Propriétés** affiche le

- Nom
- Nom DNS
- GUID
- Commentaire
- Service ID (MFA TrustBuilder)
- Objet de certificat (MFA TrustBuilder)

pour le groupe.



TrustBuilder MFA et u.trust LAN Crypt

Dans la section *MFA TrustBuilder*, vous définissez les spécifications pour l'authentification multi-facteurs des utilisateurs avec *TrustBuilder*.

Grâce au support de MFA (**M**ulti-**F**actor **A**uthentification), les utilisateurs peuvent se connecter au client *u.trust LAN Crypt* de manière particulièrement sécurisée. La connexion elle-même est alors effectuée à l'aide d'un deuxième appareil (il peut s'agir du smartphone ou de la tablette de l'utilisateur, par exemple). Les paramètres *TrustBuilder* sont configurés par l'administrateur Windows ou *TrustBuilder*. Veuillez le contacter et lui demander les informations requises *Service ID* et *Objet de Certificate* pour les paramètres *MFA TrustBuilder* de *u.trust LAN Crypt*.

Entrez le nombre requis pour le *Service ID* et l'*Objet de certificat* (« @cert.trustbuilder », le certificat API du service *TrustBuilder*) dans les champs correspondants.

Remarque : Pour que les utilisateurs de ce groupe puissent utiliser *TrustBuilder MFA*, le profil doit être créé pour eux (voir « *Fournir des règles de chiffrement - générer des fichiers de stratégie* » à la page 175). Après avoir chargé le nouveau profil, les utilisateurs peuvent effectuer leur connexion au client *u.trust LAN Crypt* via MFA. L'utilisateur reçoit alors une demande d'authentification sur son jeton MFA enregistré (par exemple, il peut s'agir de son smartphone), il y saisit son PIN et le confirme.

Remarque : Le certificat API du service *TrustBuilder* doit être installé dans le répertoire de certificats de l'utilisateur sur le client *u.trust LAN Crypt*.

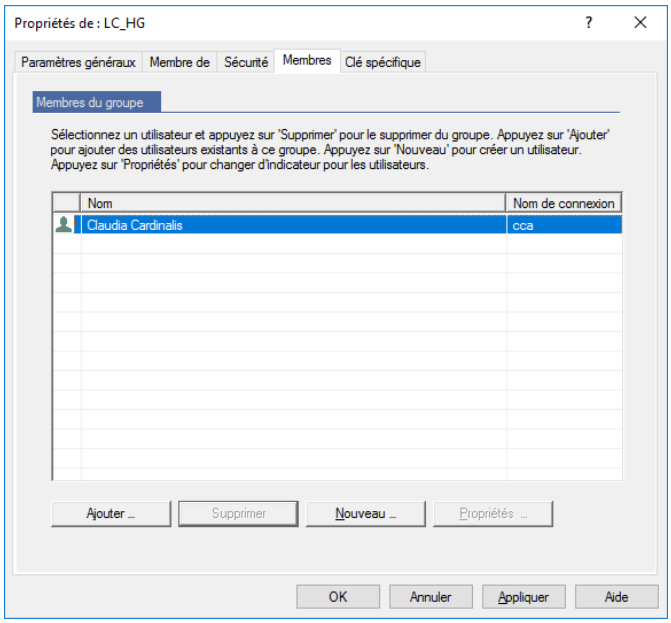
Remarque : Si vous définissez des spécifications pour l'authentification multifactorielle (MFA) pour un groupe, celles-ci ne sont pas héritées vers le bas. Vous devez donc les définir séparément pour chaque groupe.

3.12.2 Onglet « Membre de »

Sous l'onglet **Membre de**, vous voyez les groupes dont le groupe actuel est membre.

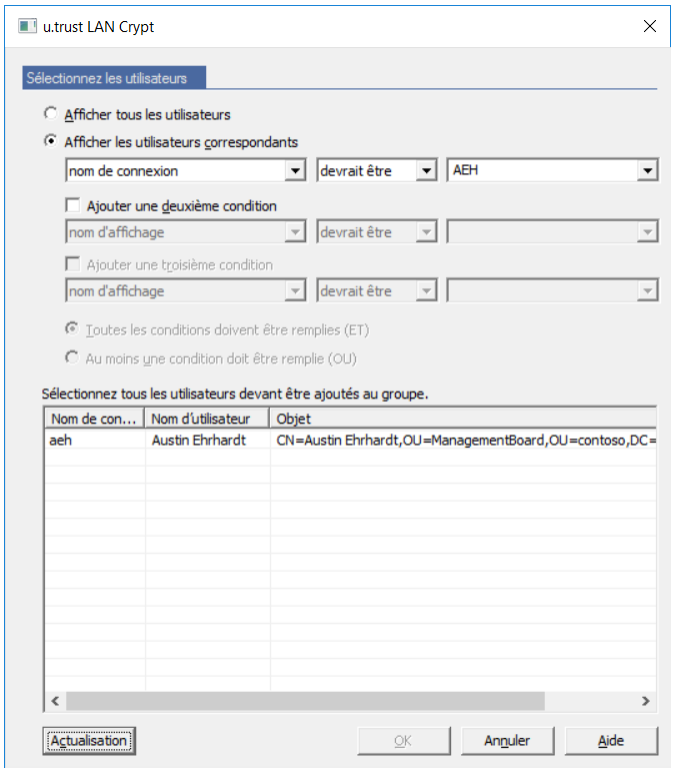
3.12.3 Ajouter/supprimer des membres

Sous l'onglet ***Membres***, vous pouvez ajouter des membres au groupe actuel. Cette liste affiche tous les utilisateurs et groupes existants qui sont membres de ce groupe. Vous ne pouvez modifier que les utilisateurs de cette liste, et non les groupes !



Ajouter … :

Ouvre une boîte de dialogue dans laquelle vous pouvez sélectionner des utilisateurs, puis les ajouter au groupe.



Affiche tous les utilisateurs ou vous permet de sélectionner des groupes d'utilisateurs spécifiques ou des utilisateurs individuels à l'aide des espaces réservés SQL.

L'affichage de tous les utilisateurs pouvant prendre un certain temps, *u.trust 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 d'entrée vous permettant de définir des critères de recherche.

Les informations utilisateur suivantes seront extraites de la base de données *u.trust LAN Crypt* :

- Nom de connexion
- Nom d'utilisateur
- Nom long
- Source (FQN)
- Adresse électronique
- Commentaire
- Attribut utilisateur quelconque
- OU parent d'utilisateur
- Nom du groupe

Vous pouvez définir des critères de recherche en fonction de ces attributs. *u.trust LAN Crypt* recherche la chaîne de caractères définie dans les attributs utilisateur récupérés.

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

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

Dans la liste déroulante de droite, vous pouvez saisir la chaîne de caractères d'*u.trust LAN Crypt* recherchée dans l'attribut défini.

Vous pouvez utiliser les caractères génériques SQL suivants pour saisir la chaîne de caractères :

%	toute séquence de caractères
_	caractère unique (par exemple, a__ signifie rechercher tous les noms contenant trois caractères et commençant par **a**)
[]	caractère unique d'une liste (Par exemple, [a-cg]% signifie rechercher tous les noms commençant par **a**, **b**, **c** ou **g**)
[^]	caractère unique non contenu dans une liste (par exemple, [^a]% signifie rechercher tous les noms ne commençant pas par **a**)

Vous pouvez spécifier jusqu'à trois conditions pour le processus de recherche

Si vous entrez plus d'une condition, vous pouvez définir la façon dont ces conditions doivent être combinées (ET/OU).

Si vous cliquez sur **OK**, tous les utilisateurs dont les noms sont sélectionnés dans la liste sont transférés dans le groupe actuel.

Nouveau :

Ouvre une boîte de dialogue qui vous permet de créer un utilisateur.

Supprimer :

Supprime l'affiliation de l'utilisateur sélectionné du groupe actuel.

Remarque : Si l'utilisateur n'est membre d'aucun autre groupe, il est supprimé de la base de données *u.trust LAN Crypt*.

Si l'utilisateur est membre de plus d'un groupe et que le groupe actuel est le groupe parent de l'utilisateur, l'action résultante dépend du type du groupe :

- Si le groupe est une unité d'organisation ou un groupe racine et que l'utilisateur est membre d'une autre UO ou d'un autre groupe racine, cette UO ou ce groupe racine devient le groupe parent de l'utilisateur. Si l'utilisateur n'est membre d'aucun autre groupe racine ou UO, il est supprimé (de manière similaire à Active Directory, où un utilisateur est supprimé lorsque l'UO à laquelle il appartient est supprimée).
- Si le groupe est un groupe simple (ni une UO ni un groupe racine), l'un des autres groupes auxquels l'utilisateur appartient devient son groupe parent.

Propriétés :

Affiche les propriétés de l'utilisateur sélectionné.

Remarque : Un utilisateur ne peut exister qu'une seule fois dans un conteneur particulier. Si vous essayez de créer/ajouter un utilisateur à un conteneur dans lequel il est déjà présent, un message s'affiche pour vous informer que cela n'est pas possible.

Cependant, plusieurs utilisateurs portant le même nom peuvent être présents dans le système, tant qu'ils ne se trouvent pas dans le même conteneur.

3.12.4 Ajout de responsables de la sécurité

L'onglet **Sécurité** permet également à un responsable de la sécurité d'ajouter des responsables de la sécurité au groupe actuel et de leur assigner des droits pour ce groupe. La condition préalable à cette action est que le responsable de la sécurité souhaitant ajouter un autre responsable de la sécurité ait l'autorisation de **Modifier une ACL**.

Remarque : Si le responsable de la sécurité ajoute des responsables de la sécurité au groupe, il peut assigner ses propres autorisations (et seulement celles-ci) à ces responsables de la sécurité.

Un responsable de la sécurité ne peut pas s'ajouter à une ACL ni modifier ses droits dans l'une d'elles.

3.13 Propriétés des utilisateurs

La boîte de dialogue des *Propriétés* d'un utilisateur (<utilisateur>/Menu contextuel/Propriétés) se compose de quatre onglets dans lesquels vous pouvez modifier les propriétés d'un utilisateur.

Certificats

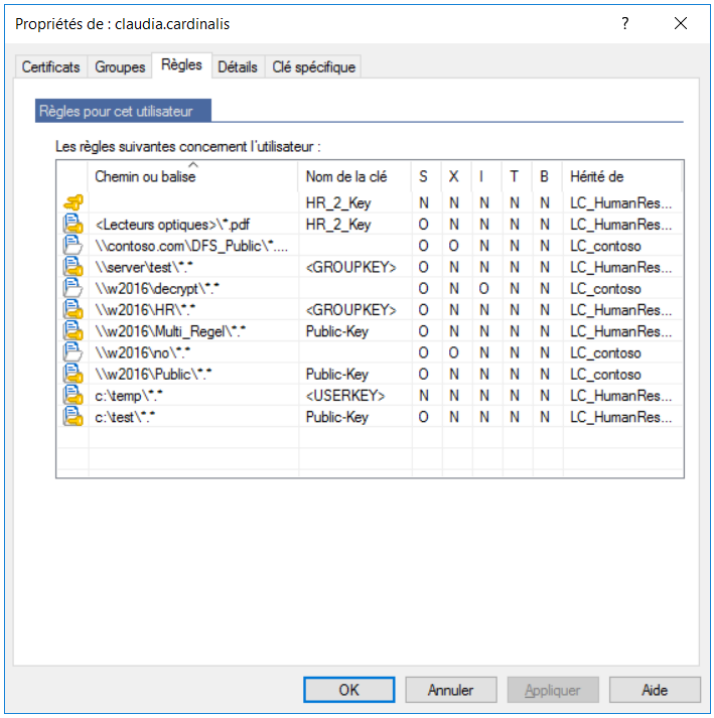
L'onglet **Certificats** affiche tous les certificats assignés à un utilisateur. Dans cet onglet, vous pouvez également créer un certificat *u.trust LAN Crypt* pour l'utilisateur, ajouter un certificat à partir du magasin de certificats et importer un certificat à partir d'un fichier (voir « *Assignation d'un certificat à un utilisateur* » à la page 164).

Groupes

L'onglet **Groupes** affiche les groupes dont l'utilisateur actuel est membre. En outre, vous pouvez supprimer les adhésions de l'utilisateur à des groupes ou en ajouter de nouveaux.

Règles

L'onglet **Règles** affiche toutes les règles de chiffrement pour l'utilisateur. Cela offre un aperçu pratique de toutes les règles de chiffrement actuellement valables pour un utilisateur particulier, même si elles proviennent de différents groupes.

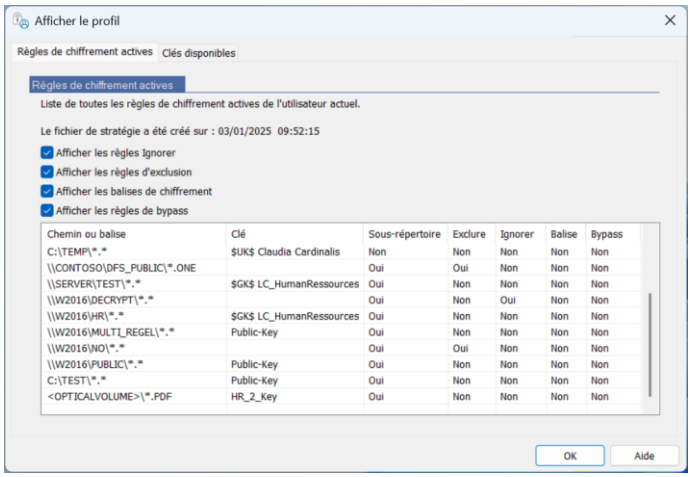


Les colonnes S, X, I, T, B indiquent le type de règle dont il s'agit :

- **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 chemin est ignoré par *u.trust LAN Crypt*. Pour plus d'informations, consultez « *Génération de règles de chiffrement* » à la page 150.
- **T** (balise) : le chemin est utilisé par l'API client *u.trust LAN Crypt* comme balise de chiffrement prédéfinie (voir « *Balises de chiffrement* » à la page 161).
- **B** (bypass) : le chemin est défini comme règle de bypass (voir « *Bypass* » à la page 156).

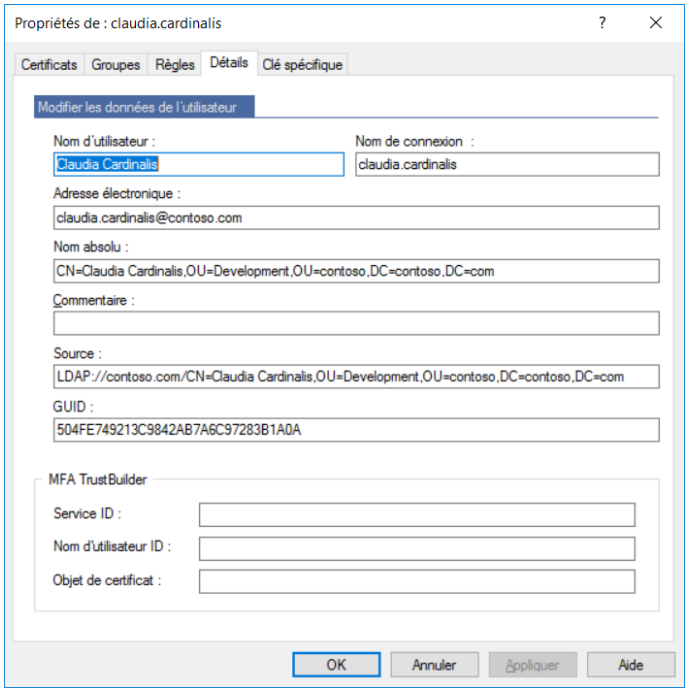
Sous **Hérité de**, apparaît le groupe dont une règle particulière a été héritée.

Dans la vue de profil d'un utilisateur du client *u.trust LAN Crypt*, vous pouvez afficher ces informations de la même manière :



Détails

Les données utilisateur s'affichent et peuvent être modifiées dans l'onglet **Détails**.



Vous pouvez saisir l'adresse électronique de l'utilisateur dans le champ *Adresse électronique*. L'adresse électronique est ajoutée au fichier journal de mot de passe pour les certificats générés par *u.trust LAN Crypt*. Elle peut, par exemple, être utilisée pour créer une lettre PIN par adresse électronique.

Remarque : Les adresses électronique des utilisateurs ne doivent pas contenir de caractères au-dessus du code ASCII 127. Elles ne doivent donc pas contenir de trémas. Il ne doit pas y avoir de point au début ni à la fin de la chaîne.

Dans la section *MFA TrustBuilder* vous pouvez définir les indications pour l'authentification multi-facteurs pour des utilisateurs individuels avec *TrustBuilder*.

Pour ce faire, contactez votre administrateur Windows qui est responsable de l'administration de *TrustBuilder* et demandez-lui les informations nécessaires. Entrez le nombre requis pour le **Service ID** et le **Objet de certificate** (« @cert.trustbuilder », le certificat API du service *TrustBuilder*) dans les champs correspondants.

Vous trouverez de plus amples informations à ce sujet et sur la manière de définir ce paramètre pour tous les utilisateurs d'un groupe dans l'onglet *Propriétés* des groupes concernés (voir « *TrustBuilder* MFA et *u.trust LAN Crypt* »).

Remarque : Faites attention lorsque vous modifiez les données de l'utilisateur. Vos modifications peuvent avoir des effets indésirables. Par exemple, si vous modifiez le *Nom de connexion* dans cet onglet, l'utilisateur peut ne plus être en mesure d'accéder à son fichier de stratégie, car le client utilise un autre *Nom de connexion* (l'ancien) pour rechercher un fichier de stratégie.

3.14 Conception de l'environnement de sécurité

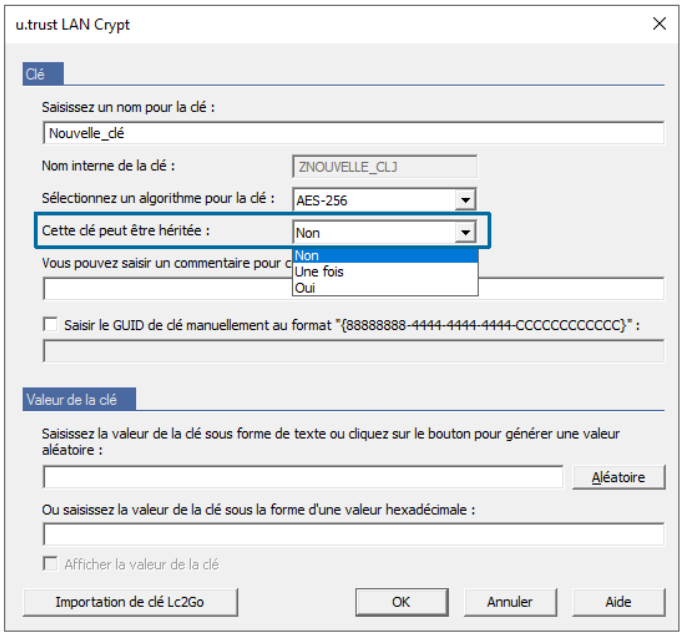
Le niveau élevé de flexibilité d'*u.trust LAN Crypt* permet de l'adapter facilement aux exigences de sécurité de toute entreprise.

Néanmoins, il est très important qu'une stratégie de sécurité à l'échelle de l'entreprise soit définie avant la création de l'environnement *u.trust LAN Crypt*.

Nous vous recommandons généralement de commencer par une stratégie de sécurité assez restrictive, car il est plus facile de libéraliser cette stratégie par la suite que de la rendre plus stricte dans le système *u.trust LAN Crypt*. Rendre une stratégie libérale plus restrictive peut entraîner des problèmes de sécurité difficiles à résoudre. Pour éviter cela, il est essentiel de définir une stratégie de sécurité à l'échelle de l'entreprise avant de générer et de distribuer des profils de chiffrement.

3.15 Génération de clés

De nouvelles clés sont générées sous le nœud du groupe dans lequel elles doivent être utilisées. Pour chaque clé, vous pouvez spécifier si elle doit être héritée vers le bas dans la hiérarchie de groupe.



Remarque : Toutes les clés existantes sont affichées dans **Paramètres centraux\Toutes les clés u.trust LAN Crypt**. Cependant, elles ne peuvent pas y être traitées. Cette vue est un aperçu des clés utilisées dans *u.trust LAN Crypt*. **Les clés ne peuvent être modifiées que dans les groupes dans lesquels elles ont été créées.**

Remarque : Un responsable de la sécurité qui n'a que l'autorisation **Créer des clés** et non les autorisations **Créer un profil** ne peut pas ajouter de valeur lors de la génération de clés. La valeur est générée automatiquement lorsqu'une clé est transmise à un profil.

Une clé *u.trust LAN Crypt* se compose des composants suivants :

- **un nom**

  Par souci de clarté, nous recommandons que le nom du groupe d'utilisateurs fasse partie du nom de la clé.

  Les noms que vous définissez revêtent une importance particulière, car *u.trust LAN Crypt* peut également trier les clés.

  u.trust LAN Crypt utilise des noms de clé spécifiques pour générer un nom de clé de 16 caractères pour un usage interne. Cela attache le préfixe de la région appropriée au début de ce nom de clé.

- **une valeur de clé**

  La longueur de la clé dépend de l'algorithme utilisé. La valeur de clé peut être spécifiée en caractères ANSI ou en notation hexadécimale (nombres et caractères autorisés : `0123456789abcdef`). L'autre valeur associée est mise à jour automatiquement.

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

- **un algorithme de chiffrement**

  AES-128, AES-256, DES, 3DES, IDEA, XOR

- **un commentaire** (facultatif)

- **GUID de clé** (facultatif)

  Cela vous permet de saisir manuellement un GUID de clé afin que les fichiers chiffrés puissent être échangés entre deux différentes installations d'u.trust LAN Crypt (voir « *Onglet Clés* » à la page 52).

  Si ce champ est vide, le GUID est créé automatiquement.

Pour générer une nouvelle clé :

1. Sélectionnez les **Clés de groupe** sous le groupe pour lequel vous souhaitez générer une clé.

2. Cliquez sur l'icône clé jaune dans la barre d'outils ou faites un clic droit dans le volet de la console droite 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 barres obliques inversées (\), les barres obliques (/), les virgules inversées et le caractère & ne sont pas autorisés dans les noms de clé. *u.trust LAN Crypt* génère un nom de clé unique de 16 caractères à partir de ce nom qui est utilisé à des fins internes. Il met également le préfixe de région (s'il a été spécifié dans les propriétés du responsable de la sécurité) au début de ce nom unique. Le nom interne est affiché à droite, à côté de la liste déroulante à partir de laquelle vous sélectionnez l'algorithme.

   Vous pouvez modifier le nom de la clé plus tard, mais pas le nom interne qui en a été généré.

4. Sélectionnez un algorithme de chiffrement dans la liste déroulante.

   Ici, vous ne pouvez voir que les algorithmes que vous avez rendus disponibles dans les **Paramètres centraux**.

   Remarque : Veuillez toujours choisir un algorithme sécurisé, tel que **AES-256** ou **AES-128** pour chiffrer vos données, car les algorithmes de chiffrement tels que XOR, IDEA, DES ou 3DES ne sont plus considérés comme sécurisés !

5. Spécifiez si la clé peut être héritée ou non dans le groupe :

   - **Non**

     La clé n'est pas héritée et n'est donc disponible que dans le groupe actuel.

   - **Une fois**

     La clé est héritée dans le(s) groupe(s) dans le niveau hiérarchique suivant en dessous du groupe actuel.

   - **Oui**

     La clé est héritée dans tous les groupes dans les niveaux de hiérarchie en dessous du groupe actuel, et elle y est disponible pour générer des règles de chiffrement.

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

7. Si nécessaire, cochez la case **Saisir le GUID de clé manuellement au format {88888888-4444-4444-4444-…}** et entrez le GUID dont vous avez besoin (ceci n'est possible que si l'option « *Les responsables de la sécurité peuvent définir le GUID pour les nouvelles clés* » est active dans les « Paramètres centraux »). Le GUID prédéfini `{88888888-4444-4444-4444-CCCCCCCCCCCC}` ne peut pas être simplement accepté ici. Vous devez le changer dans tous les cas.

8. Saisissez une valeur hexadécimale (lettres de A à F, chiffres de 0 à 9) ou une chaîne de caractères dans le champ de saisie ANSI pour la valeur clé. L'autre valeur associée est mise à jour automatiquement. Sinon, cliquez sur **Aléatoire** (recommandé) pour qu'u.trust LAN Crypt calcule une valeur.

9. Cliquez sur **OK**.

   La nouvelle clé est affichée dans la console d'administration.

3.15.1 Importation de clé Lc2Go

Vous pouvez importer des clés à partir de fichiers chiffrés avec *Lc2Go*. Pour ce faire, cliquez sur le bouton **Importation de clé Lc2Go**. Sélectionnez ensuite un fichier chiffré avec *Lc2Go* dont vous voulez importer la clé dans *u.trust LAN Crypt*. Si nécessaire, cliquez sur **Parcourir** (« **…** ») si vous voulez sélectionner et importer le fichier chiffré avec *Lc2Go* à partir d'un chemin spécifique en utilisant l'explorateur de fichiers.

Saisissez la phrase de passe associé (le mot de passe sécurisé) pour ce fichier dans le champ de saisie **Phrase de passe**.

La clé *Lc2Go* importée est affichée dans la console d'administration et peut être utilisée pour les règles de chiffrement.

3.15.2 Clés spécifiques

En plus de générer des clés manuellement, les clés spécifiques à l'utilisateur et au groupe peuvent également être utilisées dans *u.trust LAN Crypt*.

<USERKEY>

Lorsque des clés sont affectées à des chemins de chiffrement, dans la liste des clés, une clé **<USERKEY>** est également toujours affichée. Il s'agit d'un espace réservé pour une clé spécifique à l'utilisateur que le système génère automatiquement pour chaque utilisateur individuel lorsqu'il résout les règles de chiffrement.

<GROUPKEY>

Vous pouvez utiliser **<GROUPKEY>**, de la même manière que **<USERKEY>**, pour générer une clé commune pour tous les membres d'un groupe. Le système génère automatiquement la clé de groupe lorsqu'il résout les règles de chiffrement.

Exemple : Un exemple de la façon dont **<USERKEY>** pourrait être utilisé est si tous les utilisateurs utilisent un lecteur réseau `U:` qui contient un répertoire par utilisateur, et seul l'utilisateur approprié peut accéder à ce répertoire.

U:.* <USERKEY>*

Un autre exemple serait d'utiliser **<USERKEY>** pour chiffrer les répertoires temporaires locaux.

Les clés spécifiques à l'utilisateur et au groupe n'apparaissent pas dans la vue par défaut sous le nœud **Paramètres centraux**, **Toutes les clés u.trust LAN Crypt**, car elles ne sont généralement pas nécessaires. Cependant, si nécessaire, un responsable principal de la sécurité ou un responsable de la sécurité avec l'autorisation globale **Utiliser des clés spécifiques** peut afficher ces clés, de sorte que les données deviennent visibles pour lui.

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

Pour afficher ces clés spécifiques, cliquez sur **Afficher les clés spécifiques** dans le menu contextuel de la liste des clés. Maintenant, seules ces clés spécifiques sont affichées. Pour revenir à la vue par défaut, cliquez à nouveau sur **Afficher les clés spécifiques**.

Remarque : Les clés spécifiques ne sont pas supprimées de la base de données lorsque l'utilisateur / le groupe auquel elles appartiennent est supprimé. Elles restent dans la base de données et peuvent être affichées sous le nœud **Paramètres centraux**, **Toutes les clés u.trust LAN Crypt**, en cliquant sur le menu contextuel *Afficher les clés spécifiques*.

Réattribution de clés spécifiques

Dans certaines situations, vous devrez peut-être réaffecter une clé spécifique à un utilisateur ou à un groupe.

Exemple : Un utilisateur est importé d'Active Directory dans la console d'administration d'*u.trust LAN Crypt*. Une clé spécifique à l'utilisateur est générée pour cet utilisateur. Si vous supprimez le groupe dont l'utilisateur est membre dans la console d'administration d'*u.trust LAN Crypt* et le réimportez, *u.trust LAN Crypt* génère automatiquement une nouvelle clé spécifique à l'utilisateur lorsqu'il génère les fichiers de stratégie de l'utilisateur.

L'utilisateur ne peut alors plus accéder aux données chiffrées à l'aide de « l'ancienne » clé, spécifique à l'utilisateur.

Pour surmonter des situations comme celle-ci, vous pouvez configurer *u.trust LAN Crypt* de sorte que des clés spécifiques d'utilisateurs/groupes supprimés puissent être réassignées.

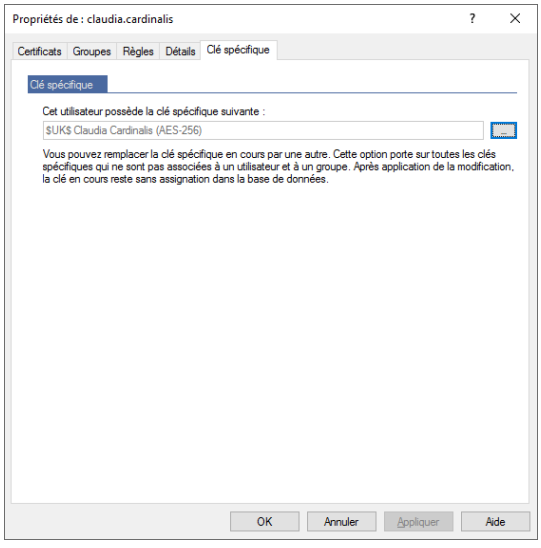
Pour ce faire, ajoutez la valeur DWORD « `ShowUserKeyPage` » au Registre Windows avec la valeur de données « `1` » sous la clé :

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Utimaco\
SGLANCrypt
```

Vous pouvez également faire cette entrée dans le Registre Windows pour un utilisateur spécifique sous

```
HKEY_CURRENT_USER\.....
```

Si cette valeur est trouvée dans le Registre Windows, la **Clé spécifique** de l'onglet est ajoutée aux boîtes de dialogue *Propriétés* (<utilisateur/groupe>/Menu contextuel/Propriétés) pour les utilisateurs et les groupes.



Si une clé spécifique est assignée à un utilisateur ou à un groupe, elle est affichée dans l'onglet **Clé spécifique**. Si aucune clé spécifique n'est affichée, vous pouvez remplacer la clé actuelle par une autre clé spécifique ou assigner une nouvelle clé. Vous pouvez utiliser toutes les clés présentes dans la base de données et n'ayant pas encore été assignées à un utilisateur ou à un groupe.

Remarque : Pour apporter des modifications, un responsable de la sécurité doit avoir l'autorisation **Utiliser des clés spécifiques**. S'il ne l'a pas, il n'a qu'un accès en lecture.

Cliquez sur le bouton **Parcourir** (« **…** ») pour afficher une liste de toutes les clés disponibles. Sélectionnez une clé et cliquez sur **OK**.

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

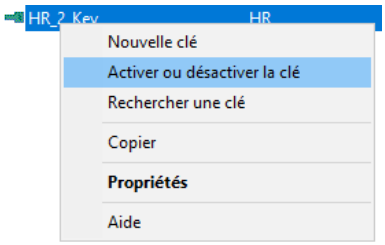
Si la clé spécifique actuelle a été remplacée par une clé différente, elle reste dans la base de données en tant que clé non assignée.

3.15.3 Rendre les clés actives/inactives

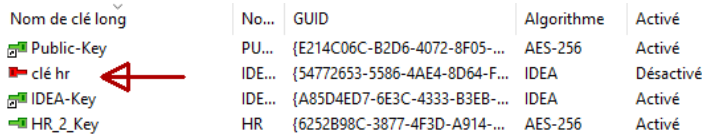
Dans *u.trust LAN Crypt*, vous pouvez basculer une clé existante pour la rendre inactive. Si vous faites cela, cette clé n'est plus disponible lorsque vous définissez des règles de chiffrement.

Cependant, vous pouvez toujours utiliser cette clé dans les règles de chiffrement qui sont déjà utilisées. Elle reste enregistrée dans la base de données d'administration et vous pouvez également l'activer à nouveau si nécessaire.

Pour basculer d'une clé inactive à une clé active (et vice versa), sélectionnez-la et cliquez sur **Activer ou désactiver la clé** dans le menu contextuel.



Vous pouvez reconnaître une clé passive grâce à son icône de clé rouge en début de ligne.



3.15.4 Relations entre les clés

En plus de générer des clés pour le groupe dans lequel elles doivent être utilisées, les clés peuvent également être mises à la disposition des utilisateurs d'un groupe en créant une relation (raccourci) avec une clé dans un groupe différent.

Exemple : Si vous souhaitez accorder aux membres d'une équipe les mêmes droits que ceux octroyés aux membres d'une équipe différente pour une durée limitée, ajoutez simplement un raccourci vers la clé d'un groupe à l'autre groupe. Le raccourci vers la clé peut ensuite être utilisé pour créer des règles de chiffrement.

Si vous ne pouvez pas utiliser de raccourci vers une clé, vous devez créer un groupe, y ajouter les utilisateurs des deux groupes, puis créer des clés et règles de chiffrement pour rendre ce simple échange de données possible. Un raccourci vers une clé fournit un moyen rapide et facile d'échanger des données.

Pour ajouter une clé à un autre groupe via un raccourci, faites-la glisser depuis le nœud **Clés de groupe** d'un groupe vers le nœud du groupe concerné. Vous pouvez également copier la clé dans le groupe source et la coller dans le groupe cible.

Une clé importée de cette façon s'affiche sous forme de raccourci :



Un responsable de la sécurité doit disposer de ces autorisations globales pour pouvoir insérer des raccourcis vers les clés :

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

Dans le groupe source, ils doivent également disposer du **droit spécifique au groupe**

- **Créer des clés**

  ainsi que

- **Copier des clés**

  dans le groupe cible.

Pour supprimer un raccourci, le responsable de la sécurité doit disposer de l'autorisation **Supprimer des clés** globale et spécifique au groupe.

Les clés insérées en tant que raccourcis ont les propriétés suivantes :

- Elles ne seront PAS héritées, et ne seront donc disponibles que dans le groupe dans lequel elles ont été créées. Elles ne seront PAS disponibles dans les sous-groupes.
- Si la clé « originale » est supprimée, tous les raccourcis sont également supprimés.

Remarque : De la même manière que pour les clés de groupe « normales », si vous supprimez une référence, cela ne signifie pas que la règle dans laquelle elles ont été utilisées n'est plus valide. Pour supprimer l'accès aux données, il vous faut supprimer la règle de chiffrement correspondante et générer un nouveau fichier de stratégie. Le client doit charger le nouveau fichier de stratégie pour la première fois afin d'empêcher un utilisateur d'accéder à ces données.

3.15.5 Suppression de clés d'un groupe

Vous pouvez uniquement supprimer une clé à partir du groupe dans lequel elle a été générée. Vous devez désactiver la clé avant de la supprimer.

La suppression de clés en cours d'utilisation entraîne leur suppression du groupe. Néanmoins, elles restent dans la base de données en tant que clés non assignées et apparaissent dans **Paramètres centraux/Toutes les clés u.trust LAN Crypt**.

Ajouter des clés à nouveau

Si vous avez à nouveau besoin de cette clé par la suite (notamment pour accéder à une sauvegarde chiffrée d'anciennes données), il vous suffit de la faire glisser de la liste de toutes les clés u.trust LAN Crypt dans le groupe pertinent, où vous pouvez l'utiliser à nouveau. Un responsable de la sécurité peut ajouter une clé à n'importe quel groupe pour lequel il a l'autorisation **Créer des clés**. La clé est véritablement ajoutée au groupe. Il ne s'agit pas d'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'apparaît plus sous **Toutes les clés u.trust LAN Crypt**.

3.15.6 Suppression des clés de la base de données

Dans les conditions suivantes, les clés peuvent effectivement être supprimées (sous le nœud **Toutes les clés u.trust LAN Crypt**) de la base de données :

- Vous devez être connecté en tant que 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.
- 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 de clés

Une fois que vous avez généré une clé, vous pouvez en modifier le nom, le type d'héritage spécifié et le commentaire.

Vous pouvez voir si une clé a déjà été utilisée dans la colonne *Utilisée* de la console.

Pour modifier une clé, accédez au groupe dans lequel la clé concernée a été générée et double-cliquez sur son nom. Une boîte de dialogue vous permettant de modifier la clé s'affiche alors.

Boîte de dialogue Propriétés

La boîte de dialogue *Propriétés* affiche des informations sur la clé sélectionnée. Cette boîte de dialogue vous permet de modifier le nom de clé long et les paramètres qui définissent si la clé peut ou non être héritée. Vous ne pouvez pas modifier le nom de clé unique de 16 caractères pour usage interne qui a été généré par *u.trust LAN Crypt*.

Remarque : Pour modifier une clé, le responsable de la sécurité doit disposer de l'autorisation **Créer des clés** spécifiques au groupe pour les groupes dans lesquels la clé a été générée. Les clés qui n'appartiennent pas à un groupe particulier ne peuvent pas être modifiées.

Double-cliquez sur une clé pour afficher ses propriétés.

La boîte de dialogue *Propriétés* se compose de trois onglets :

- L'onglet **Clé** affiche les données d'une clé. Dans cet onglet, vous pouvez modifier le nom de clé long et les paramètres qui définissent si la clé peut ou non être héritée. 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 peut être utilisée pour 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** sont fournis à titre indicatif uniquement. Aucune modification ne peut y être apportée.

3.16 Règles de chiffrement

Les règles de chiffrement d'*u.trust LAN Crypt* définissent précisément les données qui peuvent être chiffrées avec chaque clé. Une règle de chiffrement comporte un chemin de chiffrement et une clé.

Remarque : Lorsque vous spécifiez le chemin d'une règle de chiffrement, vous devez également spécifier les fichiers ou les types de fichiers. Vous pouvez également utiliser des caractères génériques (par exemple « *.* »).

Remarque : La nouvelle fonction « Multi-policy support », disponible à partir de la version 11.0.0 de *u.trust LAN Crypt*, prend également en charge le chargement de plus d'un fichier de stratégie pour les utilisateurs. Nous vous fournissons volontiers de plus amples informations à ce sujet sur demande. Veuillez-vous adresser au Support Utimaco.

Les règles de chiffrement définies pour un groupe constituent un profil de chiffrement *u.trust LAN Crypt*.

Le profil de chiffrement d'un groupe peut contenir différentes règles de chiffrement, chacune utilisée pour chiffrer un type spécifique de données.

Vous pouvez chiffrer des lecteurs entiers, des médias amovibles (tels que des disques mémoire flash USB), des lecteurs optiques, des partages réseau, des dossiers (y compris des

sous-dossiers), des types de fichiers particuliers (identifiés par leur extension de fichier) et des fichiers individuels (identifiés par leur nom de fichier ou des parties d'un nom de fichier).

Lorsque vous générez les règles de chiffrement individuelles, le système affiche toutes les clés présentes dans le groupe. Le responsable de la sécurité *u.trust LAN Crypt* peut désormais assigner les clés appropriées pour définir les données auxquelles un utilisateur doit être en mesure d'accéder.

Les règles de chiffrement sont toujours générées par groupe. Elles se composent d'un chemin et d'une clé, et sont créées dans le nœud **Règles et balises de chiffrement**. Générer une règle de chiffrement est très simple. La même boîte de dialogue vous permet en effet de saisir les détails du chemin, choisir une clé et sélectionner différentes options.

Le chemin, la sélection de clé et les diverses options proposées sont résumés dans une boîte de dialogue afin qu'une règle de chiffrement puisse être facilement créée. Les règles de chiffrement peuvent être modifiées ultérieurement si nécessaire, par exemple si l'algorithme précédemment sélectionné pour une clé ne répond plus aux exigences de sécurité requises. Dans ce cas, la clé précédemment utilisée (par exemple, avec l'algorithme IDEA) peut être remplacée par une nouvelle clé avec un algorithme au niveau de sécurité plus élevé (par exemple, AES-XTS 256 bits). Après l'exécution d'un chiffrement initial, tous les fichiers existants sont ensuite chiffrés avec la nouvelle clé et l'algorithme disposant d'un niveau de sécurité plus élevé.

Remarque : les règles de chiffrement ne peuvent en principe être modifiées que dans le groupe dans lequel elles ont été créées. Si une règle de chiffrement est « héritée », c'est-à-dire qu'elle se trouve dans un sous-groupe, elle ne peut pas être éditée ou modifiée à cet endroit. Vous pouvez le constater en affichant un groupe dans la colonne « *Hérité de* ». La règle de chiffrement a été créée dans le groupe affiché et ne peut être modifiée qu'à cet endroit.

Remarque : Si une clé précédemment utilisée doit être remplacée par une autre clé pour une règle de chiffrement existante, l'ancienne clé doit rester en la possession de l'utilisateur. L'ancienne clé est ensuite requise pour le rechiffrèrent des données chiffrées existantes qui sont encore chiffrées avec cette clé. Pour ce faire, assignez l'ancienne clé en tant que *clé sans chemin* aux utilisateurs respectifs (voir « *clé sans chemin* » à la page 159).

Remarque : Utimaco recommande généralement de chiffrer toutes les données selon l'algorithme AES, avec une longueur de clé de 256 bits. Pour des raisons de sécurité, les données encore chiffrées avec un algorithme obsolète (par exemple, DES, 3DES, IDEA, XOR) doivent absolument être chiffrées à nouveau avec l'algorithme AES 256 bits, et ce, dès que possible.

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 les données à chiffrer. Vous les définissez dans le nœud **Règles et balises de chiffrement** sous le nœud du groupe concerné. Ils s'appliquent ensuite à tous les utilisateurs qui sont présents dans ce groupe.

Remarque : Les chemins d'accès aux fichiers **.zip* ou aux dossiers compressés ne peuvent pas être utilisés comme chemins de chiffrement.

Remarque : Veuillez noter que les chemins de chiffrement ne peuvent pas contenir plus de 259 caractères.

Chemins relatifs :

u.trust LAN Crypt prend en charge les définitions de chemins relatifs. Une définition de chemin relatif spécifie un chemin vers un répertoire ou fichier qui n'identifie pas le lecteur de disque concerné, ou le répertoire le plus élevé suivant dans la hiérarchie. Si vous sélectionnez une définition de chemin relatif, le système chiffre chaque répertoire qui correspond à cette définition de chemin.

Vous pouvez utiliser les chemins relatifs de deux manières :

- **Entrée :** `\my_data\*.*`

  chiffre chaque dossier « *my_data* » dans les répertoires RACINE.

  Par exemple, il s'agirait des dossiers suivants :

  C:\my_data*.*
  D:\my_data*.*
  F:\my_data*.*
  Z:\my_data*.*

- **Entrée :** `my_data\*.*`

  chiffre **CHAQUE** dossier « *my_data* ».

  Exemple :

  C:\company**my_data*.***

  Z:\Departments\development\Team1**my_data*.***

Dans les deux cas, tous les fichiers des dossiers « **my_data** » sont chiffrés.

Si un chemin d'accès au répertoire commence par une barre oblique inverse, la définition du chemin relatif ne s'applique qu'aux dossiers racine.

Dossier par défaut

Pour faciliter le chiffrement de dossiers spécifiques à l'utilisateur, *u.trust LAN Crypt* prend en charge les répertoires par défaut prédéfinis par Windows (par exemple *Mes documents*, *Documents communs*, etc.). Le responsable de la sécurité n'a donc pas à tenir compte des variations spécifiques au système dans la configuration du client. *u.trust LAN Crypt* détermine

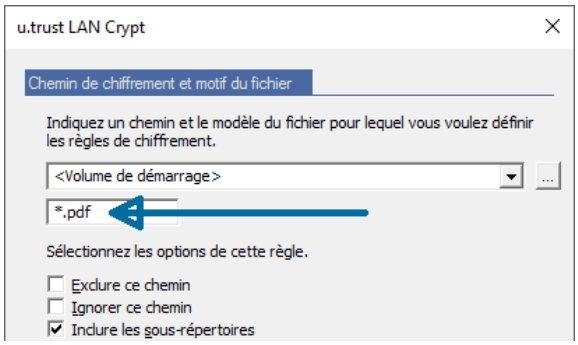
le chemin d'accès utilisateur correct dans la langue appropriée à partir du répertoire par défaut concerné, et chiffre les fichiers stockés dans ce répertoire.

Volume de démarrage

En sélectionnant l'option <*Volume de démarrage*>, vous pouvez chiffrer les fichiers situés sur le lecteur système (où Windows est également installé). Après avoir sélectionné cette option, vous pouvez également personnaliser l'entrée prédéfinie « *.* » (cela s'applique également à tous les fichiers) dans le champ d'entrée.

Exemple :

Par exemple, si seuls les fichiers PDF doivent être chiffrés sur les volumes de démarrage, modifiez l'entrée dans le champ comme suit :



Vous pouvez également chiffrer des types de fichiers supplémentaires ou des fichiers spécifiques uniquement (comme « confidentiel.txt ») sur les volumes de démarrage. Pour ce faire, créez une autre règle et modifiez l'entrée dans le champ de saisie de la même manière que décrit ci-dessus.

Tous les lecteurs locaux

L'option <*Tous les lecteurs locaux*> vous permet de créer une règle qui s'applique uniquement à tous les lecteurs locaux. Il peut s'agir, par exemple, de disques durs intégrés (même multiples), de médias amovibles ou même de lecteurs optiques.

Lecteurs optiques

L'option <*Lecteurs optiques*> vous permet de créer une règle qui s'applique exclusivement aux médias optiques. Vous pouvez ainsi définir que, par exemple, les données gravées sur un CD, DVD ou Blu-ray soient toujours automatiquement chiffrées par *u.trust LAN Crypt*. Seuls les utilisateurs en possession de la clé correspondante peuvent lire ces données par la suite ou les partager entre eux.

Partages réseau

En sélectionnant l'option <*Partages réseau*>, vous pouvez créer une règle qui s'applique à tous les partages réseau auxquels l'utilisateur a accès. Peu importe que le partage réseau soit une lettre de lecteur ou un chemin UNC.

Volumes amovibles

En sélectionnant l'option <*Volumes amovibles*>, vous pouvez créer une règle qui s'applique à tous les appareils amovibles.

Remarque : Notez que <*Volumes amovibles*> fait référence à tous les supports de stockage connectés de manière externe (par exemple clés USB, disques durs externes, etc.). Cela s'applique également aux lecteurs optiques connectés en externe. En outre, les périphériques amovibles appartiennent également aux lecteurs locaux.

Disques durs locaux

En sélectionnant l'option <*Disques durs locaux*>, vous pouvez créer une règle qui s'appliquera ensuite à tous les disques durs installés localement.

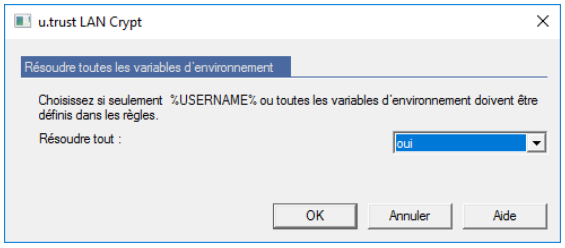
Variables d'environnement

u.trust LAN Crypt prend en charge l'utilisation de la variable d'environnement locale `%USERNAME%` dans les définitions de chemin. La variable d'environnement locale `%USERNAME%` dans la définition de chemin est résolue automatiquement par *u.trust LAN Crypt*.

Des dossiers supplémentaires peuvent être spécifiés dans *u.trust LAN Crypt* en entrant la variable d'environnement suivante :

Variable d'environnement :	Exemple :
%ALLUSERSPROFILE%	C:\ProgramData
%APPDATA%	C:\Users*username*\AppData\Roaming
%LOCALAPPDATA%	C:\Users*username*\AppData\Local
%PUBLIC%	C:\Users\Public
%USERPROFILE%	C:\Users\username

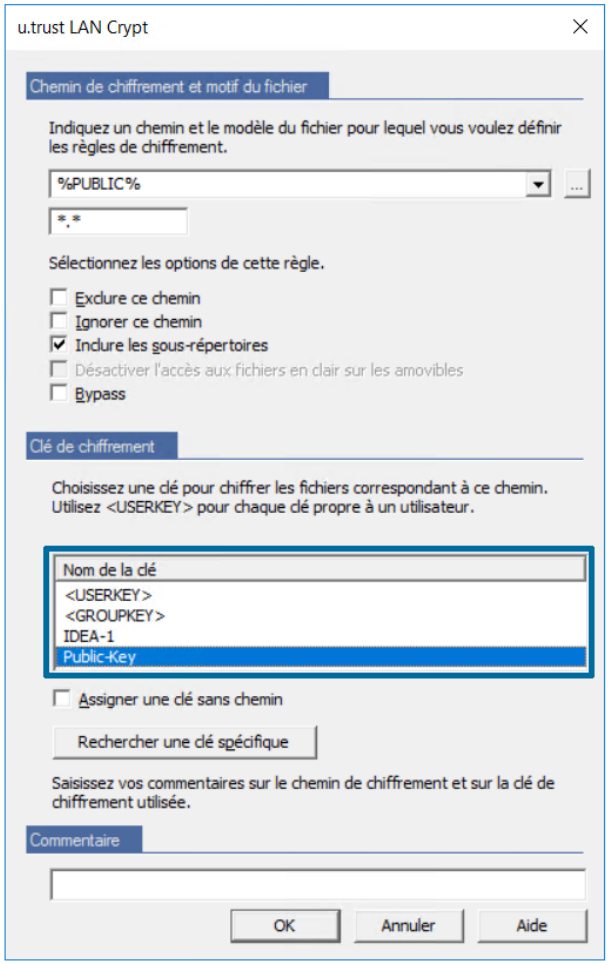
Pour résoudre ces variables d'environnement dans le client *u.trust LAN Crypt*, cela doit être défini dans la configuration d'*u.trust LAN Crypt* (voir section « *Résoudre toutes les variables d'environnement* » à la page 190).



Remarque : Les variables d'environnement ne sont pas prises en charge dans les règles de **bypass**.

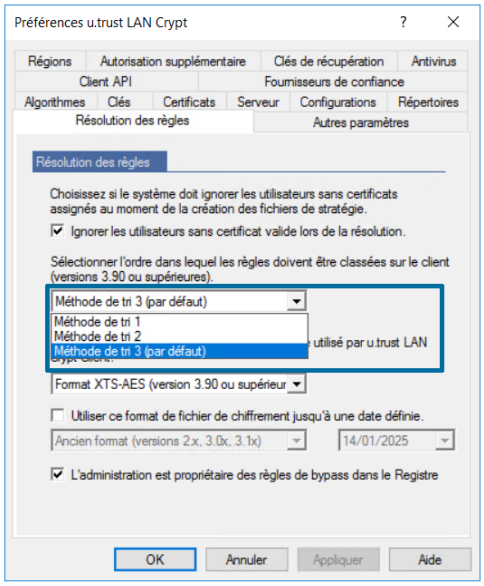
3.16.2 Clés

Vous créez les clés utilisées pour chiffrer les données avant de générer les règles de chiffrement. Toutes les clés disponibles pour le groupe concerné apparaissent dans la boîte de dialogue qui vous permet de créer une règle de chiffrement. Vous pouvez les sélectionner dans une liste à partir de cet emplacement.



3.16.3 Séquence des règles de chiffrement

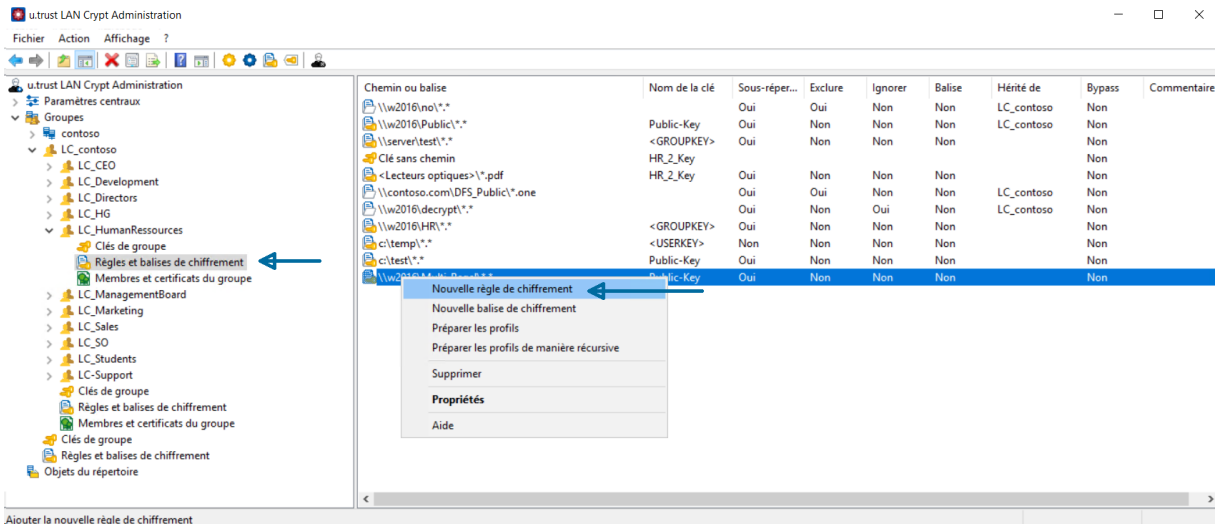
Lorsque vous chargez les fichiers de stratégie dans le client, *u.trust LAN Crypt* trie les règles de chiffrement selon la méthode que vous avez sélectionnée dans l'onglet **Résolution des règles** (voir « *Méthodes de tri* » à la page 55) dans le nœud **Paramètres centraux** :



3.16.4 Génération de règles de chiffrement

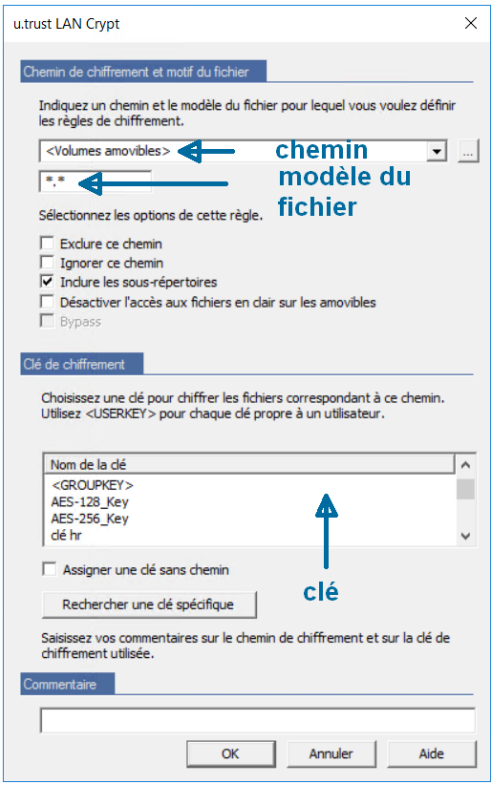
1. Cliquez avec le bouton droit sur **Règles et balises de chiffrement** sous le nœud de groupe correspondant et cliquez sur **Nouvelle règle de chiffrement** dans le menu contextuel. Si vous recherchez un groupe particulier, vous pouvez également utiliser la fonction **Trouver groupe**.

   Si des règles de chiffrement ont déjà été créées, elles sont affichées dans la fenêtre de console de droite.



   Vous pouvez également accéder à la commande **Nouvelle règle de chiffrement** dans un menu contextuel que vous affichez en cliquant avec le bouton droit dans le

volet de droite de la console. Dans le volet de droite de la console, vous pouvez voir toutes les règles de chiffrement qui ont été générées.



2. Saisissez un chemin relatif ou absolu dans le champ de saisie sous *Chemin de chiffrement et modèle du fichier*.

3. Si la nouvelle règle de chiffrement doit s'appliquer à tous les fichiers du chemin sélectionné, saisissez « *.* » comme modèle de fichier dans le champ de saisie situé en dessous. Si, en revanche, la nouvelle règle ne doit s'appliquer qu'à certains types de fichiers, saisissez par exemple « *.docx » (pour les fichiers Word) ou « *.txt » (pour les fichiers texte) comme modèle de fichier. L'utilisation de jokers (*) et de caractères de remplacement (?) dans les noms de fichiers (mais pas dans le reste du chemin) est autorisée (p. ex. « *.d?? » ou aussi « *.d* »). Le cas échéant, cliquez sur **Parcourir** (« **…** ») si vous souhaitez sélectionner un chemin spécifique pour la règle via l'explorateur de fichiers.

   Vous pouvez également choisir l'un des modèles prédéfinis contenus dans la zone de liste. Le chemin prédéfini sélectionné en conséquence est alors affiché dans le champ de saisie.

Les chemins prédéfinis suivants peuvent être choisis pour la règle de chiffrement :

```
<Données d'application locale>
<Données d'application>
<Données d'application communes>
<Mes documents>
<Documents communs>
<Cache Internet>
<Volume de démarrage>
<Tous les lecteurs locaux>
<Lecteurs optiques>
<Partages réseau>
<Volumes amovibles>
<Disques durs locaux>
```

Ici aussi, vous pouvez adapter individuellement l'indication prédéfinie du modèle de fichier « *.* » comme décrit précédemment. Vous trouverez des informations complémentaires sur les chemins prédéfinis au début de cette section, à partir de la page 147.

Entrez un chemin relatif ou absolu dans le champ de saisie sous *Chemin de chiffrement* ou sélectionnez l'un des modèles prédéfinis. Vous pouvez utiliser des jokers (*) et des caractères génériques (?) dans les noms de fichiers (par exemple (*.docx) et dans le chemin (par exemple `c:\top_secret\*.*`). Cliquez sur le bouton **Parcourir** (« … ») pour sélectionner un chemin.

Chemins relatifs et programmes prenant en charge les spécifications de fichiers ou de chemins en notation 8.3 uniquement

Si vous utilisez des programmes qui ne prennent en charge que les spécifications de fichiers ou de chemins en notation 8.3, et que vous souhaitez accéder à des fichiers chiffrés dont les noms comptent plus de 8 caractères ou des fichiers de dossiers dont les noms comptent plus de 8 caractères, vous devez utiliser la notation 8.3 pour spécifier les chemins de chiffrement.

Vous devez également définir ces règles de chiffrement. Si vous ne le faites pas, les programmes 32 bits ne fonctionneront plus.

Utilisez la commande `dir /x` pour afficher le nom 8.3 correct des noms de fichiers longs.

4. Cinq rois options apparaissent sous *Chemin de chiffrement et motif du fichier* :
   - Exclure ce chemin
   - Ignorer ce chemin
   - Inclure les sous-répertoires
   - Désactiver l'accès aux fichiers en clair sur les amovibles
   - Bypass

Exclure les chemins

Ici, vous devez définir une règle de chiffrement qui exclut ces données du chiffrement. Pour ce faire, sélectionnez l'option **Exclure ce chemin** dans la boîte de dialogue *Règles de chiffrement*. Par conséquent, les fichiers spécifiés dans la règle de chiffrement ne sont pas chiffrés. Par défaut, cette option n'est pas sélectionnée.

Cette option peut être utilisée dans une règle de chiffrement pour exclure des fichiers individuels, des types de fichiers ou des sous-dossiers d'un chemin pour lequel une règle de chiffrement existe déjà à partir du chiffrement. Pour ce faire, activez l'option **Exclure ce chemin** dans la boîte de dialogue de la nouvelle règle de chiffrement. Cela signifie que les fichiers spécifiés dans la règle de chiffrement ne sont pas chiffrés. Par défaut, cette option est désactivée. Vous pouvez également modifier ce paramètre pour les règles de chiffrement existantes. Pour ce faire, sélectionnez une règle existante avec un double clic ou via le menu contextuel *Propriétés*.

Exemple :

Tous les fichiers ayant l'extension `*.TXT` doivent être exclus du chiffrement.

Première ligne :

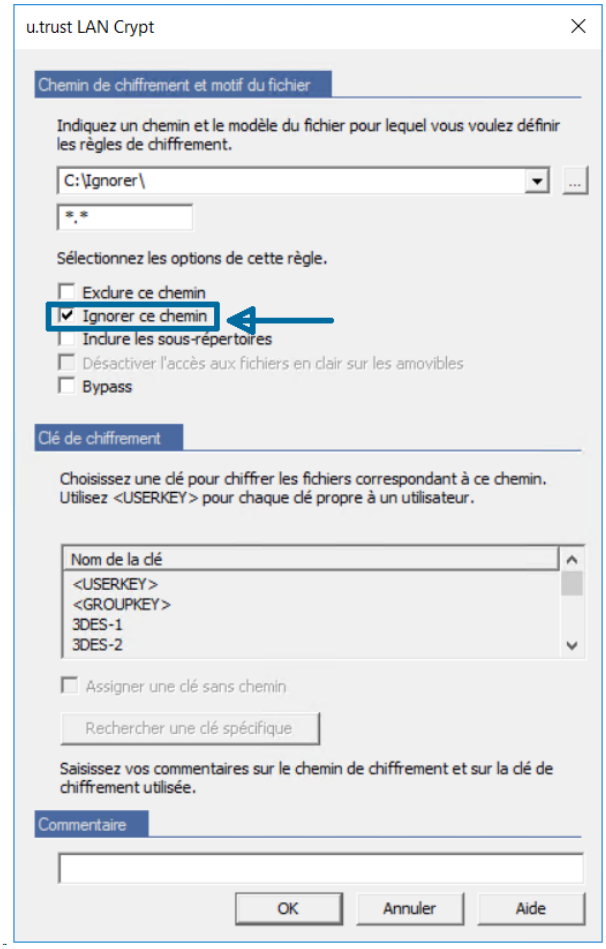
Entrée `C:\MYDIR\*.TXT`, **Exclure ce chemin**, pas de clé : exclut du chiffrement tous les fichiers avec l'extension `.TXT` dans le dossier *MYDIR*.

Deuxième ligne :

Entrée `C:\MYDIR\*.*`, **Exclure ce chemin** non sélectionné, chiffre tous les fichiers dans le dossier *MYDIR* (**sauf les fichiers *.TXT**) avec la clé spécifiée.

Ignorer ce chemin

u.trust LAN Crypt inclut l'option **Ignorer ce chemin**. *u.trust LAN Crypt* ignore tout simplement les fichiers affectés par ce type de règle de chiffrement.



Contrairement à l'option **Exclure ce chemin**, cela signifie également qu'il n'y a pas de contrôle d'accès pour ces fichiers. Vous pouvez les ouvrir (les contenus chiffrés sont affichés), les déplacer, les supprimer, etc.

Si vous avez activé l'option **Ignorer ce chemin** cela signifie que les fichiers concernés par cette règle ne seront pas protégés par le *u.trust LAN Crypt*. Les fichiers situés dans ces chemins peuvent être ouverts par les utilisateurs (le contenu éventuellement crypté d'un fichier est affiché), déplacés, supprimés, etc. Pour les fichiers situés dans des dossiers pour lesquels il existe en revanche une règle **Exclure ce chemin**, le *u.trust LAN Crypt* vérifie toutefois s'ils sont chiffrés ou non. L'accès aux fichiers chiffrés est alors refusé à l'utilisateur s'il n'est pas en possession de la clé nécessaire.

Remarque : À ce stade, nous souhaitons attirer votre attention sur le fait que les pilotes hérités et mini-filtre se comportent parfois différemment avec des clients *u.trust LAN Crypt*. Bien que pour un dossier la règle Ignorer ce chemin signifie que la protection de l'accès aux fichiers est également désactivée lorsque le pilote de chiffrement du mini-filtre est activé, la protection de l'accès aux fichiers existe toujours dans ces dossiers lorsque le pilote de chiffrement de filtre hérité (anciens clients *u.trust LAN Crypt*) est activé.

Cette option est principalement utilisée pour les fichiers auxquels on accède très fréquemment et qu'il n'y a pas de raison particulière de chiffrer. Cela améliore les performances du système. L'emplacement de l'installation d'*u.trust LAN Crypt* ou celui de Windows lui-même est également ignoré par le chiffrement. En principe, aucun fichier ne peut être chiffré ou déchiffré au niveau des emplacements pour lesquels l'option **Ignorer ce chemin** a été sélectionnée. *u.trust LAN Crypt* ignore complètement ces fichiers.

Inclure les sous-répertoires

Les sous-répertoires ou sous-dossiers ne sont pas inclus dans le chiffrement, sauf indication contraire. Pour inclure tous les sous-répertoires ou sous-dossiers dans le chiffrement, sélectionnez l'option **Inclure les sous-répertoires**.

Exemple :

Entrée : `c:\company\my_data\*.* Inclure les sous-répertoires`

Cette règle de chiffrement chiffre tous les fichiers dans :

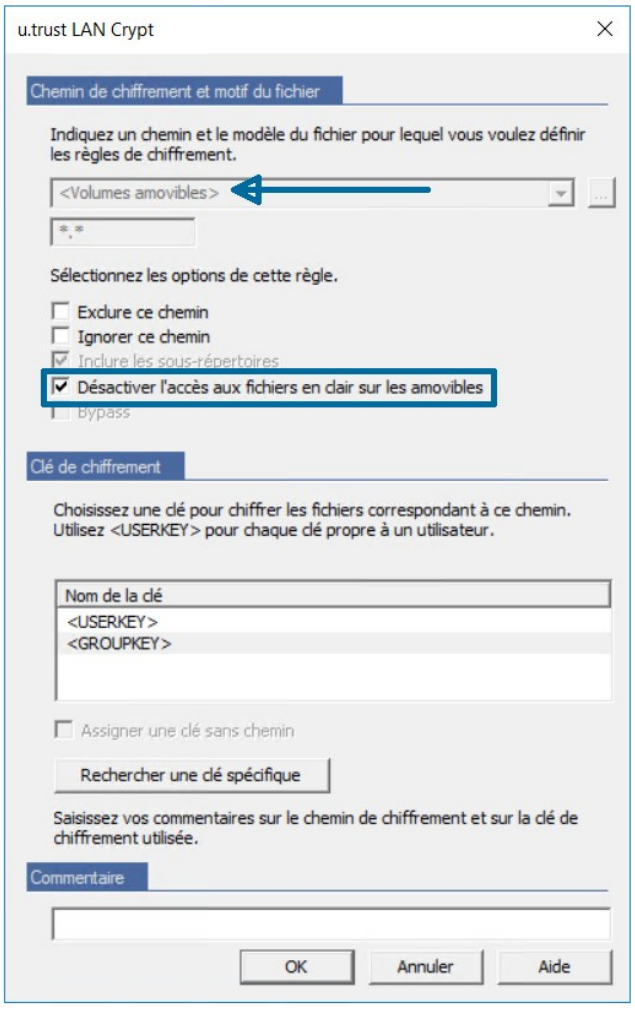
C:\company\my_data

C:\company\my_data\project X

C:\company\my_data\project X\demo

Désactiver l'accès aux fichiers en clair sur les amovibles

Cette option n'est disponible que pour les règles de chiffrement pour lesquelles <*Volumes amovibles*> est défini comme chemin prédéfini. Si vous avez défini l'option **Désactiver l'accès aux fichiers en clair sur les amovibles**, l'accès aux fichiers non chiffrés (fichiers en clair) stockés sur des supports amovibles (tels que des disques durs externes, des clés USB, etc.) pour lesquels une règle de chiffrement existe est refusé. Les utilisateurs ne peuvent alors ni lire ni ouvrir de tels fichiers.



En définissant l'option **Désactiver l'accès aux fichiers en clair sur les amovibles**, vous pouvez, entre autres, empêcher l'installation de programmes non autorisés sur les supports Volumes amovibles, tels que les sticks USB.

Remarque : Dès que vous activez cette option, l'option **Inclure les sous-répertoires** pour la règle de chiffrement est également définie automatiquement.

Remarque : Vous devez attribuer une clé à cette règle de chiffrement.

Règle de Bypass

u.trust LAN Crypt permet en option de créer une règle de **Bypass**. Tous les chemins pour lesquels une telle règle existe sont complètement ignorés par le mini pilote de filtre *u.trust LAN Crypt*. Les fichiers situés dans de tels chemins ne peuvent y être ni chiffrés ni déchiffrés. Par rapport à l'option **Ignorer ce chemin**, les accès aux fichiers ne sont pas du tout surveillés par le pilote de mini filtre dans les chemins pour lesquels une règle de bypass s'applique.

Remarque : Dès que vous activez cette option, l'option **Inclure les sous-répertoires** pour la règle de chiffrement est également définie automatiquement.

Attention : N'activez cette option que si un membre du personnel du support Utimaco vous l'a demandé !

Remarque : Les variables d'environnement ne sont pas prises en charge dans les règles de *bypass*.

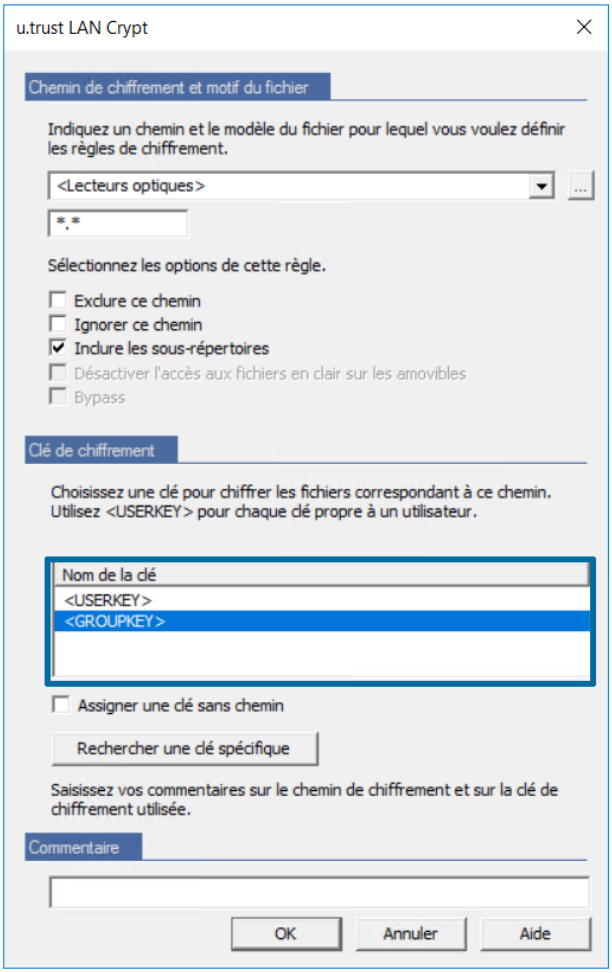
Remarque : Dans les règles de bypass, les lecteurs réseau ne doivent pas être configurés en utilisant une lettre de lecteur. Vous devez toujours utiliser le chemin UNC.

Remarque : Après avoir défini ou supprimé une règle de *bypass*, vous devez redémarrer l'ordinateur client.

Remarque : Cette fonction n'est disponible à ce stade que si vous avez activé l'option **L'administration est propriétaire des règles de bypass dans le Registre** dans le nœud **Paramètres centraux**, dans l'onglet **Résolution des règles**.

Si vous souhaitez créer une règle de chiffrement avec une clé, procédez comme suit :

5. Sélectionnez une clé dans la liste.



Remarque : La vue par défaut affiche uniquement les espaces réservés pour <*USERKEY*> et <*GROUPKEY*> ainsi que les clés créées par un responsable de la sécurité. Le bouton **Rechercher une clé spécifique** vous permet de rechercher et d'afficher les clés spécifiques.

Le chemin de chiffrement et la clé forment une règle de chiffrement *u.trust LAN Crypt*. L'ensemble des règles de chiffrement que vous définissez pour l'utilisateur ou le groupe en constituent le profil de chiffrement.

<USERKEY>

En outre, une clé <*USERKEY*> est toujours incluse dans la liste des clés. Il s'agit d'un espace réservé pour une clé spécifique à l'utilisateur. Le système le génère automatiquement pour chaque utilisateur lorsqu'il résout les règles de chiffrement.

<GROUPKEY>

De la même manière que pour <*USERKEY*>, vous pouvez utiliser <*GROUPKEY*> pour générer une clé commune pour tous les membres du groupe.

Remarque : Lorsque vous utilisez <USERKEY>, assurez-vous que seul l'utilisateur auquel cette clé a été assignée accède aux données. Les autres utilisateurs ne peuvent pas déchiffrer ces données !

Exemple : Exemple d'utilisation possible de *<USERKEY>* : tous les utilisateurs travaillent sur le même lecteur réseau `U:`, qui contient un répertoire par utilisateur. Seul l'utilisateur approprié doit pouvoir accéder à ce répertoire.

Voici à quoi peut ressembler une règle de chiffrement permettant de spécifier cela :

```
U:\*.* <USERKEY>
```

Il est également possible d'utiliser *<USERKEY>* pour chiffrer des répertoires temporaires locaux.

Assigner une clé sans chemin

La liste des chemins de chiffrement définis comprend également un espace réservé appelé *Assigner une clé sans chemin*.

Son utilisation permet aux utilisateurs d'obtenir une clé pour accéder aux données chiffrées pour lesquelles il n'existe pas de chemin de chiffrement. Cela peut notamment se produire si des fichiers chiffrés sont copiés à un emplacement pour lequel aucune règle de chiffrement n'a été définie (avec chiffrement désactivé). Les utilisateurs peuvent alors utiliser cette clé pour accéder aux fichiers avec la clé appropriée. En outre, une *clé sans chemin* est généralement nécessaire pour chiffrer à nouveau les données, et toujours lorsque cette (ancienne) clé ne comporte plus de règle de chiffrement (voir également la remarque de la section « *Règles de chiffrement* à la page 145).

Si une clé est assignée sans chemin, le système crée automatiquement un espace réservé pour permettre la génération d'autres clés sans chemin.

6. Sélectionnez les options pertinentes.
7. Sous *Commentaire*, vous pouvez saisir une description ou des informations relatives à la règle de chiffrement créée.
8. Cliquez sur **OK**.

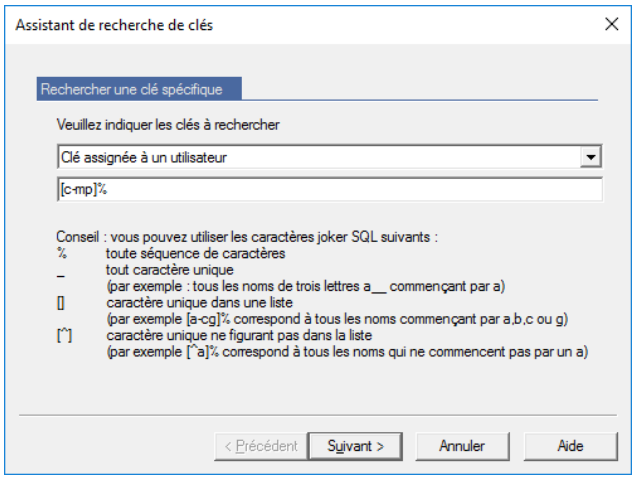
La nouvelle règle de chiffrement apparaît dans l'administration *u.trust LAN Crypt*.

Pour modifier les règles de chiffrement existantes, sélectionnez-les et cliquez sur **Propriétés** dans le *menu contextuel*. Vous pouvez également double-cliquer sur l'entrée correspondante.

Remarque : La modification des règles de chiffrement est uniquement possible dans les groupes dans lesquels elles ont été créées.

3.16.5 Rechercher une clé spécifique

Appuyez sur le bouton **Rechercher une clé spécifique** pour lancer un assistant de recherche de clés spécifiques. Sélectionner une clé dans l'assistant permet de l'ajouter à la liste de clés et de l'utiliser pour les règles de chiffrement. La clé n'est ajoutée que temporairement. Si l'assistant est exécuté à nouveau et qu'une clé différente est sélectionnée, la clé ajoutée précédemment est supprimée 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 assignée à un utilisateur**

  Recherche toutes les clés spécifiques assignées à un utilisateur. Entrez le nom d'utilisateur ou le nom de connexion dans le champ d'édition (condition de recherche). Pour effectuer une recherche par caractères génériques, vous pouvez utiliser des caractères génériques SQL. Par exemple, « Peter% » recherche toutes les clés assignées aux utilisateurs dont les noms d'utilisateur ou les noms de connexion commencent par « Peter ».

- **Clé assignée 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 avec un nom particulier. Entrez le nom long ou le nom court de la clé.

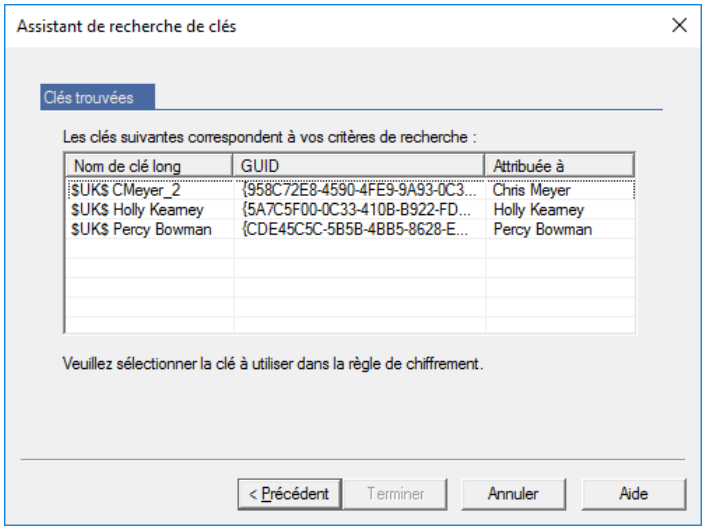
- **GUID de la clé**

  Recherche toutes les clés spécifiques avec un GUID particulier. Saisissez le GUID de la clé.

- **Clés actuellement non assignées**

  Affiche toutes les clés qui ne sont actuellement pas assignées à un utilisateur ou à un groupe.

Les résultats de recherche s'affichent sur la deuxième page.



Si une clé est actuellement assignée, le nom de l'utilisateur ou du groupe apparaît sous **Attribuée à**. La liste répertorie uniquement les clés spécifiques, même si des clés non spécifiques peuvent correspondre aux critères de recherche.

Sélectionnez une clé et cliquez sur **Terminer** pour l'ajouter à la liste contenue dans la boîte de dialogue de création de règles de chiffrement.

3.17 Balises de chiffrement

Si un produit DLP identifie des données qui doivent être chiffrées, il peut utiliser l'API client *u.trust LAN Crypt* pour chiffrer ces fichiers. Dans l'administration *u.trust LAN Crypt*, vous pouvez définir différentes balises de chiffrement qui spécifient la clé *u.trust LAN Crypt* à utiliser.

L'API client peut utiliser ces balises de chiffrement prédéfinies dans le but d'appliquer des clés spéciales pour différents contenus. Par exemple, la balise de chiffrement <CONFIDENTIAL> permet de chiffrer tous les fichiers classés comme « confidentiels » par votre produit DLP.

Voici un exemple d'utilisation de référence à une clé :

```
SGFEAPI encrypt /Tag:CONFIDENTIAL c:\documents\financial-figures.docx
```

Chiffre le fichier financial-figures.docx du dossier c:\documents à l'aide de la clé associée à la balise *<CONFIDENTIAL>*.

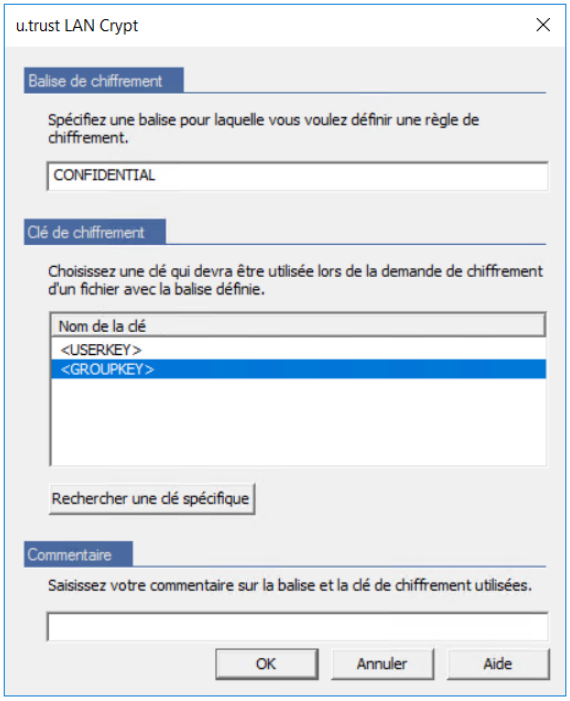
Générer une balise de chiffrement.

1. Cliquez avec le bouton droit sur **Règles et balises de chiffrement** sous le 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 en cliquant avec le bouton droit dans le volet de droite de la console. Le volet de droite de la console vous permet de voir toutes les règles de chiffrement qui ont été générées.

2. Entrez un nom pour la balise de chiffrement dans le champ de saisie sous *Balise de chiffrement*.

3. Sélectionnez une clé.



Pour plus de détails, veuillez consulter la documentation de l'API client dans le dossier \api de votre package d'installation décompressé.

Remarque : La vue par défaut affiche uniquement les espaces réservés pour <USERKEY> et <GROUPKEY> ainsi que les clés créées par un responsable de la sécurité. Le bouton **Rechercher une clé spécifique** vous permet de rechercher et d'afficher les clés spécifiques (voir la section précédente à la page 160).

<USERKEY>

En outre, une clé *<USERKEY>* est toujours incluse dans la liste des clés. Il s'agit d'un espace réservé pour une clé spécifique à l'utilisateur. Le système le génère automatiquement pour chaque utilisateur lorsqu'il résout les règles de chiffrement.

<GROUPKEY>

De la même manière que pour *<USERKEY>*, vous pouvez utiliser *<GROUPKEY>* pour générer une clé commune pour tous les membres du groupe.

Remarque : Lorsque vous utilisez <USERKEY>, assurez-vous que seul l'utilisateur auquel cette clé a été assignée accède aux données. Les autres utilisateurs ne peuvent pas déchiffrer ces données !

4. Sous *Commentaire*, vous pouvez saisir une description ou des informations relatives à la balise de chiffrement créée.

5. Cliquez sur **OK**.

La nouvelle balise de chiffrement apparaît dans l'administration *u.trust LAN Crypt*.

Pour modifier des balises de chiffrement existantes, sélectionnez-les et cliquez sur **Propriétés** dans le menu contextuel. Vous pouvez également double-cliquer 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 l'administration *u.trust LAN Crypt*, par le biais de son certificat.

Chaque profil est protégé par la clé publique de son propriétaire. Un certificat (fichier *.p12) est assigné à chaque utilisateur par le biais de l'administration *u.trust LAN Crypt*. Ce fichier contient également la clé privée. La clé privée est protégée contre tout accès non autorisé par un code PIN. *u.trust LAN Crypt* écrit le code PIN correspondant dans le fichier journal du mot de passe (`p12pwlog.csv`). Ce fichier doit toujours être particulièrement protégé contre tout accès non autorisé. Pour ce faire, le responsable (principal) de la sécurité de l'administration *u.trust LAN Crypt* peut installer l'application cliente *u.trust LAN Crypt* et créer une règle de chiffrement pour le fichier journal du mot de passe.

Remarque : Si vous installez les deux composants *u.trust LAN Crypt*, la console d'administration et l'application client sur le même ordinateur, ils doivent toujours être de la même version.

La mise à disposition préalable des certificats dans le magasin de certificats ou dans un répertoire (par exemple, LDAP) avant le début de leur assignation est recommandée. Vous pouvez utiliser les outils Windows standard pour importer les certificats dans le magasin de certificats concerné.

u.trust LAN Crypt dispose d'un *Assistant d'assignation de certificats* qui assigne automatiquement les certificats.

Remarque : Si l'utilisateur Windows qui assigne un certificat ne dispose pas du droit de modification pour le fichier journal du mot de passe dans le système de fichiers, aucun certificat *u.trust LAN Crypt* ne peut être généré.

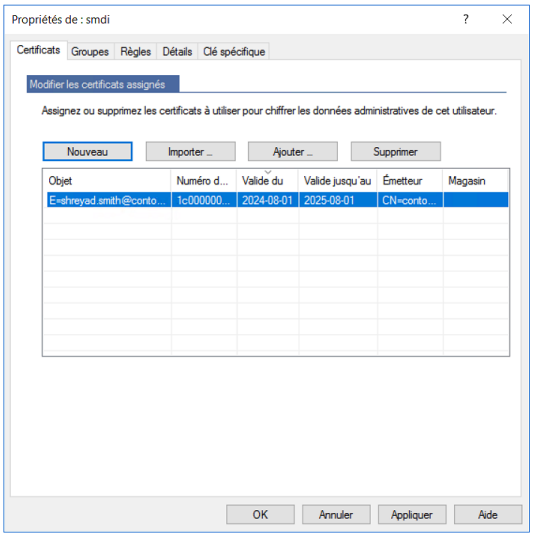
3.18.1 Assignation d'un certificat à un utilisateur

Pour assigner un certificat, procédez comme suit :

1. Sélectionnez **Membres et certificats du groupe** dans le nœud du groupe concerné. Une liste de tous les utilisateurs s'affiche dans le volet de droite de la console.

2. Double-cliquez sur un utilisateur, ou cliquez avec le bouton droit sur l'utilisateur, puis sélectionnez **Propriétés** dans le menu contextuel. La boîte de dialogue *Propriétés* s'affiche.

3. Dans cette boîte de dialogue, sélectionnez l'une des options suivantes pour assigner un ou plusieurs certificats à l'utilisateur :



- **Nouveau**

  Cliquez sur **Nouveau** si vous souhaitez que *u.trust LAN Crypt* génère un nouveau certificat pour l'utilisateur. Si aucun certificat n'est disponible, la console d'administration d'*u.trust LAN Crypt* peut même générer des certificats elle-même. Cependant, seul *u.trust LAN Crypt* doit utiliser ces certificats !

  Le certificat généré est enregistré en tant que fichier PKCS#12 dans le répertoire par défaut (voir l'onglet **Répertoires** dans le nœud **Paramètres centraux**).

  Remarque : Tout certificat généré de cette manière doit ensuite être distribué à l'utilisateur approprié. Dans le cas contraire, l'utilisateur ne pourra pas accéder à ses profils de chiffrement.

- **Importer …**

  Si le certificat dont vous avez besoin n'est pas encore présent dans le magasin de certificats, il n'apparaît pas dans la liste des certificats disponibles.

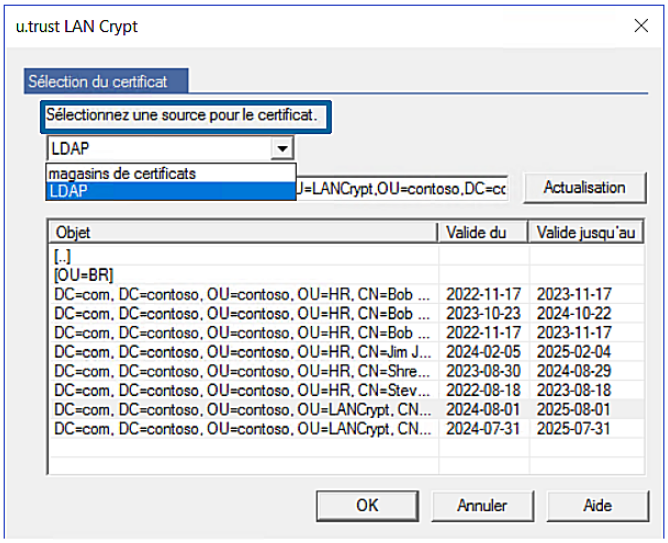
  Dans ce cas, cliquez sur **Importer …** pour que le système ouvre une boîte de dialogue dans laquelle vous pourrez sélectionner le certificat requis. Cliquez ensuite sur **OK**. Le système assigne alors le certificat à l'utilisateur.

Le certificat d'importation est automatiquement importé dans le magasin de certificats nommé *Autres personnes*.

Remarque : Seuls les fichiers de certificats dont le format est **.cer*, **.crt* ou **.der* peuvent être importés. Il est impossible d'importer des fichiers **.p12* ou **.pfx*.

- **Ajouter …**

  Sélectionnez la source du certificat :



Assignation de certificats à partir du magasin de certificats

Ouvre une boîte de dialogue dans laquelle vous pouvez assigner un certificat existant à un utilisateur. Cette boîte de dialogue affiche une liste de tous les certificats présents dans le magasin de certificats.

Attribution de certificats à l'aide d'une source LDAP

u.trust LAN Crypt vous permet d'assigner des certificats à partir d'une source LDAP.

Pour ce faire, sélectionnez **LDAP** dans la liste déroulante de la boîte de dialogue *Sélectionner une source pour le certificat*.

Un champ d'édition apparaît, dans lequel vous pouvez saisir 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_UO_1]) représentent les UO de la source LDAP. Pour afficher les certificats d'une UO, double-cliquez tout simplement dessus.

Double-cliquez sur **[..]** pour monter d'un niveau dans la hiérarchie.

Sélectionnez un certificat et cliquez sur **OK**. Le certificat est maintenant attribué au responsable de la sécurité.

Remarque : Si le serveur LDAP n'autorise pas l'ouverture de session anonyme, les identifiants de connexion du serveur doivent être saisis comme nom absolu (exemple : CN=Jane Doe,OU=Sales) dans l'onglet Serveur des **Paramètres centraux**.

Remarque : Si vous disposez d'un certificat assigné à partir d'un annuaire LDAP, la clé privée appartenant à ce certificat doit être disponible sur le poste de travail de l'utilisateur.

4. Utilisez l'une des options décrites pour sélectionner un certificat et cliquez sur **OK**.

   Le système affiche le certificat dans le volet de la console, sur le côté droit et en regard de l'utilisateur. Dans le volet de la console, le système affiche des informations sur le certificat utilisé (période de validité, numéro de série, émetteur).

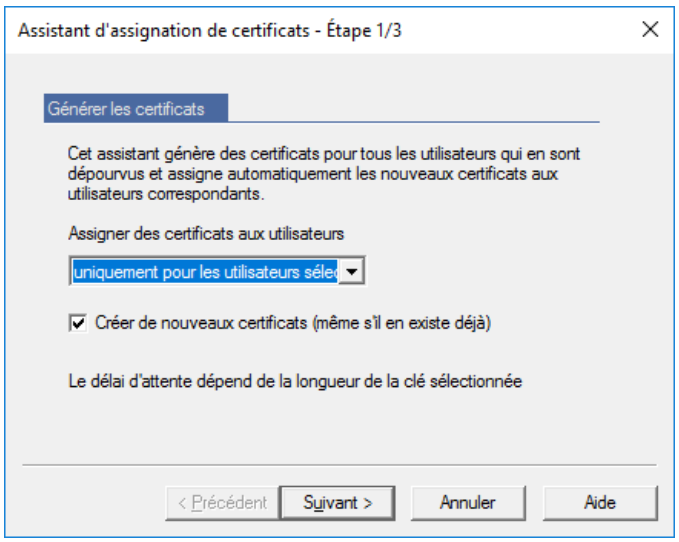
   Remarque : Le composant logiciel enfichable de certificat est disponible sous chaque nœud de groupe ou d'utilisateur. Ici, le système affiche uniquement les utilisateurs qui sont membres du groupe concerné.

3.18.2 Génération et assignation de certificats u.trust LAN Crypt

Utilisez cet assistant pour générer des certificats pour **tous** les utilisateurs auxquels aucun certificat n'a encore été assigné, puis assigner automatiquement ces certificats aux utilisateurs.

Pour ouvrir cet assistant, cliquez sur **Créer des certificats** dans le menu contextuel de chaque nœud *Membres et certificats du groupe* ou sur l'icône appropriée dans la barre d'outils.

Dans la boîte de dialogue suivante, spécifiez si vous générez et assignez les certificats **uniquement dans ce groupe**, **dans ce groupe et tous les sous-groupes** ou **uniquement pour les utilisateurs sélectionnés**.



Si vous cochez l'option **Créer de nouveaux certificats (même s'il en existe déjà)**, de nouveaux certificats seront créés pour tous les utilisateurs sélectionnés.

Uniquement pour les utilisateurs sélectionnés

Cette option ne s'affiche que si un ou plusieurs utilisateurs sont sélectionnés. Lorsque vous cliquez sur *Membres et certificats du groupe* sous le nœud de groupe souhaité dans le volet de gauche de la console, les membres du groupe s'affichent dans le volet de droite de la console. La sélection des utilisateurs fonctionne de la même manière que dans l'Explorateur Windows (sélectionnez les utilisateurs avec le bouton gauche de la souris tout en appuyant sur la touche Maj ou Ctrl).

Le système génère et assigne 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 spécifié dans les **Paramètres centraux**, et doivent être mis à la disposition des utilisateurs. Pour cela, dans la configuration *u.trust LAN Crypt*, spécifiez le dossier dans lequel *u.trust LAN Crypt* doit rechercher un fichier **.p12* pour l'utilisateur si la clé privée du fichier de stratégie n'est pas présente.

Il en va de même pour la partie publique du certificat du responsable de la sécurité. Les noms de fichiers doivent correspondre au nom de connexion de l'utilisateur (« `connexion.p12` ») afin qu'*u.trust LAN Crypt* puisse reconnaître automatiquement les fichiers de clés utilisateur.

Lorsqu'*u.trust LAN Crypt* trouve le bon fichier, il affiche une boîte de dialogue PIN. Vous devez envoyer une lettre PIN pour indiquer ce code PIN à l'utilisateur (qui se trouve dans le *fichier journal du mot de passe*). Le certificat et la clé associée sont automatiquement importés après que l'utilisateur a saisi le code PIN.

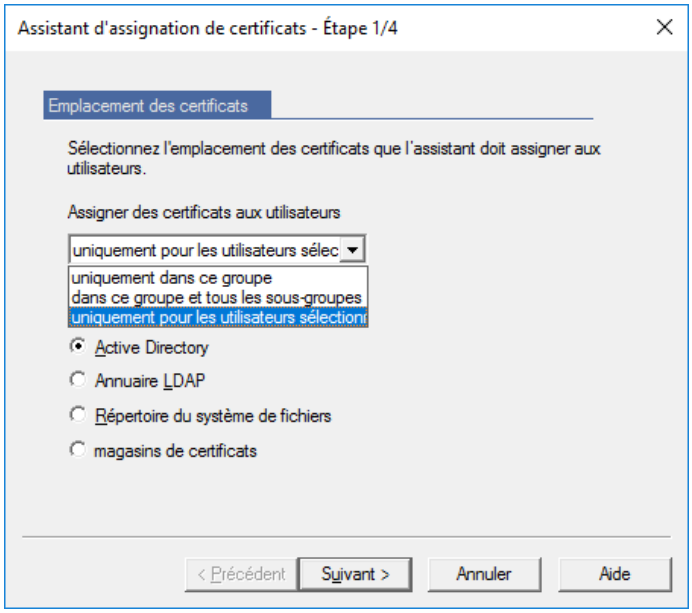
Si *u.trust LAN Crypt* trouve un fichier **.cer* contenant la partie publique du certificat du responsable de la sécurité, il l'importe automatiquement.

Alternativement, vous pouvez distribuer manuellement les fichiers de clés des utilisateurs et la partie publique du certificat d'administrateur. Si vous faites cela, assurez-vous que les clients les importent tous les deux.

3.18.3 Assistant d'assignation de certificats

u.trust LAN Crypt dispose d'un assistant qui effectue la plupart des tâches liées à l'assignation de certificats aux utilisateurs. Pour exécuter cet assistant, sélectionnez **Assistant d'assignation de certificats** dans le menu contextuel des *Membres et certificats du groupe*.

Dans la première boîte de dialogue de l'assistant, spécifiez si vous assignez les certificats aux membres qui se trouvent **uniquement dans ce groupe**, **dans ce groupe et tous les sous-groupes** ou **uniquement pour les utilisateurs sélectionnés**.



Uniquement pour les utilisateurs sélectionnés

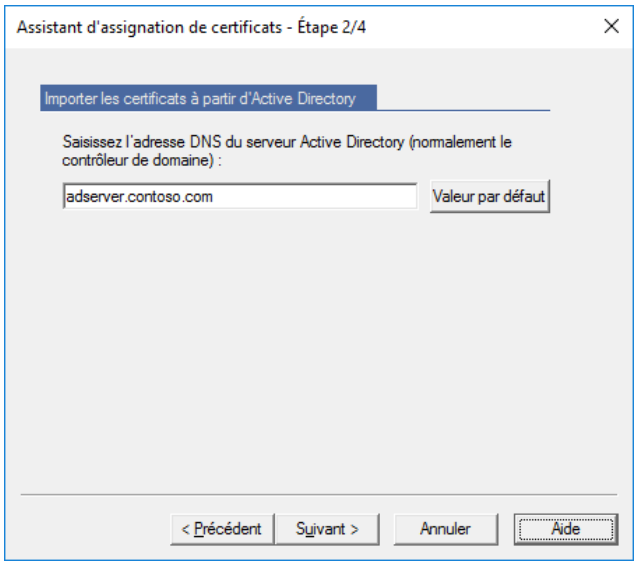
Cette option ne s'affiche que si un ou plusieurs utilisateurs sont sélectionnés. Lorsque vous cliquez sur *Membres et certificats du groupe* sous le nœud de groupe souhaité dans le volet de gauche de la console, les membres du groupe s'affichent dans le volet de droite de la console. La sélection des utilisateurs fonctionne de la même manière que dans l'Explorateur Windows (sélectionnez les utilisateurs avec le bouton gauche de la souris tout en appuyant sur la touche Maj ou Ctrl).

L'assistant prend en charge l'assignation de certificats à partir des sources suivantes :

- Assigner des certificats aux utilisateurs à partir d'**Active Directory**
- Assigner des certificats aux utilisateurs à partir de l'**annuaire LDAP**
- Assigner des certificats aux utilisateurs à partir d'un **répertoire de système de fichiers**
- Assigner des certificats aux utilisateurs à partir du **magasin de certificats**

3.18.3.1 Assignation de certificats à partir d'Active Directory

Si vous avez sélectionné l'option *Assigner des certificats aux utilisateurs à partir d'Active Directory*, vous devez saisir le nom d'un contrôleur Active Directory au format FQDN à l'étape 2 (par exemple : « `adserver.contoso.com` »).



Si vous cliquez sur **Valeurs par défaut**, le système applique l'adresse du contrôleur de domaine auquel vous êtes actuellement connecté.

Pour démarrer l'assistant, cliquez sur **Suivant**. Le système importe et assigne les certificats automatiquement. Il affiche un message pour confirmer qu'il a bien assigné les certificats. Cliquez sur **Terminer** pour fermer l'assistant.

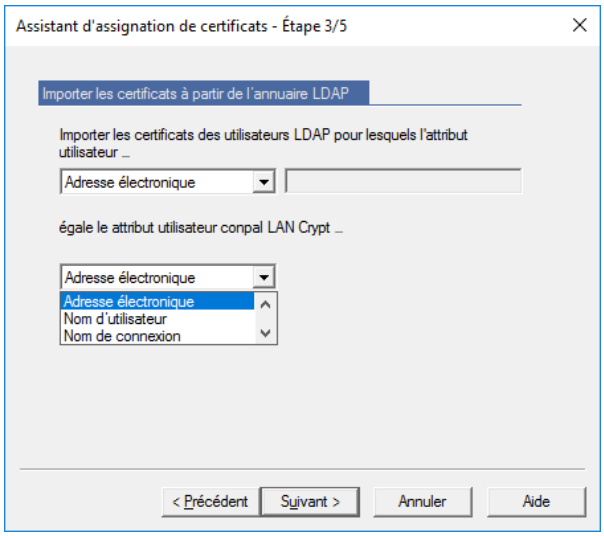
3.18.3.2 Assignation de certificats à partir d'un annuaire LDAP

Si vous sélectionnez l'option **Assigner des certificats aux utilisateurs à partir d'un annuaire LDAP**, vous devez entrer l'adresse de l'annuaire LDAP à partir duquel vous souhaitez importer les certificats à l'étape 2.

Remarque :
Microsoft AD :
Le champ de saisie ne doit pas rester vide. Ici, vous devez entrer au moins le domaine et le pays.
Exemple 1 : `DC=mydomain,DC=COM`
Exemple 2 : `OU=marketing,DC=mydomain,DC=COM`

Si vous cliquez sur **Valeurs par défaut**, le système applique l'adresse du contrôleur de domaine auquel vous êtes actuellement connecté.

Pour assigner les certificats, le système fait correspondre les propriétés de l'utilisateur LDAP avec l'utilisateur *u.trust LAN Crypt*.



Il est possible d'utiliser les propriétés de l'utilisateur LDAP suivantes :

- Adresse électronique
- Nom commun (CN)
- Nom d'affichage
- Nom de compte NT 4.0
- Nom principal utilisateur (UPN)
- Nom de famille
- Autre, attribut défini par l'utilisateur

Vous pouvez indiquer que ces propriétés correspondent aux propriétés de l'utilisateur *u.trust LAN Crypt* suivantes :

- Adresse électronique
- Nom d'utilisateur
- Nom de connexion
- Commentaire

Sélectionnez la propriété de l'utilisateur LDAP à laquelle vous souhaitez que chaque propriété de l'utilisateur *u.trust LAN Crypt* corresponde.

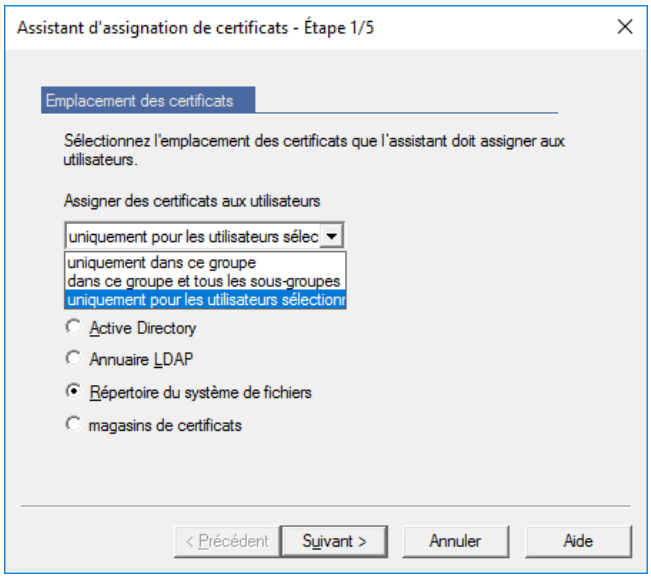
Si ces propriétés correspondent, le système importe le certificat de l'utilisateur LDAP et l'assigne automatiquement à l'utilisateur *u.trust LAN Crypt* approprié.

Remarque : Pour éviter les incohérences, nous vous recommandons d'utiliser l'*adresse électronique* comme critère d'assignation, car elle est toujours unique.

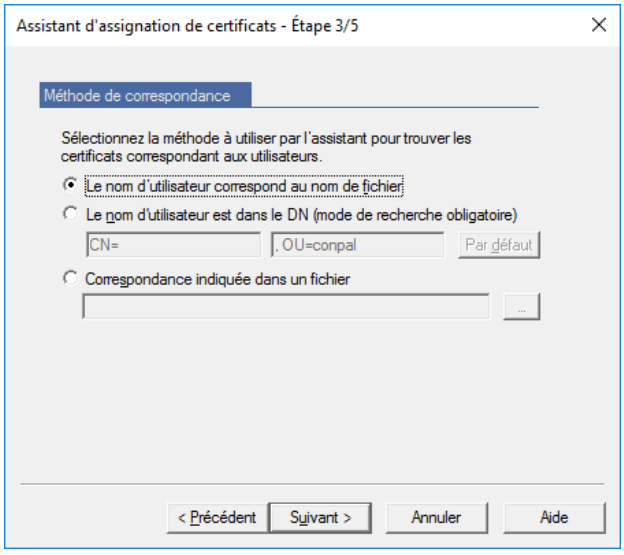
Pour démarrer l'assistant, cliquez sur **Suivant**. Le système importe et assigne les certificats automatiquement. Il affiche un message pour confirmer qu'il a bien assigné les certificats. Cliquez sur **Terminer** pour fermer l'assistant.

3.18.3.3 Assignation de certificats à partir d'un répertoire

Si vous sélectionnez l'option **Assigner des certificats aux utilisateurs à partir d'un répertoire de système de fichiers**, vous devez saisir l'adresse du répertoire à partir duquel vous souhaitez importer les certificats à l'étape 2.



Une fois le répertoire spécifié, une boîte de dialogue s'affiche. Vous y définissez la méthode qu'*u.trust LAN Crypt* doit utiliser pour assigner des certificats aux utilisateurs.



- **Le nom d'utilisateur correspond au nom de fichier**

  Sélectionnez cette option si les noms des fichiers de certificat sont identiques au nom d'utilisateur.

  Tous les utilisateurs qui correspondent à un nom de fichier sont assignés au certificat approprié.

- **Le nom d'utilisateur est dans le DN (mode de recherche obligatoire)**

  Si le nom de l'utilisateur est contenu dans le *nom absolu* du certificat, *u.trust LAN Crypt* peut le rechercher et assigner le certificat à l'utilisateur approprié. *u.trust LAN Crypt* utilise un modèle de recherche pour identifier le nom de l'utilisateur dans le DN.

  Vous pouvez spécifier ce modèle de recherche dans le champ de saisie situé sous l'option **Le nom d'utilisateur est dans le DN**. Le système recherche le nom de l'utilisateur qui apparaît entre les chaînes de deux caractères spécifiés dans le DN.

  Exemple :

  Dans le certificat, le nom d'utilisateur est toujours présent sous « CN= ».

  (par exemple `CN=JSmith,OU=Utimaco`)

  Si vous entrez `CN=` dans le premier champ de saisie et `OU=Utimaco` dans le second, u.trust LAN Crypt recherche le nom d'utilisateur qui se trouve entre ces chaînes de deux caractères (dans notre exemple, JSmith). Le certificat est automatiquement assigné à l'utilisateur.

- **Correspondance indiquée dans un fichier**

  Vous pouvez également extraire l'assignation requise d'un fichier.

  Par exemple, la partie publique du certificat généré avec l'administration de cartes à puce Utimaco est enregistrée dans un fichier de répertoire prédéfini. À l'aide de ces fichiers, l'administration de cartes à puce Utimaco génère un fichier qui enregistre le certificat assigné à chaque utilisateur. D'autres PKI peuvent également générer des listes de ce type. Bien entendu, cette liste peut même se générer elle-même.

  Elle doit utiliser le format suivant :

  nom d'utilisateur;nom de fichier

  Exemple :

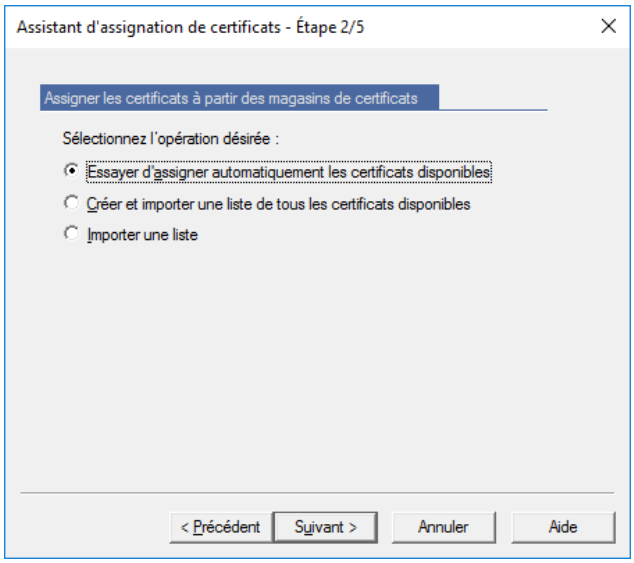
  ```
  Invité;Invité.cer
  JSmith;JSmith.cer
  ....
  ```

Le système assigne les certificats en fonction de l'assignation contenue dans ce fichier.

Cliquez sur **Suivant** pour démarrer l'assistant et assigner automatiquement les certificats.

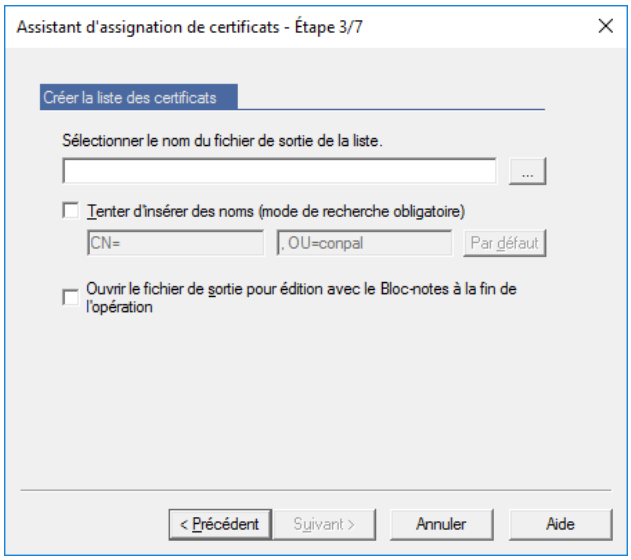
3.18.3.4 Assignation de certificats à partir des magasins de certificats

Si vous avez sélectionné l'option **Assigner des certificats aux utilisateurs à partir des magasins de certificats**, la deuxième étape de l'assistant vous invite à indiquer s'il faut générer une liste de tous les certificats disponibles et les importer, ou si une liste existante doit être importée. *u.trust LAN Crypt* utilise cette liste pour assigner les certificats.



Vous pouvez, par exemple, utiliser l'option **Importer une liste créée précédemment** si le processus d'assignation a déjà été démarré, mais a été interrompu après la génération de la liste. Le système peut ensuite réutiliser le fichier créé ici.

Si vous sélectionnez l'option **Créer et importer une liste de tous les certificats disponibles**, le système affiche cette boîte de dialogue.



Choisissez un fichier ans lequel écrire la liste.

u.trust LAN Crypt crée une liste de tous les certificats disponibles dans les magasins de certificats. Cette liste contient des espaces réservés pour les noms d'utilisateurs auxquels le certificat doit être assigné.

Exemple :

```
*****; My; OU=u.trust LAN Crypt Certificate, CN=LAN Crypt Admin; 0010-ae671e47...
*****; Root; CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com; 0010-4cad...
```

Les espaces réservés (*****) peuvent être remplacés par les noms d'utilisateur.

Si le certificat contient le nom de l'utilisateur, vous pouvez utiliser l'option suivante :

- **Tenter d'insérer des noms**

  u.trust LAN Crypt peut tenter de reconnaître un utilisateur. En effet, si le *nom absolu* (DN) du certificat contient le nom de l'utilisateur, *u.trust LAN Crypt* peut le rechercher et assigner le certificat à l'utilisateur approprié. *u.trust LAN Crypt* utilise un mode de recherche pour identifier le nom d'utilisateur dans le DN.

  Indiquez le mode de recherche dans le champ de saisie situé sous l'option « *Le nom d'utilisateur est dans le DN* ». Le système recherche le nom de l'utilisateur qui se trouve entre les chaînes de deux caractères spécifiés dans le DN.

  Exemple :

  Dans le certificat, le nom de l'utilisateur est toujours présent sous « CN= ».

  (par exemple `CN=JDoe,OU=Utimaco`)

  Si vous saisissez *CN=* dans le premier champ de saisie et *OU=Utimaco* dans le deuxième, *u.trust LAN Crypt* recherche le nom de l'utilisateur qui se trouve entre ces chaînes de deux caractères (dans notre exemple, JDoe). Le système remplace l'espace réservé par le nom de l'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 ouvre la liste des certificats après qu'elle a été générée. Vous pouvez maintenant modifier cette liste. Vous pouvez remplacer l'espace réservé par le nom de l'utilisateur dans les certificats correspondants. Lorsque vous enregistrez la liste, le système utilise la version modifiée pour assigner des certificats.

Cliquez sur **Suivant** pour démarrer l'assistant et assigner automatiquement les certificats.

3.19 Fournir des règles de chiffrement - générer des fichiers de stratégie

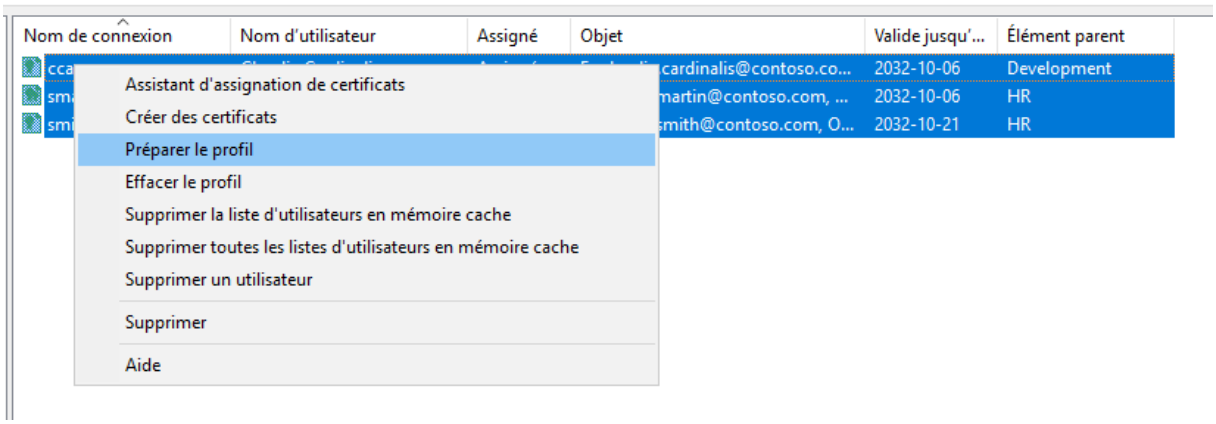
u.trust LAN Crypt enregistre tous les profils générés (ou modifiés) dans sa base de données d'administration. Ici, ils n'ont pas encore d'effet sur les utilisateurs individuels.

Pour résoudre les profils individuels et créer les fichiers de stratégie, un responsable de la sécurité *u.trust LAN Crypt* doit exécuter le résolveur de profil d'*u.trust LAN Crypt*. Cela génère des fichiers de stratégie pour chaque utilisateur en fonction des paramètres définis dans la console d'administration. Le système charge le nouveau profil de chiffrement à la connexion suivante de l'utilisateur.

Remarque : Vous devez toujours générer de nouveaux fichiers de stratégie après avoir modifié les paramètres dans la console d'administration d'*u.trust LAN Crypt* (ajout de *nouvelles clés*, de *nouvelles règles*, *TrustBuilder / TrustBuilder MFA*…). Les modifications deviennent effectives pour les utilisateurs une fois les nouveaux fichiers de stratégie chargés sur leurs machines.

3.19.1 Création (résolution) de fichiers de stratégie pour un groupe entier ou des utilisateurs sélectionnés

Les fichiers de stratégie sont créés avec l'Assistant de **préparation des profils**. Si plus d'un utilisateur est sélectionné et que la création des profils est démarrée à partir de la barre d'outils ou du menu contextuel des utilisateurs, l'assistant se lance.



Si seul un utilisateur et l'option *Préparer ou Effacer le profil* sont sélectionnés dans le menu contextuel, le profil est immédiatement créé. Une boîte de message informe le responsable de la sécurité du résultat.

Remarque : Si vous choisissez l'option **Effacer le profil** dans le menu contextuel, un profil vide est créé pour l'utilisateur. Une fois le profil mis à jour par le biais du client *u.trust LAN Crypt*, cet utilisateur n'a plus de règles de chiffrement ni de clés à sa disposition. L'accès aux données chiffrées n'est alors plus possible pour cet utilisateur. À tout moment, vous pouvez à nouveau fournir un profil à l'utilisateur. L'utilisateur ne reçoit son profil de chiffrement que lorsque le profil est à nouveau mis à jour par le biais du client *u.trust LAN Crypt*. Ce profil contient toutes les règles et clés définies pour lui. Il peut alors à nouveau travailler avec des données chiffrées.

Différents points d'entrée sont disponibles pour l'assistant, selon la vue à partir de laquelle celui-ci est lancé :

- **Sélection de la portée** (par défaut)
- **Collecter les utilisateurs et vérifier les certificats :**

  Si aucune sélection de portée n'est possible ou autorisée, par exemple si la création de profils est démarrée pour les utilisateurs sélectionnés dans le nœud **Utilisateurs et certificats sélectionnés**.

- **Création de profils :**

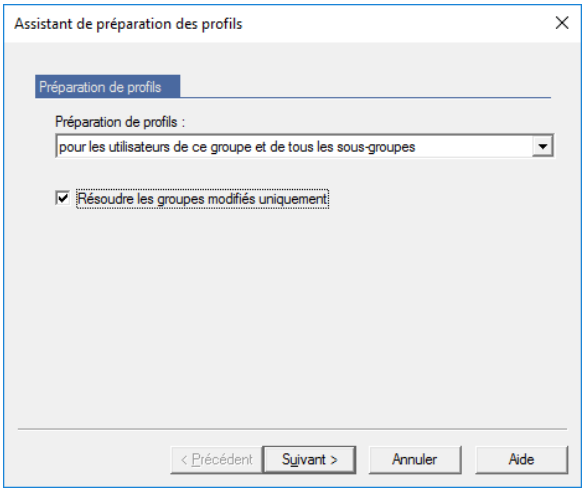
  Si l'action *Effacer le profil* est démarrée pour plusieurs utilisateurs. Cette action ne peut pas être lancée pour un groupe entier. Aucune vérification de certificat n'est nécessaire.

La première page de l'assistant permet de sélectionner la portée de 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
- les utilisateurs sélectionnés uniquement.

  Activez l'option *Résoudre les groupes modifiés uniquement* pour limiter la création de fichiers de stratégie aux utilisateurs pour lesquels de nouveaux fichiers de stratégie sont requis en raison de modifications apportées. Cela peut ainsi accélérer la génération de fichiers de stratégie au sein de grandes organisations.



La deuxième page de l'assistant affiche la progression de la collecte de toutes les données utilisateur et de la vérification des certificats de l'utilisateur. Une fois que tous les utilisateurs ont été traités, la page suivante s'affiche.

La troisième page de l'assistant affiche les avertissements de certificat. Les utilisateurs qui n'ont pas de certificat valide assigné ou ceux dont le certificat expire bientôt sont affichés sur cette page.

Les avertissements et erreurs de certificat suivants s'affichent :

- Le certificat de l'utilisateur expirera bientôt (avertissement).
- Tous les certificats assignés à l'utilisateur ont expiré (erreur).
- Un utilisateur n'a pas de certificat assigné (erreur).
- L'utilisateur n'a pas de certificat assigné et est marqué comme devant être ignoré (avertissement).

En cas d'erreur, au moins une des options de cette page doit être sélectionnée afin de pouvoir continuer la création de profils :

- **Ne plus m'avertir à propos des 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, et ce, 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 également être configuré dans les **Paramètres centraux**.

Cliquez sur le bouton **Précédent** pour revenir à la page de sélection de la portée de l'assistant.

La quatrième page de l'assistant affiche une barre de progression relative à la création de tous les profils. L'assistant peut être annulé, mais cela interrompt uniquement la création de profils. Les fichiers de stratégie déjà créés ne sont ni supprimés ni restaurés.

La cinquième et dernière page de l'assistant affiche le nombre de profils créés. Un message d'erreur s'affiche si une erreur est survenue et a forcé l'interruption de la création de profils.

Remarque : L'apport de modifications aux onglets **Antivirus**, **Résolution des règles** ou **Autres paramètres** dans les **Paramètres centraux** entraîne toujours une modification des fichiers de stratégie de tous les utilisateurs. Après une modification de ce type, de nouveaux fichiers de stratégie doivent être créés pour tous les utilisateurs.

3.19.2 Approvisionnement sélectionné via le composant logiciel enfichable de certificat

Vous pouvez également utiliser le composant logiciel enfichable de certificat pour fournir des fichiers de stratégie. Il est accessible sous le nœud **Membres et certificats du groupe** ainsi que sous chaque nœud de groupe.

Si vous utilisez le composant logiciel enfichable de certificat pour générer des fichiers de stratégie, vous pouvez également utiliser les fonctions supplémentaires suivantes :

- Sélectionnez les utilisateurs auxquels un certificat doit être assigné. Vous n'avez pas besoin de générer de nouveaux fichiers de stratégie pour tous les utilisateurs.

Comme dans l'Explorateur Windows, vous pouvez sélectionner plusieurs utilisateurs en même temps (clic + Maj ou Ctrl).

- Le responsable de la sécurité voit immédiatement quels utilisateurs sont présents dans le groupe.
- Le système affiche des icônes de certificat en regard du nom d'utilisateur pour indiquer le statut de ces certificats :
  - **Une couleur rouge signifie :**
    le certificat a expiré.
  - **Une couleur jaune signifie :**
    le certificat s'exécute dans la période d'avertissement d'expiration configurée.
  - **Une couleur verte signifie :**
    tout fonctionne correctement.
  - **Une couleur grise signifie :**
    soit aucun certificat n'a été assigné à l'utilisateur, soit cet utilisateur a été omis lorsque le système a assigné des certificats.

Pour fournir les fichiers de stratégie, sélectionnez les utilisateurs requis, puis cliquez sur l'icône d'engrenage bleue 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 logiciel enfichable de certificat pour effacer les profils d'un ou plusieurs utilisateurs. Effacer un profil signifie générer un profil vide. L'utilisateur doit se connecter une fois à un fichier de stratégie vide pour écraser les paramètres du fichier de stratégie actuel mis en cache sur sa machine. Après cette opération, il ne peut plus accéder aux données chiffrées.

Pour effacer un profil, sélectionnez l'utilisateur dans le composant logiciel enfichable de certificat et cliquez sur l'icône **Effacer le profil pour l'utilisateur sélectionné** ou cliquez sur **Effacer le profil** dans le menu contextuel.

Vous pouvez sélectionner plusieurs utilisateurs (sélectionnez les utilisateurs avec le bouton gauche de la souris tout en maintenant la touche Maj enfoncée) et effacer leurs profils en cliquant sur l'icône .

Remarque : Les paramètres contenus dans les **Paramètres centraux** d'*u.trust LAN Crypt* définissent la manière dont les profils sont effacés. Le processus d'effacement des profils est similaire à celui de la préparation des profils.

3.20 Journalisation de la base de données

u.trust LAN Crypt enregistre les événements déclenchés par la console d'administration d'*u.trust LAN Crypt* dans la base de données *u.trust LAN Crypt*. Les fonctions de journalisation

d'*u.trust LAN Crypt* vous permettent de spécifier les événements à enregistrer, d'archiver les événements et de consulter les entrées du journal.

Les autorisations globales **Lire les entrées du journal** et **Gérer la journalisation** contrôlent la façon dont les responsables de la sécurité accèdent au module de journalisation. Ces droits peuvent être accordés aux responsables de la sécurité par le responsable principal de la sécurité.

Lire les entrées d'enregistrement	Le responsable de la sécurité peut afficher les paramètres de journalisation ainsi que les événements enregistrés.
Gérer l'enregistrement	Le responsable de la sécurité peut modifier les paramètres de journalisation. Il est autorisé à archiver, supprimer et consulter les entrées.

Les paramètres de base de la journalisation peuvent être définis dans la *console d'administration d'u.trust LAN Crypt*, sous le nœud **Journalisation** dans les **Paramètres centraux**. Seuls les responsables de la sécurité disposant au moins de l'autorisation **Lire les entrées du journal** peuvent afficher ce nœud.

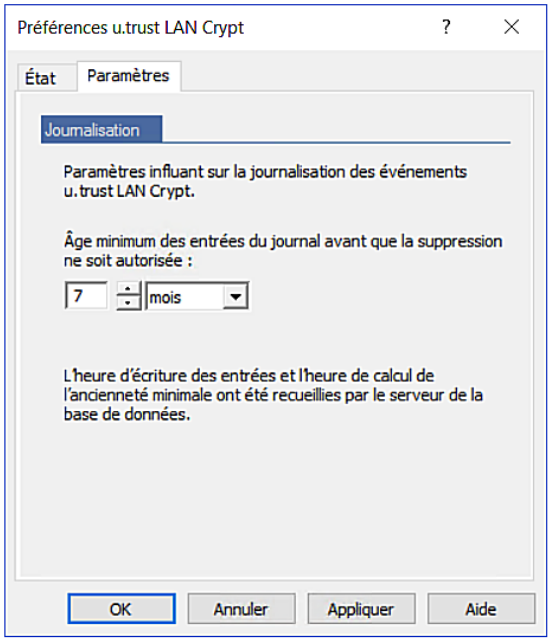
Seul un responsable principal de la sécurité peut définir les paramètres de base. Il est possible de les sécuriser davantage grâce à l'ajout d'un second niveau d'autorisation (scénario **Gérer la journalisation** ; nécessite les autorisations globales **Lire les entrées du journal** et **Gérer la journalisation**).

Les paramètres de base spécifient également les événements à enregistrer. Seul un responsable principal de la sécurité peut spécifier cela.

Remarque : Les événements qui se produisent avant qu'un responsable de la sécurité ne se connecte ne peuvent pas être enregistrés directement dans la base de données. Ils sont mis en cache et écrits dans la base de données après la prochaine connexion réussie.

3.20.1 Paramètres

Cliquez sur *Propriétés* dans le menu contextuel du nœud **Journalisation** pour afficher une boîte de dialogue qui vous permettra de définir les paramètres de base.



Onglet Paramètres

Sur cette page, vous indiquez la période à l'issue de laquelle les entrées du journal peuvent être supprimées.

Lors de l'utilisation de bases de données distribuées, ce paramètre garantit que les entrées peuvent être copiées vers le siège avant leur suppression au niveau des sites individuels.

Onglet État

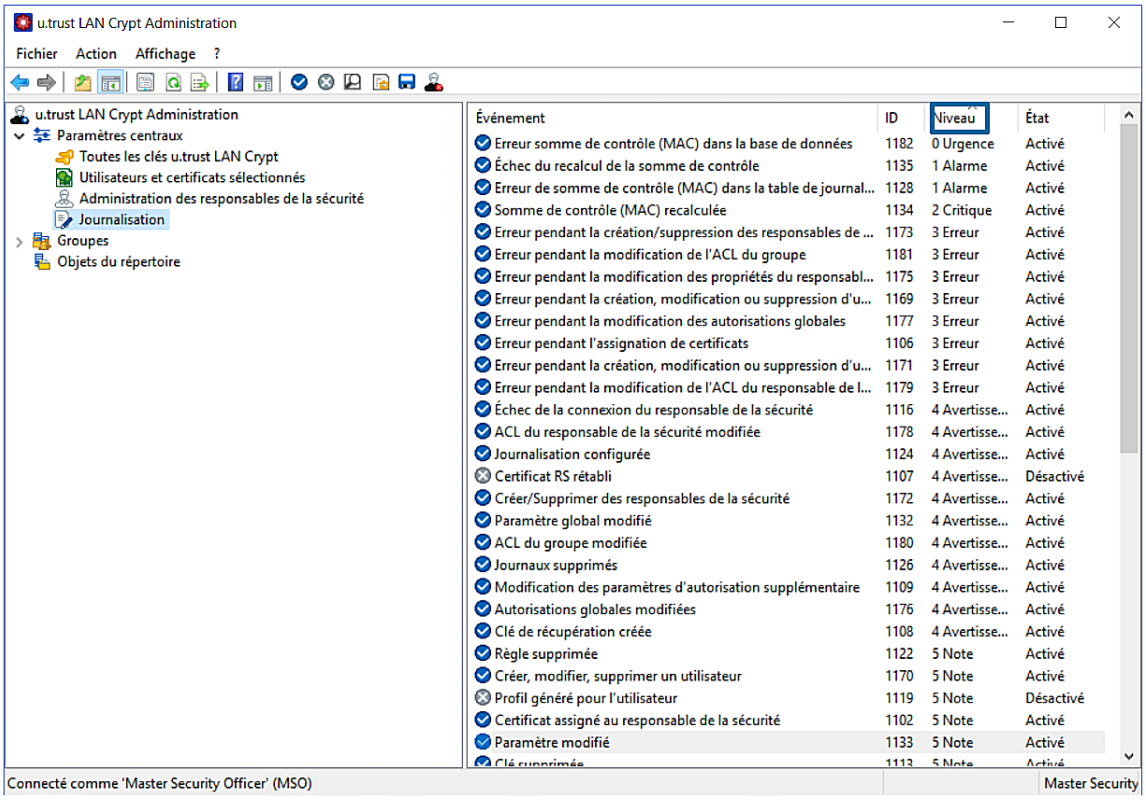
L'onglet **État** affiche des informations sur le nombre d'entrées enregistrées. S'il y a plusieurs emplacements, l'affichage peut être développé pour chaque emplacement. En outre, il indique le nombre d'entrées déjà archivées et si celles-ci peuvent être supprimées.

3.20.2 Événements enregistrés

Si le nœud **Journalisation** est sélectionné, tous les événements pouvant être enregistrés s'affichent dans le volet de droite de la console. Ici, vous pouvez sélectionner l'événement à enregistrer.

Remarque : Seuls les responsables principaux de la sécurité peuvent sélectionner les événements à enregistrer.

Cliquez sur l'en-tête de la colonne **Niveau** pour trier les événements en fonction des catégories (Urgence, Alarme, Critique, Erreur, Avertissement, Information, Note).



Pour sélectionner un événement à enregistrer, double-cliquez dessus ou sélectionnez-le et cliquez sur le symbole approprié dans la *barre d'outils*.

- Active-le ou les événements sélectionnés pour la journalisation.
- Désactive-le ou les événements sélectionnés pour la journalisation.

Vous pouvez sélectionner plusieurs événements en même temps (clic + Maj ou Ctrl).

Une fois les événements sélectionnés, cliquez sur l'icône de disquette dans la barre d'outils pour enregistrer les paramètres. Cependant, dans chaque cas, il vous sera demandé si vous souhaitez enregistrer les paramètres ou non lorsque vous quittez cette vue sans enregistrer.

3.20.3 Affichage et exportation des entrées

Remarque : Pour afficher et exporter des entrées, un responsable de la sécurité doit disposer de l'autorisation globale **Lire les entrées du journal**.

Un responsable de la sécurité disposant de l'autorisation globale **Lire les entrées du journal** peut afficher les entrées et les exporter vers 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 dans la barre d'outils.


Cette action ouvre la boîte de dialogue qui vous permet d'afficher et d'exporter les entrées enregistrées.

Cette boîte de dialogue affiche tous les événements qui ont été sélectionnés pour la journalisation.

Cliquez sur les en-têtes de colonnes pour trier les entrées.

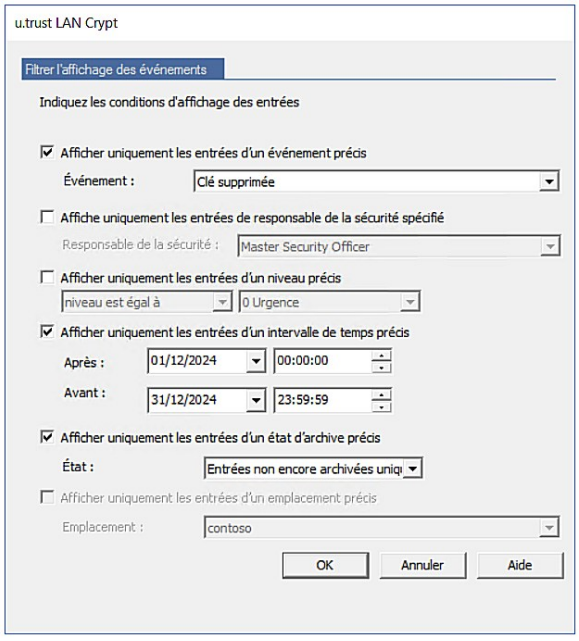
Double-cliquez sur une entrée pour en afficher les détails.

u.trust LAN Crypt dispose également d'un filtre qui vous permet de spécifier des conditions pour les entrées affichées.

3.20.4 Filtrage des événements

Les paramètres de journalisation peuvent être définis dans le nœud **Journalisation**. Une fonction de filtrage est disponible pour l'affichage et l'exportation des événements enregistrés. Si le nœud **Journalisation** est sélectionné, cela peut être défini par le biais du menu contextuel (bouton droit de la souris) ou du menu **Action**, via **Afficher et exporter les entrées**.

Cliquer sur **Afficher et exporter les entrées** dans le nœud **Journalisation** ouvre une boîte de dialogue qui vous permet de spécifier un filtre pour les événements affichés.



Vous pouvez filtrer les événements à l'aide des conditions suivantes :

- **Afficher uniquement les entrées d'un événement précis**

  Si vous sélectionnez cette option, seules les entrées de l'événement que vous avez sélectionné dans la liste déroulante s'affichent. La liste comporte tous les événements qui peuvent être enregistrés (par exemple « *Clé supprimée* », « *Règle modifiée* », etc.).

- **Afficher uniquement les entrées de responsable de la sécurité spécifié**

  Sélectionner cette option vous permet de sélectionner un responsable de la sécurité dans la liste déroulante. Seuls les événements enregistrés lorsque le responsable de la sécurité spécifié était connecté s'affichent alors. La liste déroulante répertorie uniquement les responsables de la sécurité pour lesquels des entrées existent.

- **Afficher uniquement les entrées d'un niveau précis**

  Sélectionner cette option vous permet de sélectionner un niveau particulier ou une gamme de niveaux pour lesquels les entrées doivent être affichées. *Niveau inférieur ou égal à* et *Niveau supérieur ou égal à* font référence aux nombres antérieurs au niveau.

- **Afficher uniquement les entrées d'un intervalle de temps précis**

  Sélectionner cette option vous permet de définir une période durant laquelle les entrées ont été enregistrées.

- **Afficher uniquement les entrées d'un état d'archive précis**

  Si vous sélectionnez cette option, vous pouvez spécifier si les *Entrées archivées uniquement* ou les *Entrées non encore archivées uniquement* doivent s'afficher (les entrées qui ont déjà été archivées restent dans la base de données jusqu'à ce qu'elles soient supprimées). Si cette option n'est pas sélectionnée, les deux types d'entrées s'affichent.

- **Afficher uniquement les entrées d'un emplacement spécifié**

  Sélectionnez cette option pour spécifier un emplacement à partir duquel les entrées doivent être affichées. Si vous utilisez une base de données distribuée, plusieurs emplacements peuvent être impliqués. La manière dont la base de données est répliquée détermine quels emplacements peuvent être affichés.

Remarque : Même après avoir exécuté la fonction **Afficher et exporter les Entrées**, le filtre peut être défini en cliquant sur le bouton **Filtrer** dans la boîte de dialogue **Afficher les événements**. Alternativement, cette fonction est également disponible via le menu **Affichage** et après avoir sélectionné **Filtre**.

3.20.5 Archivage, suppression, vérification des entrées

Remarque : Un responsable de la sécurité a besoin de l'autorisation globale **Gérer la journalisation** avant de pouvoir archiver, supprimer et vérifier les entrées. Si le responsable de la sécurité obtient ce droit, l'autorisation global **Lire le protocole** lui est automatiquement accordé.

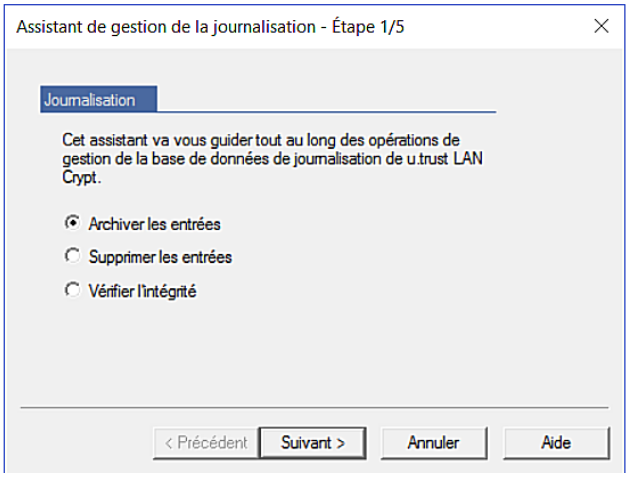
Un responsable de la sécurité disposant de l'autorisation globale **Gérer la journalisation** peut archiver, supprimer et vérifier les entrées enregistrées.

Cliquez sur **Archiver, supprimer et vérifier les entrées** dans le menu contextuel du nœud **Journalisation** ou cliquez sur le symbole dans la barre des tâches pour lancer un assistant qui effectuera ces tâches.

Lancez l'assistant pour archiver, supprimer et vérifier les entrées enregistrées.

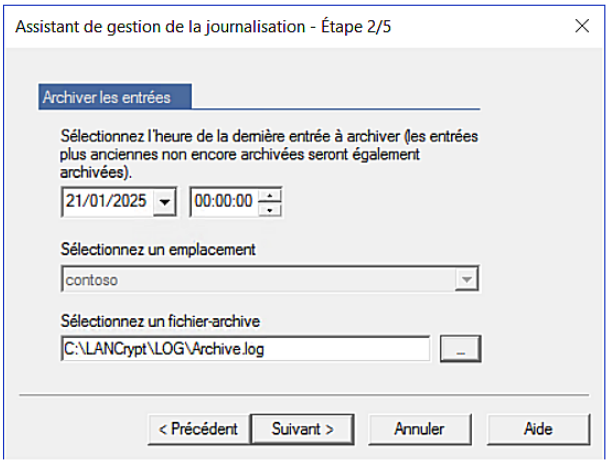
Archivage des entrées

Pour archiver les entrées, sélectionnez **Archiver les entrées** et cliquez sur **Suivant**.



Dans la boîte de dialogue suivante, saisissez :

- La date et l'heure de la dernière entrée à archiver. Toutes les entrées antérieures à cette date qui n'ont pas encore été archivées seront également archivées. En outre, à ce stade, vous pouvez également archiver par emplacement (si l'option est disponible).



Remarque : Vous ne pouvez sélectionner des emplacements différents que si vous travaillez avec une base de données distribuée. Les emplacements qui peuvent être sélectionnés à ce stade dépendent de la manière dont la base de données est répliquée. Un seul emplacement est indiqué dans le graphique ci-dessus. L'emplacement correspond toujours à l'entrée que vous avez définie lors de l'installation d'*u.trust LAN Crypt*. Cette entrée ne pourra pas être modifiée par la suite.

- Le nom du fichier dans lequel les entrées doivent être écrites.

Cliquez sur **Suivant**. Dans la boîte de dialogue suivante, vous pouvez voir le nombre d'entrées qui ont été 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 qui ont déjà été archivées restent dans la base de données et peuvent être supprimées. Leur état est défini sur *Archivé*.

Suppression des entrées

Pour supprimer des entrées archivées, sélectionnez *Supprimer les entrées archivées* et cliquez sur **Suivant**.

Remarque : Les entrées qui n'ont pas encore été archivées ne peuvent pas être supprimées.

Dans la boîte de dialogue suivante, spécifiez :

- La date et l'heure de la dernière entrée à partir de laquelle la suppression doit avoir lieu. Toutes les entrées de journal antérieures à ce moment (même si elles n'ont pas encore été archivées) seront supprimées.

  Remarque : La dernière heure possible dépend de l'âge minimum spécifié des entrées de journal, que vous pouvez définir dans l'onglet **Paramètres** du nœud **Journalisation**.

- L'emplacement (si disponible) à partir duquel les entrées doivent être supprimées.

Cliquez sur **Suivant**. Dans la boîte de dialogue suivante, vous pouvez voir le nombre d'entrées qui ont été 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 enregistrés, sélectionnez *Vérifier l'intégrité de l'archive* et cliquez sur **Suivant**.

Dans la boîte de dialogue suivante, sélectionnez les données à vérifier. Vous pouvez sélectionner les entrées dans la base de données ou les entrées archivées à vérifier.

Pour vérifier les entrées dans une base de données distribuée, sélectionnez l'emplacement des entrées à vérifier.

Si vous souhaitez consulter une archive, sélectionnez un fichier en cliquant sur le bouton **Parcourir** (« **…** »).

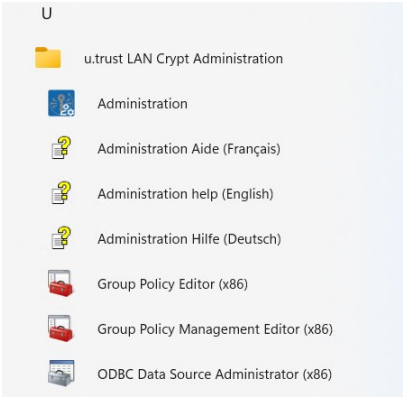
Cliquez sur **Suivant**. Dans la boîte de dialogue suivante, vous pouvez voir le nombre d'entrées qui ont été sélectionnées.

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, l'avertissement correspondant s'affiche.

Cliquez sur **Terminer** pour fermer l'assistant.

4 Configuration d'u.trust LAN Crypt

Remarque : Les paramètres de configuration doivent être définis avec l'Éditeur de stratégie de groupe 32 bits (*GPME.msc*) ou l'Éditeur de stratégie de groupe local 32 bits (*GPEdit.msc*). Les deux éditeurs sont liés dans le menu Démarrer de Windows sous le dossier **u.trust LAN Crypt Administration**.



Cela garantit que la bonne version est démarrée.

Remarque : Si vous souhaitez configurer la stratégie de groupe *u.trust LAN Crypt* pour un contrôleur de domaine sur un ordinateur Windows 11 à l'aide d'un composant logiciel enfichable en tant qu'administrateur, vous devez installer les fichiers de modèle d'administration de *u.trust LAN Crypt* (voir, entre autres, la note sur cette page). Sur un système Windows Server pris en charge, vous pouvez également utiliser la console d'administration des stratégies de groupe 32 bits (GPME.msc) en tant qu'administrateur.

Les paramètres suivants sont spécifiques à l'ordinateur ou à l'utilisateur. Pour modifier ces paramètres, vous avez besoin de droits d'administrateur dans le domaine ou dans Active Directory. Ces réglages doivent être uniquement effectués par un administrateur système.

Vous sélectionnez les paramètres de configuration dans le nœud **Configuration de u.trust *LAN Crypt***. Ce nœud s'affiche lorsque vous travaillez avec des stratégies système dans chaque ordinateur et nœud utilisateur de la console de gestion. Dans l'environnement Active Directory, le nœud **Configuration de u.trust *LAN Crypt*** apparaît dans les GPO *Configuration ordinateur* ou *Configuration utilisateur* (*Paramètres Windows / u.trust LAN Crypt*).

Remarque : Vous pouvez également utiliser le modèle d'administration (**.admx* et **.adml*) fourni dans le dossier « \Config » de votre package d'installation décompressé. Les fichiers ADMX doivent être copiés dans le dossier « `C:\Windows\PolicyDefinitions` » ou, si c'est possible, dans le magasin central. Les fichiers de langue respectifs (*.ADML), en revanche, doivent être copiés dans le sous-dossier de langue correspondant (par exemple « `fr-FR` »). Ils sont lus directement lors de la prochaine ouverture de l'éditeur de stratégie de groupe et leur syntaxe est vérifiée. Pour plus d'informations concernant les fichiers de modèles d'administration, veuillez consulter la documentation suivante :

`https://learn.microsoft.com/fr-fr/troubleshoot/windows-client/group-policy/create-and-manage-central-store`

En général, les paramètres de configuration sont destinés aux machines. Cependant, vous pouvez définir des paramètres spécifiques à l'utilisateur pour attribuer des droits spécifiques aux utilisateurs sélectionnés. Si un paramètre spécifique à l'utilisateur est créé, celui-ci **annule** un paramètre spécifique à la machine.

Si vous souhaitez annuler un paramètre spécifique à l'utilisateur afin qu'un paramètre spécifique à la machine s'applique, vous devez définir l'état de ce paramètre sur **Non configuré**. Pour ce faire, sélectionnez un paramètre et appuyez sur la touche **Suppr**. Dans la console de gestion, **non** apparaît alors sous la colonne *Configuré*.

4.1 Paramètres client

Si le nœud **Paramètres client** est sélectionné, les paramètres configurables s'affichent dans le volet de droite de la console. Double-cliquez sur une entrée pour ouvrir une boîte de dialogue dans laquelle vous pouvez définir les paramètres dont vous avez besoin.

4.1.1 Autoriser le chiffrement/déchiffrement

Tout utilisateur d'*u.trust LAN Crypt* peut chiffrer ou déchiffrer des fichiers en sélectionnant un élément dans le menu contextuel de ces fichiers. Cela signifie que les utilisateurs peuvent même chiffrer des fichiers pour lesquels aucune règle n'a été définie.

Pour empêcher cela, vous pouvez spécifier ici que cette option ne s'affiche pas dans le menu contextuel de ces fichiers.

Autoriser le chiffrement/déchiffrement : non

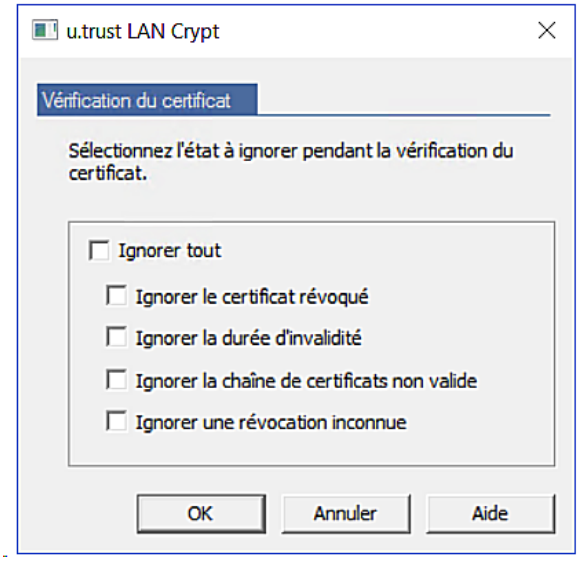
Empêche les fichiers pour lesquels aucune règle de chiffrement n'a été définie d'être chiffrés ou déchiffrés via leur menu contextuel.

4.1.2 Ignorer pendant la vérification du certificat

u.trust LAN Crypt vous permet de spécifier si des erreurs détectées lors de la vérification des certificats utilisateur doivent être ignorées.

Cette procédure est utile si la période de validité d'un certificat a expiré et qu'aucun nouveau certificat n'est encore disponible. Pour s'assurer qu'un utilisateur peut continuer à accéder à son profil de chiffrement, la période de vérification de validité peut être ignorée jusqu'à l'émission d'un nouveau certificat.

Par conséquent, le même certificat, qui a effectivement expiré, peut toujours être utilisé. Lorsqu'un nouveau certificat est disponible, vous pouvez à nouveau annuler **Ignorer la durée d'invalidité**.



Remarque : Ignorer les erreurs qui se produisent lors de la vérification des certificats implique toujours une réduction de la sécurité.

- **Ignorer le certificat révoqué**

  Si un certificat se trouve dans une **L**iste de **R**évocation de **C**ertificats évaluée lors de la connexion, il peut ne pas être utilisé pour la connexion. Néanmoins, un utilisateur peut continuer à accéder à son profil de chiffrement même si cette option est sélectionnée.

- **Ignorer la durée d'invalidité**

  Si cette option est sélectionnée, l'utilisateur peut continuer à accéder à son profil de chiffrement même si la période de validité d'un certificat a expiré.

- **Ignorer la chaîne de certificats non valide**

  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 l'ordinateur client ou est conservée dans le mauvais magasin de certificats.

- **Ignorer une révocation inconnue**

  Lorsque les PKI de certains fournisseurs écrivent les raisons de la révocation d'un certificat à une liste de révocation de certificats, elles ne sont pas conformes aux normes communes. En général, vous ne pouvez pas utiliser de certificat si la raison de la révocation n'est pas connue. Cependant, si cette option est sélectionnée, l'utilisateur peut continuer à accéder à son profil de chiffrement.

Remarque : Veuillez noter qu'ignorer les erreurs détectées lors de la vérification des certificats utilisateur implique généralement une compromission de la stratégie de sécurité de l'entreprise. Conformément à la norme RFC 5280, le client *u.trust LAN Crypt* ne reconnaît pas les statuts de révocation inconnus. Par conséquent, donnez une autre raison à la révocation d'un certificat.

Ces paramètres peuvent également être définis sous Paramètres du serveur. La vérification des certificats est effectuée lorsqu'un responsable de la sécurité se connecte à la console d'administration d'*u.trust LAN Crypt* et lorsqu'une autorisation supplémentaire est exécutée.

4.1.3 Résoudre toutes les variables d'environnement

u.trust LAN Crypt résout la variable d'environnement *%USERNAME%* pour les chemins (à l'exception des chemins d'accès dans les règles de bypass).

Ici, vous pouvez spécifier si d'autres variables d'environnement doivent être résolues dans les chemins.

Cependant, l'utilisation d'autres variables d'environnement dans les chemins peut créer des problèmes si les utilisateurs sont en mesure de les modifier. Cela peut entraîner un dysfonctionnement des données de chemin dans le profil de chiffrement. En outre, les variables d'environnement peuvent affecter différents chemins en fonction de la version de Windows utilisée.

4.1.4 Entrées de menu activées

Ici, vous pouvez indiquer les options de menu à afficher dans le menu utilisateur de *u.trust LAN Crypt* sur un ordinateur client. Par défaut, toutes les options de menu s'affichent. Si vous supprimez une option de menu à cet emplacement, elle n'apparaît pas sur l'ordinateur client. Cela signifie également que cette fonctionnalité n'est pas disponible sur ce client. Cela vous permet, par exemple, d'empêcher la désactivation du chiffrement sur un ordinateur client.

4.1.5 Règles Ignorer par défaut

Le pilote *u.trust LAN Crypt* étant toujours chargé au démarrage d'un poste de travail, la vérification du chiffrement de tous les fichiers est déjà faite. Cela inclut donc également la vérification des droits d'accès appropriés, même si aucun profil de chiffrement spécifique à l'utilisateur n'a encore été chargé. Cela peut ralentir les performances dans cette phase.

Cependant, en définissant un paramètre spécifique à la machine dans la configuration d'*u.trust LAN Crypt*, il est possible de configurer le pilote *u.trust LAN Crypt* afin qu'il ignore des lecteurs ou dossiers spécifiques jusqu'au chargement complet du profil de chiffrement de l'utilisateur.

Double-cliquez sur **Règles Ignorer par défaut** dans les paramètres client pour ouvrir une boîte de dialogue. Celle-ci vous permet de spécifier les répertoires que le pilote *u.trust LAN Crypt* doit ignorer (par exemple « c:*.*;d:*.* »).

Si vous saisissez plusieurs chemins, séparez chacun d'eux par un point-virgule.

Cependant, si vous utilisez cette règle, vous devez garder en tête que le contrôle d'accès spécifique à *u.trust LAN Crypt* n'est effectué que lorsque le profil de chiffrement de l'utilisateur est chargé.

Exemple :

Si vous saisissez « `c:\*.*;d:\*.*` » comme **Règles Ignorer par défaut**, le pilote ignorera tous les dossiers des lecteurs **C** et **D** jusqu'à ce que le profil de chiffrement de l'utilisateur soit chargé.

Même si vous utilisez *u.trust LAN Crypt* sur un serveur Terminal Server, vous pouvez accélérer les performances en utilisant le paramètre **Règles Ignorer par défaut**. Si, par exemple, plusieurs utilisateurs travaillent sur le même serveur Terminal Server, mais qu'un seul d'entre eux utilise *u.trust LAN Crypt*, vous pouvez demander au pilote d'ignorer les sessions de tous les autres utilisateurs. Aucun profil de chiffrement n'ayant été chargé pour eux, seules les **Règles Ignorer par défaut** s'appliquent.

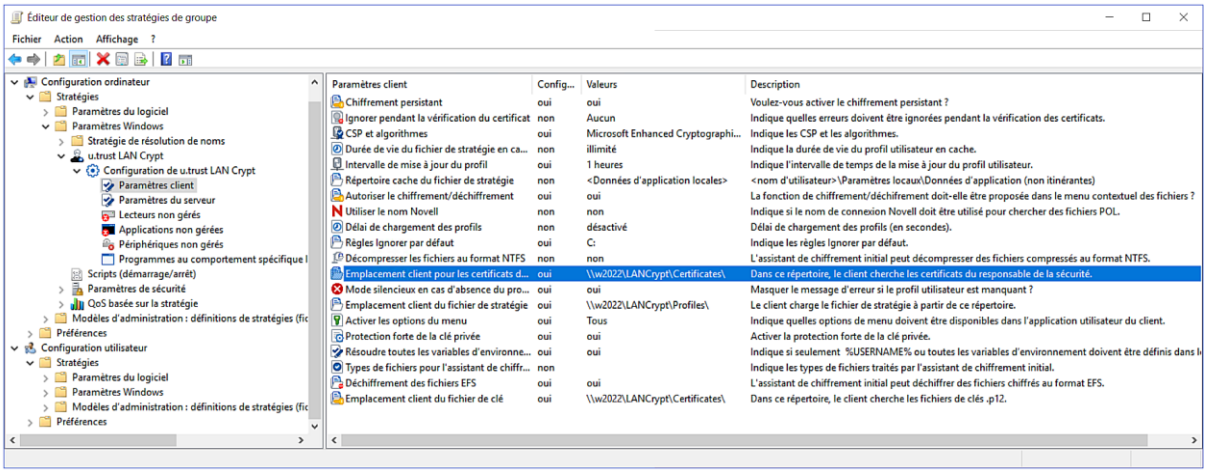
Remarque : Veuillez noter que les entrées que vous définissez ici incluent également tous les sous-dossiers.

Remarque : Par ailleurs, lors d'une nouvelle installation d'*u.trust LAN Crypt* (cela ne concerne pas les mises à jour), la « **Règle Ignorer par défaut** » est prédéfinie avec la valeur « * ». En conséquence, la protection d'accès spécifique à *u.trust LAN Crypt* est inactive pour tous les chemins et fichiers, et ce, jusqu'au chargement du profil de l'utilisateur. Les utilisateurs peuvent supprimer des fichiers chiffrés pendant cette période ou lorsqu'ils ont déchargé leur profil. Cela est vrai même s'ils n'ont pas de clé pour les fichiers qui y sont stockés.

Vous pouvez modifier cela en définissant un chemin pour la « **Règle Ignorer par défaut** » (par exemple « C:\Programmes*.* »).

4.1.6 Emplacement client pour les certificats des responsables de la sécurité

Pour indiquer l'emplacement de stockage, sélectionnez **Paramètres client** et, dans le volet de droite de la console, double-cliquez sur **Emplacement client pour les certificats des responsables de la sécurité**.



Une fois le chemin d'accès spécifié, *u.trust LAN Crypt* tente automatiquement d'importer le certificat du responsable de la sécurité à partir de ce répertoire si le certificat du fichier de

stratégie utilisateur correspondant n'est pas présent. En conséquence, il importe tous (!) les fichiers **.cer* du répertoire que vous avez spécifié.

4.1.7 Emplacement client du fichier de clé

Pour indiquer l'emplacement de stockage, sélectionnez **Paramètres client** et, dans le volet de droite de la console, double-cliquez sur **Emplacement client du fichier de clé**.

Une fois le chemin d'accès spécifié, *u.trust LAN Crypt* tente automatiquement d'importer un fichier de clé **.p12* pour l'utilisateur si la clé privée du fichier de stratégie n'est pas présente. Ce fichier doit être nommé « `nomdeconnexion.p12` » afin que le système puisse reconnaître son appartenance à un utilisateur particulier.

Les deux chemins décrits ci-dessus ne sont pas des paramètres par défaut. Cela signifie que la partie publique des certificats des responsables de la sécurité ou des certificats utilisateur ne se charge pas automatiquement tant que l'administrateur système ne spécifie pas les chemins.

L'administration d'*u.trust LAN Crypt* stocke les fichiers **.p12* des utilisateurs et la partie publique des certificats des responsables de la sécurité dans le même dossier. Cependant, du point de vue du client, ces chemins peuvent être configurés séparément de sorte que l'une ou l'autre de ces fonctions peut être désactivée si nécessaire. Malgré cela, ces chemins sont généralement les mêmes. Si vous souhaitez que les certificats des responsables de la sécurité et les certificats utilisateur soient chargés automatiquement à partir de différents dossiers, vous devez les copier manuellement dans les dossiers pertinents.

4.1.8 Emplacement client du fichier de stratégie

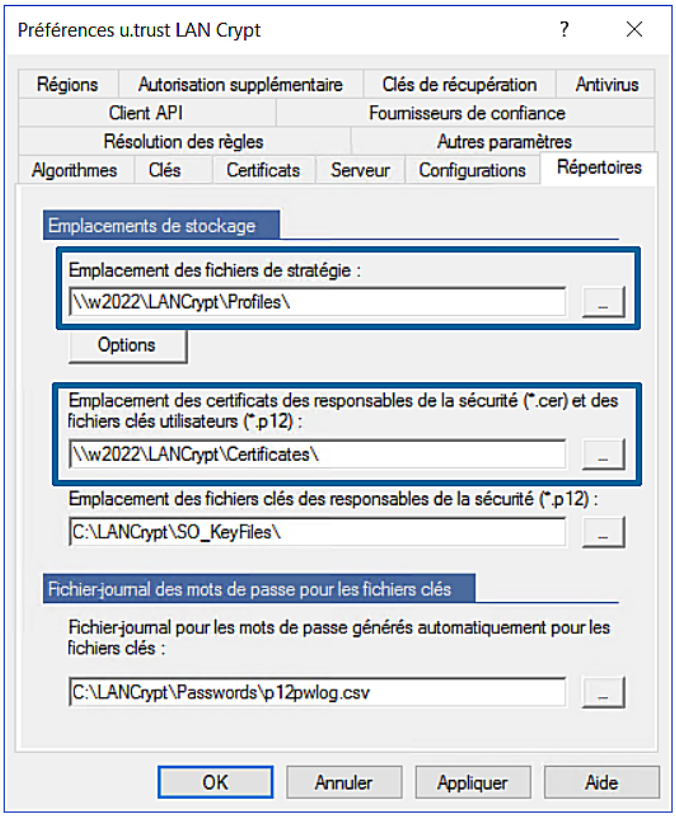
Pour indiquer l'emplacement de stockage, sélectionnez **Paramètres client** et, dans le volet de droite de la console, double-cliquez sur **Emplacement client du fichier de stratégie**.

Entrez le chemin d'accès correspondant à l'emplacement du fichier de stratégie spécifique à l'utilisateur. Pour s'assurer que les clients peuvent accéder à leurs fichiers de stratégie (par exemple, sur un lecteur réseau partagé), le chemin doit être entré du point de vue des clients.

Il s'agit généralement du dossier dans lequel ils ont été générés par le responsable de la sécurité via la console d'administration d'*u.trust LAN Crypt*. Vous devez suivre les règles de capitalisation UNC (**U**niversal **N**aming **C**onvention), car aucun lecteur de disque n'est associé à ces fichiers à ce stade !

Dans ce paramètre, vous pouvez utiliser la variable d'environnement *%LOGONSERVER%* (pour l'équilibrage de charge, etc.).

Les chemins saisis dans la stratégie de groupe pour les certificats des responsables de la sécurité, les fichiers de clé et les fichiers de stratégie doivent correspondre aux chemins définis dans la console d'administration d'*u.trust LAN Crypt*, au niveau du nœud **Paramètres centraux**, dans l'onglet **Répertoires**.



4.1.9 Répertoire cache du fichier de stratégie

Pour indiquer l'emplacement de stockage du cache, sélectionnez **Paramètres client** et, dans le volet de droite de la console, double-cliquez 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 avoir l'autorisation d'écrire des données dans ce répertoire local. Cela garantit que le profil de chiffrement d'un utilisateur est disponible même s'il n'y a pas de connexion à un réseau.

Vous pouvez soit utiliser l'un des emplacements de stockage indiqués dans la liste, soit sélectionner <autre> et saisir un autre emplacement dans le champ de saisie.

Remarque : Les emplacements de stockage suggérés sont des dossiers Windows standard qui dépendent du système d'exploitation utilisé. <*Données d'application locales*> fait toujours référence à un dossier sur la machine locale, tandis que tous les autres (par exemple, les utilisateurs itinérants) peuvent également être situés sur des lecteurs réseau.

Si un emplacement de stockage est spécifié manuellement, il faut s'assurer que ce dossier existe également sur les ordinateurs clients.

Remarque : Si vous souhaitez supprimer un utilisateur de votre environnement *u.trust LAN Crypt*, vous devez savoir que la copie locale reste enregistrée sur l'ordinateur. Tant que c'est le cas, l'utilisateur peut accéder aux données avec les droits qu'elles contiennent. Pour éviter cela, vous devez créer un fichier de stratégie vide pour cet utilisateur. Pour ce faire, supprimez le fichier de stratégie et l'utilisateur de tous les groupes (voir « *Effacement des profils* » à la page 178).

4.1.10 Délai de chargement des profils

Ici, vous pouvez spécifier une période (en secondes) qui s'écoulera avant que le profil utilisateur ne soit chargé. Ce délai est important si, par exemple, un certificat sur jeton est utilisé. Le délai de chargement du profil garantit que le jeton est accessible lorsque le certificat est requis. Valeur par défaut : 20 secondes.

4.1.11 Types de fichiers pour l'assistant de chiffrement initial

Si vous définissez des types de fichiers spécifiques ici, seuls les fichiers du type spécifié seront traités par l'assistant de chiffrement initial. L'utilisateur ne peut pas modifier ce paramètre dans l'assistant de chiffrement initial !

Ce paramètre n'affecte que les fichiers pour lesquels une règle de chiffrement existe.

Si un dossier contient également d'autres fichiers d'un type de fichier spécifié ici, ils ne seront pas inclus dans le chiffrement initial. Ils ne seront chiffrés que lorsque l'utilisateur les ouvrira et les enregistrera à nouveau.

Si vous avez l'intention de laisser l'utilisateur définir ce paramètre lui-même dans l'assistant de chiffrement initial, définissez le paramètre sur non configuré.

Si vous avez spécifié des types de fichiers ici et que vous avez l'intention de laisser l'utilisateur faire une sélection plus tard, définissez le paramètre sur **Non configuré** à nouveau.

Remarque : Ce paramètre ne s'applique qu'à l'assistant de chiffrement initial. Si le chiffrement est démarré via l'extension Explorateur « *Chiffrement selon le profil* », le paramètre n'a aucun effet.

Spécifiez les types de fichiers dans une liste séparée par des points-virgules.

Exemple : `docx ; xlsx ; pdf ; txt`

4.1.12 Durée de vie de la stratégie en cache

Comportement standard d'u.trust LAN Crypt

Lorsqu'un utilisateur se connecte à Windows, son profil mis en cache sera chargé en premier. *u.trust LAN Crypt* vérifie ensuite si un nouveau fichier de stratégie est disponible pour l'utilisateur en établissant une connexion à l'emplacement spécifié du fichier de stratégie (lecteur réseau). Si un nouveau fichier de stratégie est trouvé à cet emplacement, le profil utilisateur mis en cache est mis à jour.

L'avantage de cette approche est que l'utilisateur peut commencer à travailler avec des fichiers chiffrés tandis qu'*u.trust LAN Crypt* vérifie si une nouvelle version du fichier de stratégie existe.

Si le lecteur réseau n'est pas accessible, l'utilisateur travaille avec le profil utilisateur mis en cache jusqu'à ce qu'il puisse être mis à jour.

Si cette option est définie sur **Non configuré**, le comportement d'*u.trust LAN Crypt* est conforme à la description.

En utilisant ce paramètre, vous pouvez modifier le comportement standard.

Remarque : Vous pouvez définir une option sur **Non configuré** en la sélectionnant et en cliquant sur **Supprimer** dans son menu contextuel (clic droit). Dans la colonne *Configuré*, **non** apparaît en regard de l'option correspondante.

Ici, vous pouvez spécifier la durée de validité de la stratégie en cache sur les ordinateurs clients.

Durant la période définie ici, le fichier de stratégie est valide sur le client et l'utilisateur peut accéder aux données chiffrées, et ce, même s'il n'y a pas de connexion à l'emplacement du fichier sur le partage de stratégie.

La période pendant laquelle les fichiers de stratégie sont mis en cache et sont donc valides peut être définie en jours ou en semaines.

Lorsque la période spécifiée expire, *u.trust LAN Crypt* tente de charger le fichier de stratégie à partir du lecteur réseau pour le mettre à jour à nouveau. Si cela n'est pas possible, le fichier de stratégie sera déchargé. L'utilisateur ne peut alors plus accéder aux données chiffrées. Le fichier de stratégie ne sera mis à jour et chargé à nouveau que lorsqu'un fichier de stratégie valide sera disponible (par exemple lors de la prochaine connexion avec une connexion à l'emplacement client pour les fichiers de stratégie). L'utilisateur peut ainsi à nouveau accéder aux données chiffrées. Le compteur relatif à la durée du stockage en cache est réinitialisé.

En spécifiant la durée de stockage du cache, vous pouvez d'une part vous assurer que les ordinateurs clients reçoivent des fichiers de stratégie à jour, à intervalles réguliers et que les utilisateurs utilisent des stratégies à jour, à tout moment. D'autre part, vous pouvez empêcher les utilisateurs de travailler avec les mêmes fichiers de stratégie pendant une période de temps illimitée, car un utilisateur peut continuer à travailler avec une version en cache du fichier de stratégie pendant une période de temps illimitée, si cette option est définie sur **Non configuré**.

Le compteur relatif à la durée de stockage en cache autorisée est réinitialisé dans les situations suivantes :

- L'emplacement de stockage des fichiers de stratégie est accessible et un fichier de stratégie valide a été transféré au client (par exemple lorsque l'utilisateur se connecte ou à la suite d'un intervalle de mise à jour spécifié). Cependant, le fichier de stratégie n'est pas nouveau par rapport au fichier existant.
- Un nouveau fichier de stratégie est disponible et a été chargé avec succès.

Le compteur pour la durée de stockage du cache autorisée **NE SERA PAS** réinitialisé dans les situations suivantes :

- 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, il n'a pas pu être chargé en raison d'une erreur.
- Un nouveau fichier de stratégie est disponible. Cependant, il nécessite un nouveau certificat. L'utilisateur n'a pas ce certificat ou n'est pas en mesure de le charger.

Si la mise à jour du fichier de stratégie échoue, l'heure d'expiration du fichier de stratégie mis en cache sera affichée 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 d'*u.trust LAN Crypt*. Une mise à jour automatique sera également effectuée en fonction des paramètres d'intervalle de mise à jour pour le profil utilisateur.

Les fichiers de stratégie ne sont pas mis en cache.

Si cette option est définie sur « 0 », le fichier de stratégie ne sera pas mis en cache. Cela signifie que les utilisateurs reçoivent leurs profils utilisateur lors de la connexion, si l'emplacement du fichier de stratégie est accessible. S'il n'est pas accessible ou si une erreur se produit lors du chargement du profil, l'utilisateur ne peut pas accéder aux fichiers chiffrés.

4.1.13 Décompresser les fichiers au format NTFS

Ce paramètre permet à l'assistant de chiffrement initial de traiter les fichiers compressés au format NTFS. Si vous définissez l'option **Décompresser les fichiers au format NTFS** sur **Oui**, l'assistant décompresse les fichiers compressés au format NTFS et les chiffre, si cela s'applique.

Si vous définissez l'option **Décompresser les fichiers au format NTFS** sur **Non**, l'assistant de chiffrement initial ignorera les fichiers compressés au format NTFS. Ils ne seront donc pas chiffrés, même si une règle de chiffrement a été spécifiée pour eux.

Après avoir configuré cette option, les utilisateurs ne peuvent pas la modifier dans l'assistant de chiffrement initial ! Les utilisateurs ne peuvent configurer cette option eux-mêmes dans l'assistant de chiffrement initial que s'il a été défini sur non configurer ici.

Remarque : Lorsque vous compressez des fichiers au format NTFS qui ont déjà été chiffrés par *u.trust LAN Crypt*, ces fichiers ne peuvent plus être déchiffrés par *u.trust LAN Crypt*. Un message d'erreur s'affiche lorsque vous tentez de déchiffrer ces fichiers. Les fichiers que vous souhaitez compresser au format NTFS ne doivent pas avoir été préalablement chiffrés avec *u.trust LAN Crypt*.

4.1.14 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 et les chiffre à nouveau si une règle de chiffrement *u.trust LAN Crypt* s'applique.

Si vous définissez l'option **Déchiffrement des fichiers EFS** sur **Non**, l'assistant de chiffrement initial ignorera les fichiers EFS chiffrés. Ils ne seront donc pas chiffrés à nouveau par *u.trust LAN Crypt*, même si une règle de chiffrement a été spécifiée pour eux.

Après avoir configuré cette option, les utilisateurs ne peuvent pas la modifier dans l'assistant de chiffrement initial ! Les utilisateurs ne peuvent configurer cette option eux-mêmes dans l'assistant de chiffrement initial que s'il a été défini sur non configurer ici.

Remarque : Vous pouvez définir une option sur **Non configuré** en la sélectionnant et en cliquant sur Supprimer dans son menu contextuel (clic droit). Dans la colonne *Configuré*, **Non** sera affiché en plus de l'option correspondante.

4.1.15 Intervalle de mise à jour du profil

Ce paramètre définit la fréquence à laquelle *u.trust LAN Crypt* vérifie les nouveaux fichiers de stratégie et les met à jour si nécessaire.

Pour mettre à jour les fichiers de stratégie, *u.trust LAN Crypt* a besoin d'accéder au lecteur réseau sur lequel les fichiers de stratégie sont stockés. *u.trust LAN Crypt* vérifie si une nouvelle version du fichier de stratégie existe sur le lecteur réseau et met à jour le fichier de stratégie sur l'ordinateur client si nécessaire.

u.trust LAN Crypt effectue automatiquement toutes les étapes nécessaires au chargement réussi du profil utilisateur (avec si nécessaire la recherche de nouveaux certificats, la vérification des nouveaux certificats, etc.). Le remplacement de l'ancien profil par le nouveau profil, ainsi que le chargement du nouveau profil, ne sont effectués que si aucune erreur ne se produit pendant le processus. Par la suite, le compteur relatif à la durée du stockage en cache est réinitialisé. Si les fichiers de stratégie sont identiques, le compteur est également réinitialisé.

L'intervalle de mise à jour peut être spécifié en minutes, heures, jours et semaines.

Remarque : *u.trust LAN Crypt* n'autorise pas les intervalles de mise à jour inférieurs à 15 minutes. Si cette option est définie sur **Non configuré**, les fichiers de stratégie ne sont pas mis à jour automatiquement.

4.1.16 Mode silencieux en cas d'absence du profil utilisateur

Si le paramètre par défaut s'applique, *u.trust LAN Crypt* affiche un message d'erreur si le système ne trouve pas de profil utilisateur.

Ici, vous pouvez indiquer que ce message d'erreur doit être supprimé si aucun profil utilisateur n'est trouvé.

Si vous définissez **Masquer le message d'erreur** sur **Oui**, le message d'erreur ne s'affiche pas.

Remarque : Ce paramètre peut être particulièrement utile dans les environnements de serveurs Terminal Server, si tous les utilisateurs ne doivent pas travailler avec *u.trust LAN Crypt*.

4.1.17 Chiffrement persistant

Les fichiers ne restent généralement chiffrés que tant qu'ils sont soumis à une règle de chiffrement. Par exemple, si un utilisateur copie un fichier chiffré dans un dossier pour lequel aucune règle de chiffrement n'a été définie, le fichier est déchiffré dans le dossier cible. Si vous définissez le **chiffrement persistant** sur **oui**, vous pouvez garantir que les fichiers restent chiffrés, même lorsqu'ils sont déplacés ou copiés.

Pour désactiver cette fonction, double-cliquez sur **Chiffrement persistant** et sélectionnez **non** dans le champ de liste **Activer le chiffrement persistant**.

4.1.18 Protection forte de la clé privée

Ici, vous pouvez spécifier que l'utilisateur est invité à s'authentifier chaque fois que la clé privée est utilisée par *u.trust LAN Crypt*. Si vous activez ce paramètre, il s'applique également au responsable de la sécurité (voir « *Activer la protection forte de la clé privée* » sous « *Paramètres d'administration u.trust LAN Crypt* » à la page 200).

Remarque : Cette politique n'a aucun effet sur les certificats importés précédemment ou manuellement. L'activation de ce paramètre ne s'appliquera qu'aux certificats importés ultérieurement via *u.trust LAN Crypt*.

4.1.19 Générateur de nombres aléatoires

Pour la génération sécurisée de clés, *u.trust LAN Crypt* utilise un générateur de nombres aléatoires intégré. Vous pouvez définir ici l'algorithme que le générateur de nombres aléatoires doit utiliser. Le choix a une influence sur la sécurité des clés générées. « *BasicRandom* » offre de bonnes performances avec une sécurité modérée et convient aux systèmes disposant de ressources limitées. Il est pris en charge par toutes les versions précédentes de *LAN Crypt*. « *AdvancedRandom* » offre un équilibre entre bonne entropie et performance. « *SuperRandom* », en revanche, fournit une entropie nettement plus élevée et est recommandé pour les environnements auxquels s'appliquent des exigences de sécurité particulièrement élevées.

Remarque : Le nouvel algorithme « *SuperRandom* » n'est pris en charge qu'à partir de la version 13.0.0 de *u.trust LAN Crypt*.

Sélectionnez un algorithme pour le générateur de nombres aléatoires dans la zone de liste :

- BasicRandom
- AdvancedRandom
- SuperRandom

Si vous définissez le paramètre du générateur de nombres aléatoires sur **Non configuré**, *u.trust LAN Crypt* utilise « *SuperRandom* » par défaut.

Remarque : Vous pouvez définir l'algorithme du générateur de nombres aléatoires dans les paramètres du client et du serveur (voir « *Générateur de nombres aléatoires* » dans la section « *Paramètres du serveur* » à la page 202). Cependant, seul le même algorithme peut être utilisé dans les deux paramètres. Si vous modifiez l'algorithme du générateur de nombres aléatoires dans l'un des deux paramètres, la modification sera également appliquée à l'autre paramètre.

4.1.20 Empêcher les fichiers en clair

Avec ce paramètre, vous pouvez empêcher la création de fichiers en clair dans les chemins réseau définis, sur les lecteurs réseau connectés ou locaux si aucun profil utilisateur *u.trust LAN Crypt* n'a encore été chargé ou si l'utilisateur n'en possède pas. Vous pouvez saisir ici aussi bien des chemins réseau (chemins UNC) que des chemins locaux.

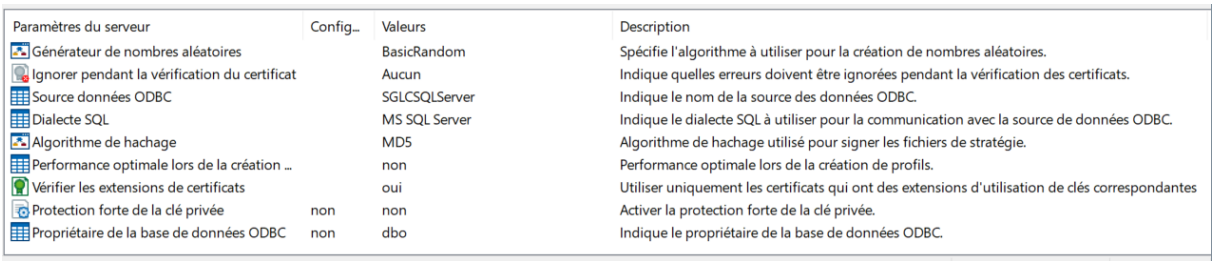
Exemple :

```
\\serveur1.local.intern\share1\
\\serveur2.extern\share2\
C:\Nom du dossier\
```

Remarque : Veuillez utiliser uniquement des chemins UNC pour les dossiers réseau au lieu de lettres de lecteur (voir les exemples ci-dessus). Cela garantit que les chemins fonctionnent pour tous les utilisateurs, car les lettres de lecteur peuvent varier d'une configuration à l'autre.

4.2 Paramètres du serveur

Remarque : Vous devez définir ces paramètres pour le serveur. Ils n'ont aucun effet sur les ordinateurs clients, sauf dans le cas d'une exception (« *Activer la protection forte de la clé privée* »).



Paramètres du serveur	Config...	Valeurs	Description
Générateur de nombres aléatoires		BasicRandom	Spécifie l'algorithme à utiliser pour la création de nombres aléatoires.
Ignorer pendant la vérification du certificat		Aucun	Indique quelles erreurs doivent être ignorées pendant la vérification des certificats.
Source données ODBC		SGLCSQLServer	Indique le nom de la source des données ODBC.
Dialecte SQL		MS SQL Server	Indique le dialecte SQL à utiliser pour la communication avec la source de données ODBC.
Algorithme de hachage		MD5	Algorithme de hachage utilisé pour signer les fichiers de stratégie.
Performance optimale lors de la création ...		non	Performance optimale lors de la création de profils.
Vérifier les extensions de certificats		oui	Utiliser uniquement les certificats qui ont des extensions d'utilisation de clés correspondantes
Protection forte de la clé privée	non	non	Activer la protection forte de la clé privée.
Propriétaire de la base de données ODBC	non	dbo	Indique le propriétaire de la base de données ODBC.

Cependant, si vous n'utilisez **pas** les paramètres standard, il est essentiel que vous définissiez ces paramètres de serveur avant de démarrer la fonction d'administration pour la première fois !

4.2.1 Activer la protection forte de la clé privée

Ici, vous pouvez indiquer que le responsable (principal) de la sécurité est invité à s'authentifier chaque fois que la clé privée est utilisée par *u.trust LAN Crypt*. Si vous activez ce paramètre, il s'applique également aux clients (voir « Protection forte de la clé privée » sous « *Paramètres client* » à la page 198).

Remarque : Sur les ordinateurs sur lesquels vous utilisez l'*u.trust LAN Crypt ScriptingAPI*, vous devez désactiver ce paramètre via la stratégie de groupe. Dans le cas contraire, la demande de mot de passe nécessite toujours une interaction utilisateur lors de l'exécution d'un script.

4.2.2 Dialecte SQL

Ici, vous indiquez le dialecte SQL à utiliser pour communiquer avec la source de données ODBC.

Sélectionner :

- MS SQL-Server
- Oracle
- Standard-SQL

Cela sera ensuite utilisé dans la configuration de votre système.

4.2.3 Propriétaire de la base de données ODBC

Ici, vous entrez le propriétaire de la base de données pour vous assurer qu'il est possible d'accéder à la base que vous utilisez.

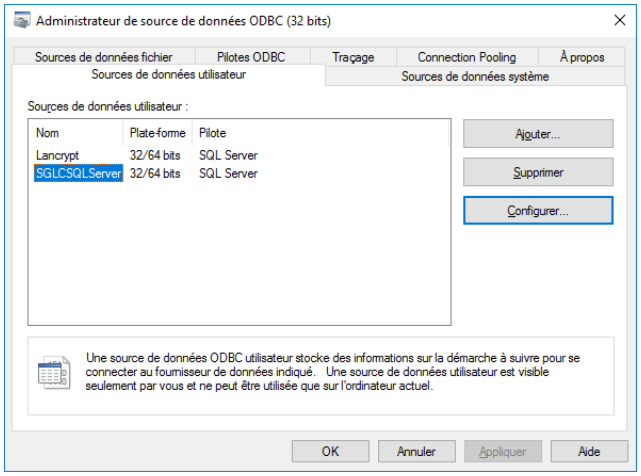
Pour MS SQL Server, la valeur par défaut « *dbo* » du générateur ne doit pas être modifiée. Il n'est nécessaire de le modifier que si vous utilisez une base de données Oracle.

Attention : Si vous utilisez une base de données Oracle, vous devez entrer le propriétaire de la base de données ici en **MAJUSCULES**. Il doit s'agir du même nom que celui utilisé lors de la création des tables de base de données.

4.2.4 Source de données ODBC

Ici, vous entrez le nom qui doit être utilisé pour accéder à la source de données ODBC.

u.trust LAN Crypt utilise **SGLCSQLServer** comme nom par défaut pour la source de données ODBC. Si vous souhaitez utiliser un nom différent, saisissez-le ici avant d'exécuter l'administration *u.trust LAN Crypt* pour la première fois.



Remarque : Le nom de la source de données ODBC est sensible à la casse ! Le nom que vous saisissez ici doit être identique au nom saisi lors de la création de la source de données ODBC. **Seules les sources de données ODBC 32 bits peuvent être utilisées.**

4.2.5 Générateur de nombres aléatoires

Pour la génération sécurisée de clés, *u.trust LAN Crypt* utilise un générateur de nombres aléatoires intégré. Vous pouvez définir ici l'algorithme que le générateur de nombres aléatoires doit utiliser. Le choix a une influence sur la sécurité des clés générées. « *BasicRandom* » offre de bonnes performances avec une sécurité modérée et convient aux systèmes disposant de ressources limitées. Il est pris en charge par toutes les versions précédentes de *LAN Crypt*. « *AdvancedRandom* » offre un équilibre entre bonne entropie et performance. « *SuperRandom* », en revanche, fournit une entropie nettement plus élevée et est recommandé pour les environnements auxquels s'appliquent des exigences de sécurité particulièrement élevées.

Remarque : Le nouvel algorithme « *SuperRandom* » n'est pris en charge qu'à partir de la version 13.0.0 de *u.trust LAN Crypt*.

Sélectionnez un algorithme pour le générateur de nombres aléatoires dans la zone de liste :

- BasicRandom
- AdvancedRandom
- SuperRandom

Si vous définissez le paramètre du générateur de nombres aléatoires sur **Non configuré**, *u.trust LAN Crypt* utilise « *SuperRandom* » par défaut.

Remarque : Vous pouvez définir l'algorithme du générateur de nombres aléatoires dans les paramètres du serveur et du client (voir « *Générateur de nombres aléatoires* » dans la section « *Paramètres du client* » à la page 198). Cependant, seul le même algorithme peut être utilisé dans les deux paramètres. Si vous modifiez l'algorithme du générateur de nombres aléatoires dans l'un des deux paramètres, la modification sera également appliquée à l'autre paramètre.

4.2.6 Ignorer pendant la vérification du certificat

Ici, vous pouvez indiquer le statut de certificat à ignorer lorsqu'un responsable de la sécurité se connecte ou lorsque des certificats sont assignés dans la console d'administration.

4.2.7 Algorithme de hachage

L'algorithme de hachage utilisé est uniquement affiché à cet endroit.

4.2.8 Vérifier les extensions de certificats

Par défaut, lorsqu'*u.trust LAN Crypt* assigne des certificats à partir du magasin de certificats, il utilise uniquement des certificats dont les valeurs *Chiffrement de clé* et/ou *Chiffrement de données* sont définies pour la propriété « *utilisation de la clé* ».

Cependant, dans **Vérifier les extensions de certificats**, vous pouvez indiquer que cette vérification n'est pas effectuée. Cela permet à *u.trust LAN Crypt* d'utiliser des certificats avec d'autres propriétés.

Vérifier les extensions de certificats : **non** permet d'utiliser des certificats avec d'autres propriétés.

Remarque : Cependant, le fait que ces types de certificats puissent ou non être utilisés avec *u.trust LAN Crypt* dépend du CSP ou du KSP que vous utilisez. Si vous décidez de désactiver cette vérification, assurez-vous que le type de certificat que vous souhaitez utiliser peut effectivement être utilisé avec *u.trust LAN Crypt*.

4.2.9 Performance optimale lors de la création de profils

Ce paramètre vous permet d'optimiser les performances lors de la création de fichiers de stratégie. Par défaut, lors de la création d'un fichier de stratégie, le fichier de stratégie temporaire est écrit dans le répertoire de cache du résolveur `%LOCALAPPDATA%\Utimaco\ResolverCache`, copié à partir de là, puis supprimé.

En revanche, avec le paramètre **oui**, le fichier de stratégie temporaire est immédiatement déplacé dans le répertoire de sortie lors de la création du profil. Il en résulte une amélioration des performances lors de la création des fichiers de stratégie.

Remarque : Cependant, si vous activez le paramètre **Performance optimale lors de la création de profils** et que le répertoire de cache du résolveur et le répertoire de sortie se trouvent sur le même support de stockage, les fichiers de profil créés dans le répertoire de sortie reçoivent la ACL héritée du répertoire de cache du résolveur, au lieu de la ACL héritée du répertoire de sortie.

Si vous définissez ce paramètre sur **Non configuré** ou **non**, lors de la création d'un fichier de stratégie est créé, le fichier de stratégie temporaire sera toujours écrit dans le répertoire de cache du résolveur par défaut, copié à partir de là, puis supprimé.

4.3 Lecteurs non gérés, applications non gérées, périphériques non gérés

u.trust LAN Crypt vous permet d'indiquer que des lecteurs, applications et périphériques (systèmes de fichiers réseau) doivent être « non gérés » (ignorés) par le pilote de filtre d'*u.trust LAN Crypt*, et donc exclus du chiffrement/déchiffrement transparent.

Un programme de sauvegarde est un exemple d'application susceptible de ne pas être gérée (appelée « non gérée »). Si vous souhaitez que les données de sauvegarde restent chiffrées, vous pouvez exclure cette application du processus de chiffrement/déchiffrement. Les données restent alors chiffrées lorsqu'elles sont sauvegardées.

Vous pouvez considérablement améliorer les performances en excluant des lecteurs de disque entiers. Si, par exemple, aucun chiffrement ne doit être effectué sur le lecteur « E: », celui-ci peut simplement être défini comme un « lecteur ignoré ». Sinon, vous pouvez définir une règle pour ce lecteur de disque en utilisant l'option « Ignorer la règle de chiffrement ».

Lorsque vous marquez un lecteur comme « non géré », le pilote de filtre ne traite pas le profil. Les opérations de fichiers s'exécutent donc plus rapidement.

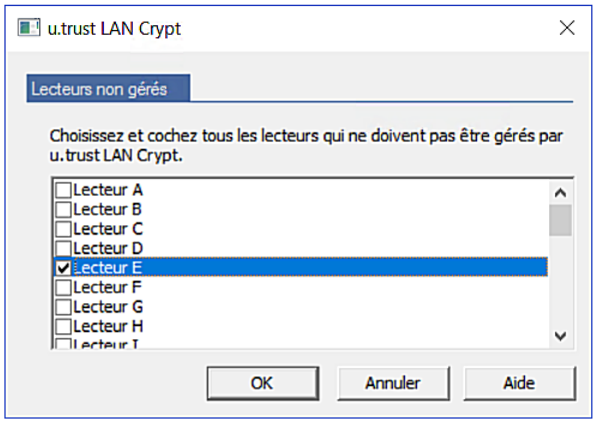
Ces paramètres se trouvent dans le nœud **configuration LAN Crypt**.

Remarque : Comme il s'agit de paramètres spécifiques à la machine, ils ne deviennent effectifs qu'une fois l'ordinateur client redémarré.

4.3.1 Ajout de lecteurs non gérés

Sélectionnez **Lecteurs non gérés** et cliquez sur **Ajouter un ou des lecteurs non gérés** dans le menu contextuel.

Sélectionnez les lecteurs qu'*u.trust LAN Crypt* doit ignorer, puis cliquez sur **OK**.



4.3.2 Ajout d'applications non gérées

Double-cliquez sur **Applications non gérées** dans les **paramètres client** pour ouvrir une boîte de dialogue dans laquelle vous pouvez spécifier les applications non gérées.

Utilisation typique :

- Les programmes de sauvegarde peuvent être définis comme « non gérés » pour s'assurer qu'ils lisent et enregistrent toujours les données chiffrées.
- Les applications qui peuvent provoquer des erreurs lors d'une utilisation simultanée avec *u.trust LAN Crypt*, mais qui ne nécessitent pas de chiffrement, peuvent généralement être exclues du processus de chiffrement.

Pour spécifier une application non gérée, vous devez entrer le nom complet de son fichier exécutable.

Saisissez le nom et le chemin de l'application (si nécessaire).

Si nécessaire, activez l'option **Inclure les processus enfants** et cliquez sur **OK**.

4.3.3 Ajout de périphériques non gérés

Double-cliquez sur **Périphériques non gérés** dans les *Paramètres client* pour ouvrir une boîte de dialogue dans laquelle vous pouvez spécifier les **Périphériques non gérés**.

La boîte de dialogue *Périphériques non gérés* affiche les systèmes de gestion de fichiers en réseau et certains types de lecteurs que vous pouvez exclure du processus de chiffrement d'*u.trust LAN Crypt*. Pour des raisons techniques, vous ne pouvez pas exclure les lecteurs réseau uniques ici. Vous ne pouvez exclure que des systèmes entiers de gestion de fichiers en réseau.

Remarque : Les responsables de la sécurité peuvent exclure des lecteurs de disque (réseau) individuels du processus de chiffrement en créant une règle de chiffrement à cette fin.

Outre ces systèmes de gestion de fichiers en réseau standard, vous pouvez également exclure des périphériques spécifiques en saisissant leur nom. Cela peut être utile si des systèmes de gestion de fichiers de fournisseurs tiers sont utilisés et que vous souhaitez les exclure du processus de chiffrement.

Vous pouvez exclure les périphériques prédéfinis suivants du chiffrement :

- Client pour réseaux Microsoft
- Client Microsoft pour Netware
- Client Novell pour Netware
- Mappage du lecteur du client Citrix
- Fournisseur UNC multiple

Ainsi que les périphériques supplémentaires suivants, par type :

- 1 Volume de démarrage
- 2 Volumes amovibles
- 4 Lecteurs optiques
- 8 Disques durs locaux
- 15 Tous les lecteurs locaux
- 16 Partage réseau

Saisissez le nom du ou des périphériques, puis cliquez sur **OK**.

Les administrateurs peuvent utiliser des outils tels que l'arborescence de périphériques d'OSR pour afficher les noms des systèmes de gestion de fichiers actuellement utilisés sur le système.

5 ANNEXE

5.1 Journalisation

.... Autorisations ajoutées pour « Security Officer_Utimaco-NI ». Autorisé : 0x86000000 - Refusé : 0x0)…

Les valeurs après **Autorisé :** et **Refusé :** indiquent quelles autorisations ont été réellement modifiées.

Vous pouvez utiliser les tableaux suivants pour interpréter les valeurs :

Autorisé : 0x86000000

ACL du responsable de la sécurité : Lire	0x80000000
ACL du responsable de la sécurité : Modifier le certificat	0x02000000
ACL du responsable de la sécurité : Changer de région	0x04000000
Autorisé :	0x86000000

Autorisations globales d'un responsable de la sécurité

Autorisations	Valeurs
Créer des responsables de la sécurité	0x000001
Créer des profils	0x000002
Créer des clés	0x000004
Copier des clés	0x000008
Supprimer des clés	0x000010
Lire la clé	0x000020
Créer des certificats	0x000040
Attribuer des certificats	0x000080
Administrer les groupes	0x000200
Connexion à la base de données	0x000400
Autoriser les opérations	0x000800
Administrer les utilisateurs	0x001000
Créer des règles	0x002000

Autorisations	Valeurs
Modifier les autorisations globales	0x004000
Modifier les ACL	0x008000
Utiliser des clés spécifiques	0x010000
Modifier la configuration	0x020000
Lire les entrées d'enregistrement	0x040000
Gérer l'enregistrement	0x080000
Importer des objets de répertoire	0x100000

ACL d'un groupe

Créer une clé	0x00000001
Copier une clé	0x00000002
Supprimer la clé	0x00000004
Créer des règles	0x00000008
Attribuer 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 des responsables de la sécurité

Autorisations	Valeur
Modifier le nom	0x01000000
Modifier le certificat	0x02000000
Modifier de région	0x04000000
Assigner la configuration	0x08000000
Supprimer un responsable de la sécurité	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 dispose de l'autorisation globale de créer davantage de responsables de la sécurité.
Créer des profils	Le responsable de la sécurité dispose de l'autorisation globale d'exécuter le résolveur de profil et de générer des fichiers de stratégie pour les utilisateurs individuels. Cette autorisation globale est la condition préalable pour définir l'autorisation **Créer des profils** d'un groupe spécifique pour un responsable de la sécurité. **Créer des profils** permet au responsable de la sécurité de créer des profils pour les utilisateurs. Pour cela, il doit disposer de l'autorisation **Créer des profils** pour leur groupe parent. Disposer de cette autorisation constitue une condition préalable à l'assignation de valeurs aux clés. Un responsable de la sécurité qui dispose de la seule autorisation **Créer des clés** ne peut générer que des clés sans valeurs !

Autorisations	Description
Créer des profils pour tous les membres	Cette autorisation nécessite que l'autorisation **Créer des profils** soit définie. Cette autorisation globale est la condition préalable pour définir l'autorisation **Créer des profils** pour un groupe spécifique. **Créer des profils pour tous les membres** permet à un responsable de la sécurité de créer des profils pour tous les utilisateurs. Pour cela, le responsable de la sécurité doit disposer de l'autorisation **Créer des profils** sur le groupe parent de l'utilisateur ou de l'autorisation **Créer des profils pour tous les membres** sur l'un des groupes dont l'utilisateur est membre. **Remarque :** L'autorisation globale **Créer des profils** étant une condition préalable pour **Créer des profils pour tous les membres**, ce qui suit s'applique : Désactiver l'autorisation **Créer des profils** désactive également automatiquement l'autorisation **Créer des profils pour tous les membres**. Activer l'autorisation **Créer des profils pour tous les membres** active automatiquement l'autorisation **Créer des profils**.
Créer des clés	Le responsable de la sécurité peut générer des clés dans les groupes individuels. Un responsable de la sécurité qui dispose de la seule autorisation **Créer des clés** ne peut générer que des clés sans valeurs ! Dans la console d'administration, des clés sans valeur peuvent être assignées aux groupes et aux utilisateurs. La valeur elle-même est générée lorsque des fichiers de stratégie sont générés. Pour générer des clés avec valeurs manuellement, le responsable de la sécurité doit disposer de l'autorisation **Créer des profils**.
Copier des clés	Le responsable de la sécurité est autorisé à copier des clés.
Supprimer des clés	Le responsable de la sécurité peut supprimer des clés de groupes individuels.
Lire la clé	Le responsable de la sécurité peut voir les données des clés individuelles d'un groupe.
Créer des certificats	Le responsable de la sécurité peut générer des certificats pour les utilisateurs.

Autorisations	Description
Attribuer des certificats	Le responsable de la sécurité est autorisé à assigner des certificats aux utilisateurs. Le responsable de la sécurité est autorisé à exécuter l'assistant permettant d'assigner des certificats. Cette autorisation globale est la condition préalable qui permet de définir l'autorisation **Assigner des certificats** à un groupe spécifique pour un responsable de la sécurité. **Assigner des certificats** permet au responsable de la sécurité d'assigner des certificats aux utilisateurs. Pour cela, le responsable de la sécurité doit disposer de l'autorisation **Assigner des certificats** pour le groupe parent de l'utilisateur.
Assigner des certificats à tous les membres	Cette autorisation nécessite que l'autorisation **Assigner des certificats** soit définie. Cette autorisation globale est la condition préalable qui permet de définir l'autorisation **Assigner des certificats à tous les membres** pour un groupe spécifique. **Assigner des certificats à tous les membres** permet à un responsable de la sécurité d'assigner des certificats à tous les utilisateurs. Pour cela, le responsable de la sécurité doit disposer de l'autorisation **Assigner des certificats** sur le groupe parent de l'utilisateur ou de l'autorisation **Assigner des certificats à tous les membres** sur l'un des groupes dont l'utilisateur est membre. **Remarque :** L'autorisation globale **Assigner des certificats** étant une condition préalable pour **Assigner des certificats à tous les membres**, ce qui suit s'applique : Désactiver l'autorisation **Assigner des certificats** désactive également automatiquement l'autorisation **Assigner des certificats à tous les membres**. Activer l'autorisation **Assigner des certificats à tous les membres** active automatiquement l'autorisation **Assigner des certificats**.
Administrer les groupes	Le responsable de la sécurité peut apporter des modifications aux groupes. Ajout de sous-groupes, déplacement de groupes, synchronisation de groupes et suppression de groupes.
Connexion à la base de données	Le responsable de la sécurité peut se connecter à la base de données *u.trust LAN Crypt*. Le paramètre par défaut pour cette autorisation est *actif*. Avec cette autorisation, un responsable de la sécurité peut facilement apporter des modifications à la base de données sans grande difficulté (par exemple si le personnel quitte l'entreprise). Ce droit n'est pas accordé

Autorisations	Description
	aux personnes qui ne sont autorisées à agir que si quelqu'un d'autre autorise leurs actions. Cela garantit que ces personnes ne peuvent autoriser que les actions qui nécessitent une confirmation, et n'ont aucun moyen d'apporter des modifications dans *u.trust LAN Crypt*.
Autoriser les opérations	Le responsable de la sécurité peut participer à des actions qui nécessitent une confirmation.
Administrer les utilisateurs	Le responsable de la sécurité peut ajouter des utilisateurs à un groupe, les supprimer d'un groupe et synchroniser des groupes.
Copier des utilisateurs	Le responsable de la sécurité est autorisé à ajouter (copier) des utilisateurs à des groupes. Cette autorisation globale est la condition préalable qui permet de définir l'autorisation **Copier des utilisateurs** pour un groupe spécifique pour un responsable de la sécurité. Pour ajouter un utilisateur à un groupe, le responsable de la sécurité doit disposer de 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 autorisations globales accordées à un autre responsable de la sécurité.
Modifier les ACL	Le responsable de la sécurité peut modifier l'ACL d'un groupe.
Utiliser des clés spécifiques	Le responsable de la sécurité peut utiliser des clés spécifiques concrètes dans les règles de chiffrement et afficher des clés spécifiques dans **Toutes les clés u.trust LAN Crypt**.
Modifier la configuration	Le responsable de la sécurité peut modifier la configuration (chemins). Cette autorisation est nécessaire pour afficher l'onglet **Configuration** dans le nœud **Paramètres centraux**, et pour que le responsable de la sécurité puisse apporter des modifications dans l'onglet **Répertoires** s'il est connecté à la base de données.
Lire les entrées d'enregistrement	Le responsable de la sécurité peut afficher les paramètres utilisés pour la journalisation et les événements enregistrés.

Autorisations	Description
Gérer l'enregistrement	Le responsable de la sécurité peut modifier les paramètres d'enregistrement. Il est autorisé à archiver, supprimer et vérifier les entrées.
Importer des objets de répertoire	Le responsable de la sécurité peut importer des UO, des groupes et des utilisateurs à partir d'un service d'annuaire et les ajouter à la base de données *u.trust LAN Crypt*. Pour pouvoir importer des objets du répertoire, le responsable de la sécurité a également besoin des autorisations **Administrer les groupes** et **Administrer les utilisateurs**. Celles-ci sont définies automatiquement lorsque l'autorisation **Importer des objets du répertoire** est sélectionnée. Si le responsable de la sécurité ne dispose pas de cette autorisation, le nœud **Objets du répertoire** (utilisé pour importer des UO, des groupes et des utilisateurs) n'apparaît pas dans la console d'administration.

5.2.2 Autorisations pour modifier les paramètres d'un responsable de la sécurité

Autorisations	Description
Modifier le nom	Permet de modifier le nom du responsable de la sécurité auquel le propriétaire de l'autorisation est assigné.
Modifier le certificat	Permet de modifier le certificat du responsable de la sécurité auquel le propriétaire du droit est assigné.
Modifier de région	Permet de modifier le préfixe de région du responsable de la sécurité auquel le propriétaire du droit est assigné.
Assigner la configuration	Permet de modifier la configuration du responsable de la sécurité auquel le propriétaire du droit est assigné.
Supprimer un responsable de la sécurité	Permet de supprimer le responsable de la sécurité auquel le propriétaire de l'autorisation est assigné.
Modifier les autorisations globales	Permet de modifier les autorisations globales du responsable de la sécurité auquel le propriétaire de l'autorisation est assigné.
Modifier une ACL	Permet de modifier l'ACL du responsable de la sécurité auquel le propriétaire de l'autorisation est assigné.
Lire	Affiche le responsable de la sécurité auquel le propriétaire de l'autorisation est assigné dans le nœud **Paramètres centraux** \ **Administration des responsables de la sécurité**. Il s'agit de la condition préalable pour tous les droits qui permettent le traitement de ce responsable de la sécurité. Est défini automatiquement si un droit de ce type est sélectionné.

5.2.3 Autorisations des responsables de la sécurité pour le traitement des groupes

Autorisations	Description
Créer une clé	Le responsable sécurité est autorisée à générer des clés dans le groupe.
Copier des clés	Le responsable de la sécurité est autorisé à copier des clés.
Supprimer la clé	Le responsable de la sécurité est autorisé à supprimer des clés.
Créer des règles	Le responsable de la sécurité est autorisé à générer des règles pour les utilisateurs.
Attribuer des certificats	Le responsable de la sécurité est autorisé à assigner des certificats aux utilisateurs. Le responsable de la sécurité est autorisé à exécuter l'assistant utilisé pour assigner des certificats. **Assigner des certificats** permet au responsable de la sécurité d'assigner des certificats aux utilisateurs du groupe, là où le groupe est également le groupe parent.
Attribuer des certificats à tous les membres	Cette autorisation nécessite que l'autorisation **Assigner des certificats** soit définie. **Assigner des certificats à tous les membres** permet au responsable de la sécurité d'assigner des certificats à tous les utilisateurs du groupe : les utilisateurs dont le groupe est le groupe parent ainsi que les utilisateurs qui sont membres du groupe et ont un groupe parent différent. **Remarque :** Définir **Assigner des certificats à tous les membres** sur **Autoriser** définit automatiquement **Assigner des certificats** sur **Autoriser**. Définir **Assigner des certificats** sur **Refuser** définit automatiquement **Assigner des certificats à tous les membres** sur **Refuser**.
Ajouter un utilisateur	Le responsable de la sécurité est autorisé à ajouter manuellement des utilisateurs au groupe. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Copier des utilisateurs	Le responsable de la sécurité est autorisé à ajouter des utilisateurs de ce groupe à un autre groupe. Cela n'est autorisé que pour les membres dont ce groupe est également l'objet parent.

Autorisations	Description
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 des 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 des utilisateurs.
Supprimer des sous-groupes	Le responsable de la sécurité est autorisé à supprimer les sous-groupes de ce groupe. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Déplacer des groupes	Le responsable de la sécurité est autorisé à déplacer les groupes créés manuellement dans l'administration (avec un « *glisser-déposer* »). Les groupes importés ne peuvent pas être déplacés. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Modifier les propriétés	Le responsable de la sécurité est autorisé à modifier les propriétés d'un groupe.
Supprimer un groupe	Le responsable de la sécurité est autorisé à supprimer des groupes. Cela suppose que le responsable de la sécurité a supprimé l'autorisation **Supprimer des sous-groupes** dans le groupe ci-dessus. Cette autorisation est une condition préalable à l'importation / la synchronisation des groupes et des utilisateurs.
Créer des profils	Le responsable de la sécurité est autorisé à exécuter le résolveur de profil et à 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, là où le groupe est également le groupe parent.

Autorisations	Description
Créer des profils pour tous les membres	Cette autorisation nécessite que l'autorisation **Créer des profils** soit définie. **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 ainsi que les utilisateurs qui sont membres du groupe et ont un groupe parent différent. **Remarque :** Définir **Créer des profils pour tous les membres** sur **Autoriser** définit automatiquement **Créer des profils** sur **Autoriser**. Définir **Créer des profils** sur **Refuser** définit automatiquement **Créer des profils pour tous les membres** sur **Refuser**.
Modifier une ACL	Le responsable de la sécurité est autorisé à modifier l'ACL du groupe (par exemple en ajoutant un autre responsable de la sécurité).
Lire	Le responsable de la sécurité dispose des droits de lecture pour ce groupe et peut voir le contenu des composants logiciels enfichables. Est défini automatiquement, si les autorisations de modification sont accordées.
Visible	Le responsable sécurité peut consulter le groupe. Est défini dans le nœud de base et héritée vers le bas. Si ceci est refusé pour le responsable de la sécurité, le groupe est masqué (l'autorisation de **Lecture** doit également être refusée).

6 Mentions légales

Copyright © 2023 - 2026 Utimaco IS GmbH, 2018 - 2023 conpal GmbH, 1996 - 2018 Sophos Limited et Sophos Group. Tous droits réservés.

Tous les autres noms de produits et de sociétés mentionnés sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système d'extraction ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, par photocopie, enregistrement ou autre, à moins que vous ne disposiez d'une licence valide permettant la reproduction de la documentation conformément aux termes de la licence, ou que vous ayez l'autorisation écrite préalable du propriétaire du droit d'auteur.

Vous trouverez des informations sur les droits d'auteur de fournisseurs tiers dans le document Logiciel tiers de votre répertoire de produits.

7 Support technique

Obtenez un support technique pour u.trust LAN Crypt de l'une des manières suivantes :

- Sur https://support.hsm.utimaco.com, les clients enregistrés disposant de contrats de maintenance actifs ont accès aux téléchargements, à la documentation et aux éléments de connaissance.

Téléchargez la documentation du produit client pour Windows sur

- https://help.lancrypt.com/docs/windows/13_0_3/de/ en allemand
- https://help.lancrypt.com/docs/windows/13_0_3/en/ en anglais
- https://help.lancrypt.com/docs/windows/13_0_3/fr/ en français
- https://help.lancrypt.com/docs/windows/13_0_1/jp/ en japonais

Téléchargez la documentation du produit client pour macOS sur

- https://help.lancrypt.com/docs/macOS/de/ en allemand
- https://help.lancrypt.com/docs/macOS/en/ en anglais

Téléchargez la documentation du produit *pour iOS / iPadOS* sur

- https://help.lancrypt.com/docs/ios/de/ en allemand
- https://help.lancrypt.com/docs/ios/en/ en anglais

Téléchargez la documentation du produit *pour Android* sur

- https://help.lancrypt.com/docs/android/de/ en allemand
- https://help.lancrypt.com/docs/android/en/ en anglais

Téléchargez la documentation du produit *u.trust LAN Crypt 2Go* at

- https://help.lancrypt.com/docs/2Go/de/ en allemand
- https://help.lancrypt.com/docs/2Go/en/ en anglais

Téléchargez la documentation du produit d'administration sur

- https://help.lancrypt.com/docs/admin/13_0_1/de/ en allemand
- https://help.lancrypt.com/docs/admin/13_0_1/en/ en anglais
- https://help.lancrypt.com/docs/admin/13_0_1/fr/ en français
- https://help.lancrypt.com/docs/admin/13_0_1/jp/ en japonais

Les clients enregistrés pour la maintenance peuvent envoyer un courriel à l'adresse

support@utimaco.com

en incluant leur(s) numéro(s) de version du logiciel *u.trust LAN Crypt*, système(s) d'exploitation et niveau(x) de correctifs, ainsi que le texte de tout message d'erreur.