Creating Trust in
the Digital Society

utimaco®

u.trust LAN Crypt 管理コンソール

製品バージョン: **11.0.0**
文書作成年月 : **2024年9月**

内容

1 概要 4

1.1 u.trust LAN Crypt とは？ 4

1.2 u.trust LAN Crypt によるデータ保護 6

1.3 透過的暗号化 8

1.4 アーキテクチャ 12

2 はじめに 15

2.1 証明書 15

2.2 インストール 20

2.3 無人インストール 22

2.4 アップグレード 24

2.5 言語設定 26

2.6 アンインストール 26

3 管理 27

3.1 必要なステップ 29

3.2 u.trust LAN Crypt を管理するための準備 29

3.3 マスターセキュリティオフィサー 33

3.4 管理コンソール：概要 37

3.5 中央設定 40

3.6 すべての u.trust LAN Crypt キーの表示 69

3.7 選択されたユーザーと証明書の表示 71

3.8 セキュリティオフィサーの作成 73

3.9 管理コンソールコンソールへのログオン 86

3.10 グループとユーザーのインポート 87

3.11 セキュリティオフィサーの OU への配属 100

3.12 グループのプロパティ 106

3.13 ユーザーのプロパティ 111

3.14 セキュリティ環境の設計 113

3.15 キーの生成 114

3.16 暗号化ルール 121

3.17 暗号化タグ 135

3.18 証明書の割り当て 136
3.19 暗号化ルールの提供 - ポリシーファイルの生成 146
3.20 データベースのロギング 150
4 u.trust LAN 暗号化設定 156
4.1 クライアント設定 157
4.2 LAN Crypt の管理設定 166
4.3 処理しないドライブ、アプリケーション、デバイス 168
5 付録 171
5.1 ロギング 171
5.2 権限 174
6 法的通知 181
テクニカルサポート 181

1 概要

1.1 u.trust LAN Crypt とは？

u.trust LAN Crypt は透過的ファイル暗号化を提供し、大規模な組織内のユーザーが秘密裏にデータを交換できるようにするために開発されました。暗号化されたファイルはユーザーのハードディスク、リムーバブルメディア、ネットワークドライブに保存できます。

u.trust LAN Crypt バージョン 11.0.0 では、ユーザープロファイルに、他の u.trust LAN Crypt 環境のポリシーファイルから作成されたルールとキーを含めることができるようになりました（マルチポリシー対応）。u.trust LAN Crypt API を使用することで、他の u.trust LAN Crypt 環境の暗号化ファイルにアクセスできるようになります。このような追加ポリシーファイルが正常に読み込まれると、拡張ルールとキーがユーザーのクライアントに表示されます。詳細については、Utimaco サポートにお問い合わせください。

LAN Crypt バージョン 4.1.0 から、新たに統合された多要素認証(MFA)を使用して、初めてコンピュータにログインすることができます。

暗号化プロセスはユーザーにとって完全に透過的です。ファイルの作成時や保存時に自動的に行われます。これらのファイルは、データが読み取られる際にも透過的に復号化されます。このプロセスは、Windows コンピュータのファイルシステムに組み込まれたフィルタドライバーによって実行されます。バージョン 4.0.0 から、LAN Crypt は将来性のあるミニフィルタドライバーを使ってファイルの暗号化を行うオプションを初めて提供します。バージョン 4.1.0 からのこの最新のファイルフィルタドライバーは、以前のすべてのインストールに含まれていた従来のファイルフィルタドライバーを完全に置き換えます。

注意：

バージョン 4.1.0 から、LAN Crypt クライアントはレガシーフィルタドライバーを含まなくなりました。しかし、レガシーフィルタドライバーを使用していた以前の LAN Crypt クライアントは、互換性のためにまだサポートされています。

u.trust LAN Crypt フィルタドライバーは、ウイルススキャナに似た方法で動作します。どのファイルにアクセスするかを識別し、そのファイルに対して適切な暗号化または復号化処理を実行します。あるユーザーが信頼されたディレクトリにファイルを移動すると、そのユーザーのコンピュータ上でファイルは暗号化され、同じグループのメンバーである他の信頼されたユーザーがこのディレクトリからファイルを読むたびに、そのファイルは暗号化された状態でこのユーザーに転送されます。ファイルはターゲットコンピュータに到達するまで復号化されず、そこでユーザーはファイルを変更することができます。その後、暗号化されたディレクトリに戻される前に再び暗号化されます。

暗号化されたファイルは、個々のユーザーに割り当てられることはありません。正しいキーを持つユーザーであれば誰でも暗号化されたファイルにアクセスすることができます。このため、管理者は論理的なユーザーグループを作成し、そのメンバーで暗号化されたファイルを共有することができます。u.trust LAN Crypt は、ユーザーやユーザーグループにキーを提供し、それぞれのキーを使って異なるドアや金庫を開けることができます。

権限のないユーザーは、暗号化されたファイルに物理的にアクセスすることができます（ただし、u.trust LAN Crypt をインストールしていないワークステーションからのみ）。ただし、u.trust LAN Crypt の認証がない場合、ファイルを読むことはできません。

その結果、ファイルシステム自体にアクセス保護が定義されていなくても、ネットワークが攻撃されたり、従業員が組織のセキュリティポリシーに従わなかったりしても、ファイルは常に保護されます。

LAN、ファイルサーバー、ローカルハードディスク、リムーバブルメディアに保存された知的財産を不正アクセスから保護する必要がある場合、u.trust LAN Crypt が最適です。

セキュリティオフィサー（SO）は、1 つ以上の暗号化ルールを定義することで、u.trust LAN Crypt で保護するファイルやフォルダを一元的に指定できます。例えば、すべての Word 文書を保護するために、セキュリティオフィサーは*.docx というルールを定義します。このルールがポリシーファイルの一部としてクライアントシステム全体にロールアウトされると、すべての Word 文書がどこに保存されていても暗号化されます。必要に応じて、複数の暗号化ルールを組み合わせて暗号化プロファイルを作成できます。

この例では、3 つの異なるルールが 1 つの暗号化プロファイルにまとめられています。

ルール	キー	説明
*.docx	キー1	これにより、すべての Word 文書がどこに保存されていても、"キー1"で暗号化されます。
D:¥Data¥*.*.	キー2	指定したフォルダ内のすべてのファイルをキー2 で暗号化します。
¥¥Server1¥Share1¥HR¥*.xlsx	キー3	指定したサーバーフォルダー内のすべての Excel ファイルをキー3 で暗号化します。

u.trust LAN Crypt を使用すると、セキュリティオフィサーは非常に複雑なルールを定義して、実際に必要なデータだけが非常に特定の場所で暗号化されるようにすることができます。これらのルールは、ファイルサーバーまたは Windows ドメインコントローラのネットログオンフォルダに保存できるポリシーファイルにロールアウトされます。セキュリティオフィサーは、ボタンをクリックするだけで、個々のユーザーに合わせたポリシーを作成することができます。このポリシーには、そのユーザーに適用されるすべてのキーとルールが含まれています。

セキュリティオフィサーは、u.trust LAN Crypt 管理コンソールグラフィカルユーザーインタフェースを使用して、これらのポリシーファイルを生成および管理します。このインタフェースには、Microsoft 管理コンソール（MMC）が使用されます。Snap-Ins は、セキュリティオフィサーの作業を容易にするさまざまなツールを提供します。

ポリシーファイルは、ユーザーごとに証明書によって個別に保護されています。そのため、このファイルに含まれるすべてのキーは、各ユーザーの証明書の公開キーで暗号化され、u.trust LAN Crypt クライアントアプリケーションを介してこのファイルを開くことができるのは、使用されている証明書の秘密鍵も所有している正規ユーザーのみとなります。組織内で既に利用可能な公開キー基盤（PKI）を使用することができます。また、セキュリティオフィサーが u.trust LAN Crypt を使って証明書を生成することもできます。

u.trust LAN Crypt 管理コンソールデータは SQL データベースに保存されます。もちろん、すべての重要なデータレコード、特にキーデータは SQL データベース内で暗号化されます。

u.trust LAN Crypt は、システム管理機能に依存しないデータベースを使用するため、セキュリティ機能とシステム管理機能を厳密に分離することができます。

マスターセキュリティオフィサー(MSO)のみが、常にすべての権限を持ちます。マスターセキュリティオフィサーは、u.trust LAN Crypt の管理に関する個々のタスクや権限を他のセキュリティオフィサーに委譲することもできます。

1.2 u.trust LAN Crypt によるデータ保護

u.trust LAN Crypt は、機密ファイルをファイルサーバーやワークステーションにセキュア保存できることを保証します。暗号化と復号化はクライアントワークステーション上の RAM で実行されるため、データは LAN または WAN ネットワークを介してセキュア転送されます。ファイルサーバー自体に特別なセキュリティソフトウェアをインストールする必要はありません。

ポリシーファイルには、透過的暗号化に必要なすべてのルール、アクセス権、キーが含まれています。

ユーザーがワークステーションで u.trust LAN Crypt を使ってデータを暗号化復号化するには、ポリシーファイルにアクセスできなければなりません。これは、ポリシーファイルがある場所のネットワーク共有を通じて行われます。ポリシーファイルは暗号化され、証明書によって不正使用から保護されています。これらを使用できるようにするには、ユーザーは証明書の秘密鍵を持っており、パスワードを知っている必要があります。

すべての暗号化/復号化タスクは、最小限のユーザー操作でクライアントワークステーション上で透過的に実行されます。

u.trust LAN Crypt は、ディレクトリやファイルに対して異なる権限を定義することで、信頼されたユーザーを異なる信頼されたグループにまとめることができます。これらの権限は、ユーザーの暗号化プロファイルにグループ化されます。ユーザーは、証明書に割り当てられた秘密鍵を所有することで、暗号化プロファイルを含むポリシーファイルにアクセスできます。

ポリシーファイルに同じ暗号化プロファイルが含まれている u.trust LAN Crypt ユーザーは、すべて信頼されたグループのメンバーです。ユーザーは暗号化やキー交換の心配をする必要はありません。ポリシーファイルにアクセスできるだけで、データを開いたり閉じたりするたびに、透過的に暗号化または復号化されます。

暗号化プロファイルはポリシーファイルを介して配布されるため、ユーザーを集中管理する LAN モデルから、ユーザーがノートブックで作業するリモートモデルまで、あらゆる組織形態に対応できます。

注意：通常の操作でも、Windows は作業メモリの一部をハードディスクにスワップすることがよくあります。クラッシュやいわゆるブルースクリーンの場合などには、メモリの内容全体がハードディスクに書き込まれることさえあります。その結果、他の方法ではメインメモリにしかない機密情報（開いているドキュメントの内容など）が、ハードディスク上のファイルに保存される可能性があります。ハードディスクの暗号化（BitLocker や Utimaco DiskEnCrypt など）により、機密性の高いデータのコンテンツは暗号化された状態でハードディスクに保存されるため、スパイ行為から最適に保護されます。このような理由から、ハードディスク暗号化は重要な基本的保護手段として、また u.trust LAN Crypt を使用する際の追加機能として推奨されます。

u.trust LAN Crypt は、Windows、macOS、Android、iOS / iPadOS のモバイルデバイスをサポートしています。

u.trust LAN Crypt 管理コンソールおよび Windows 管理

u.trust LAN Crypt の設定と暗号化プロファイルの管理には、別の管理用コンピュータを使用します。Windows の管理と u.trust LAN Crypt の管理を明確に区別するために、セキュリティオフィサーの役割を確立する必要があります。セキュリティオフィサーは、暗号化されたデータを特定のディレクトリに保存し、誰がそのデータにアクセスできるかを指定するために、ポリシーファイルに暗号化プロファイルを定義します。管理ステーションでポリシーファイルを作成した後、セキュリティオフィサーはそれを展開します。

u.trust LAN Crypt の管理には、Windows の標準ツールである Microsoft 管理コンソール（MMC）を使用します。u.trust LAN Crypt 管理コンソールのユーザーインターフェースは、MMC 用のスナップインで構成されています。u.trust LAN Crypt 管理コンソールは、管理対象のほとんど（ユーザーデータ、キー、暗号化パスなど）を独自のデータベースに保存します。

ActiveDirectory のような Windows ツールではなく、このデータベースアプローチを使用することには、2 つの大きな利点があります：

- システム管理とセキュリティ管理は厳密に分離することができます。これは u.trust LAN Crypt が専用のデータベースを使用し、システム管理から完全に独立しているためです。u.trust LAN Crypt 管理コンソールデータベースのキーは暗号化されているため、不正アクセスから保護されています。さらに、このデータベースは u.trust LAN Crypt システムが意図せず変更されるのを防ぎます（例えば、システム管理者が必要なセキュリティオブジェクトを削除した場合など）。
- 一方、システム管理者でない人にシステム設定の変更を許可するのは、多くの場合良い考えとは言えません。システム管理のためにデータの書き込み権限を与えることは現実的な問題であることは明らかです。u.trust LAN Crypt に特化したデータを別のデータベースに保存するもう一つの良い理由がこれです。

最高の保護を提供するため、u.trust LAN Crypt の機能は 2 つの部分に分かれています：

- u.trust LAN Crypt ユーザー機能

  u.trust LAN Crypt のユーザー機能には、データの暗号化と復号化情報が含まれます。この情報は u.trust LAN Crypt を使用する日常業務に必要です。ユーザーが暗号化情報へのアクセスを許可されると、ファイルは透過的に暗号化復号化されます。それ以上のユーザー操作は必要ありません。さらに、u.trust LAN Crypt には様々な表示機能があり、ユーザーは自分の暗号化プロファイルや提供されたキーを確認することができます。

- u.trust LAN Crypt セキュリティオフィサーの機能

  u.trust LAN Crypt 管理コンソールは、セキュリティオフィサーに予約されている機能を提供します。暗号化ルールの管理は、セキュリティオフィサーの証明書を持っている場合にのみ可能です。その場合のみ、新しい暗号化プロファイルの作成や既存のプロファイルの管理などが可能になります。

両コンポーネントは別々に取り付けることができます。

1.3 透過的暗号化

ユーザーにとって、透過的暗号化とは、暗号化された形で（暗号化されたフォルダやドライブに）保存されたすべてのデータが、アプリケーションによって開かれたときに RAM で自動的に復号化されることを意味します。ファイルが保存されると、再び自動的に暗号化されます。

- 暗号化ルールのあるファイルはすべて自動的に暗号化されます。
- ファイルが暗号化されたフォルダにコピーまたは移動された場合、そのフォルダに適用される暗号化ルールに従って暗号化されます。もちろん、同じフォルダ内の異なるファイル拡張子やファイル名に対して異なる暗号化ルールを定義することもできます。暗号化はフォルダに固有のものではありません。暗号化ルールに完全に依存します。
- 暗号化されたファイルの名前が変更されても、暗号化されたままです（新しいファイル名/ファイル拡張子に別の暗号化ルールがないか、暗号化ルールがない場合）。
- 暗号化されたファイルを、現在の暗号化ルールがもはや有効でない場所にコピーまたは移動した場合、永続的暗号化がデフォルトで有効になっているため、暗号化されたままとなります。
- 暗号化されたファイルを、現在の暗号化ルールが無効で別の暗号化ルールが有効な場所にコピーまたは移動した場合、これらのファイルはまず復号化され、新しい暗号化ルールに従って再び暗号化されます。
- 透過的暗号化は、すべてのファイル操作に適用されます。暗号化されたデータを操作している間、これらのプロセスはすべてバックグラウンドで実行されるため、ユーザーはこれらのプロセスに全く気付かないままです。
- 永続的暗号化を使用すると、暗号化ルールが存在しないフォルダにファイルをコピーまたは移動するときに、ユーザーが意図せずにファイルを復号化するのを防ぐことができます。

1.3.1 暗号化されたデータへのアクセス

ユーザーが適切なキーを所有していない場合、フォルダ内の暗号化されたデータへのアクセスは許可されません。ユーザーは、このフォルダ内の暗号化されたファイルの読み取り、コピー、移動、名前の変更、その他の操作はできません。

ファイルが暗号化されたキーをユーザーが持っている場合、暗号化プロファイルにこれらのファイルを参照する暗号化ルールがなくても、いつでもこれらのファイルを開いて作業することができます。

1.3.2 フォルダの名前の変更と移動

パフォーマンス上の理由から、u.trust LAN Crypt は Windows エクスプローラを使用して完全なフォルダを移動しても暗号化ステータスを変更しません。つまり、フォルダを移動したり名前を変更したりしても、暗号化、復号化、再暗号化は行われません。

ファイルが暗号化されていた場合、新しいフォルダまたは新しい保存場所に暗号化されたまま残ります。ユーザーが適切なキーを所有している場合、これらのファイルを通常通り操作することができます。

注意：ただし、これは新しい保存場所に暗号化ルールがない場合にのみ適用されます。ただし、暗号化ルールがある場合、ファイルは新しい保存場所に適用される暗号化ルールに従って暗号化されます。

ファイルやフォルダの安全な移動: u.trust LAN Crypt では、ファイルやフォルダをセキュア移動することもできます。ファイルは暗号化ルールに従って暗号化、復号化、再暗号化されます。移動元ファイルは、移動後にセキュア削除（ワイプ）されます。

この機能は、Windows エクスプローラのコンテキストメニューの u.trust LAN Crypt のセキュア移動項目から利用できます。ダイアログを使用して、ファイルを移動する場所を選択できます。

1.3.3 ファイルの明示的復号化

永続的暗号化機能が無効になっている場合、復号化対象のファイルは、暗号化ルールが存在しない場所またはフォルダにコピーまたは移動するだけで、自動的に復号化されます。すると、自動的に復号化されます。

ただし、これは

- 適切な暗号化プロファイルがロードされています、
- ユーザーが正しいキーを持っているかどうかを確認します、
- 新しい場所の暗号化ルールがアクティブな暗号化プロファイルに存在しない場合。

1.3.4 暗号化ファイルの削除 - Windows のごみ箱

暗号化プロファイルがロードされている場合、あなたがキーを所有する暗号化されたファイルを削除することができます。

注意：ファイルの削除とは、実際には Windows のごみ箱に移動させることを意味します。最高レベルのセキュリティを提供するため、u.trust LAN Crypt で暗号化されたファイルはごみ箱に暗号化されたまま残ります。ごみ箱を空にするのにキーは必要ありません。

1.3.5 暗号化から除外されるファイル/フォルダ

次のファイルとフォルダは、暗号化から自動的に除外されます（これらのファイルに対して暗号化ルールが定義されている場合でも）。

- u.trust LAN Crypt インストールフォルダ内のファイル。
- Windows のインストールフォルダ内のファイル。
- ポリシーファイルのキャッシュ。

  場所は u.trust LAN Crypt 管理コンソールで指定され、ステータスダイアログのプロファイルタブに表示されます。
- システムドライブのルートディレクトリ。サブフォルダは除外されません。
- インデックスされた場所（search-ms）。

1.3.6 永続的暗号化

通常、ファイルは暗号化ポリシーが適用されている間だけ、u.trust LAN Crypt によって暗号化されます。そのため、暗号化ルールが適用されないフォルダにファイルをコピーまたは移動すると、ファイルは復号化されます。

暗号化されたファイルの不要な平文コピーを作成されたくない場合は、永続的暗号化を使用するとこれを防ぐことができます。永続的暗号化を使用すると、暗号化されたファイルが移動またはコピーされても復号化されないようにすることができます。

セキュリティオフィサーまたはシステム管理者は、Windows のグループポリシー（GPO）を介して u.trust LAN Crypt の設定でこの動作を無効にすることができます。デフォルトでは、この機能は u.trust LAN Crypt で既に有効になっています。永続的暗号化が無効化されている場合、暗号化されたファイルは暗号化ルールで定義されていない場所にコピー/移動されると復号化され、平文テキストで保存されます。

永続的暗号化については、以下のルールが適用されます：

- u.trust LAN Crypt ドライバーは、パス情報を含まないファイル名のみを保持します。この名前のみが比較に使用されるため、コピー元とコピー先のファイル名が同じ場合にのみ検出されます。コピー中にファイル名が変更された場合、コピー結果のファイルは異なるファイルとみなされ、永続的暗号化の対象外となります。
- 暗号化されたファイルを、暗号化ルールが適用されていない場所に別のファイル名で名前を付けて保存すると、ファイルは平文テキストになります。
- ファイルに関する情報は、限られた時間のみ保持されます。操作に時間がかかりすぎる場合（15 秒以上）、新しく作成されたファイルは別の独立したファイルと見なされるため、永続的暗号化の対象外となります。

1.3.6.1 永続的暗号化と暗号化ルールの比較

前述のように、永続的暗号化は、暗号化されたファイルがその暗号化状態、たとえば元の暗号化キーを保持することを保証しようとします。これは、ファイルが暗号化ポリシーが適用されていないフォルダに移動された場合は、まったく問題なく機能します。しかし、ファイルが暗号化ポリシーが適用される場所にコピーまたは移動された場合、暗号化ポリシーの優先順位が高くなるため、永続的暗号化よりも優先されます。ファイルは暗号化ルールで定義されたキーで暗号化され、元々使用されていたキーでは暗号化されません。

1.3.6.2 永続的暗号化 vs. 無視パスルール

無視パスルールは永続的暗号化も上書きするため、無視パスが適用されるフォルダにコピーされた暗号化ファイルは、平文で保存されます。

無視パスルールは、主に非常に頻繁にアクセスされるファイルや、暗号化される特別な理由がないファイルに使用されます。これにより、システムのパフォーマンスが向上します。

注意：ミニフィルタが暗号化ドライバーとして使用されている場合、無視パスルールの対象となるフォルダ内のファイルに対するアクセス保護はありません。

1.3.6.3 永続的暗号化と除外パス規則の比較

除外パスのルールは永続的暗号化も上書きするため、該当する除外パスを持つフォルダにコピーされた暗号化ファイルは平文で保存されます。

注意：除外パスルールが適用されるフォルダ内のファイルについては、アクセス保護が存続します。

1.3.7 永続的暗号化の制限

技術的な理由により、永続的暗号化にはいくつかの制限があり、言い換えれば、永続的暗号化の実際の結果が必ずしもユーザーの期待に沿うとは限りません。

永続的暗号化が不足する一般的なシナリオをいくつか紹介します：

平文のままであるべきファイルが暗号化

- 平文ファイルは、暗号化ルールを適用する場合としない場合の両方で、複数の場所にコピーされます。

  平文ファイルが同時に複数の場所にコピーされ、そのうちの 1 つに暗号化ルールが適用されている場合、元のファイルは暗号化されていないにもかかわらず、そのファイルの他のコピーも暗号化される可能性があります。ファイルが最初に暗号化された場所にコピーされた場合、そのファイルはドライバーの内部リストに追加されます。2つ目のコピーが他の場所に作成されると、ドライバーはそのファイル名をリストに見つけ、2 つ目のコピーも暗号化します。

- 暗号化されたファイルにアクセスした後、同じ名前のファイルを作成します。

  暗号化されたファイルが開かれ（アクセスされ）、その直後に同じ名前の新しいファイルが作成された場合、新しく作成されたファイルは、最初に開かれたファイルと同じキーで暗号化されます。

  注意：暗号化されたファイルの読み取りと新しいファイルの作成に同じアプリケーション/スレッドが使用されている場合にのみ適用されます。

  一般的な使用例　Windows　エクスプローラで、暗号化ルールのあるフォルダを右クリックし、新規作成 > テキスト文書をクリックします。すぐに暗号化ルールのないフォルダを右クリックし、新規作成→テキスト文書をクリックします。つ目のファイルも暗号化されます。

ファイルは暗号化されません

- ファイルの複数のコピーが作成されます。

  暗号化されたファイルのコピーが元のファイルと同じフォルダに作成された場合、これらのコピーは暗号化されません。作成されたコピーはファイル名が異なるため（doc.txt　と　doc　-　Copy.txt）、ファイル名の一致が失敗し、永続的暗号化によって暗号化されません。

1.3.8 DLP 製品のクライアント API と暗号化タグ

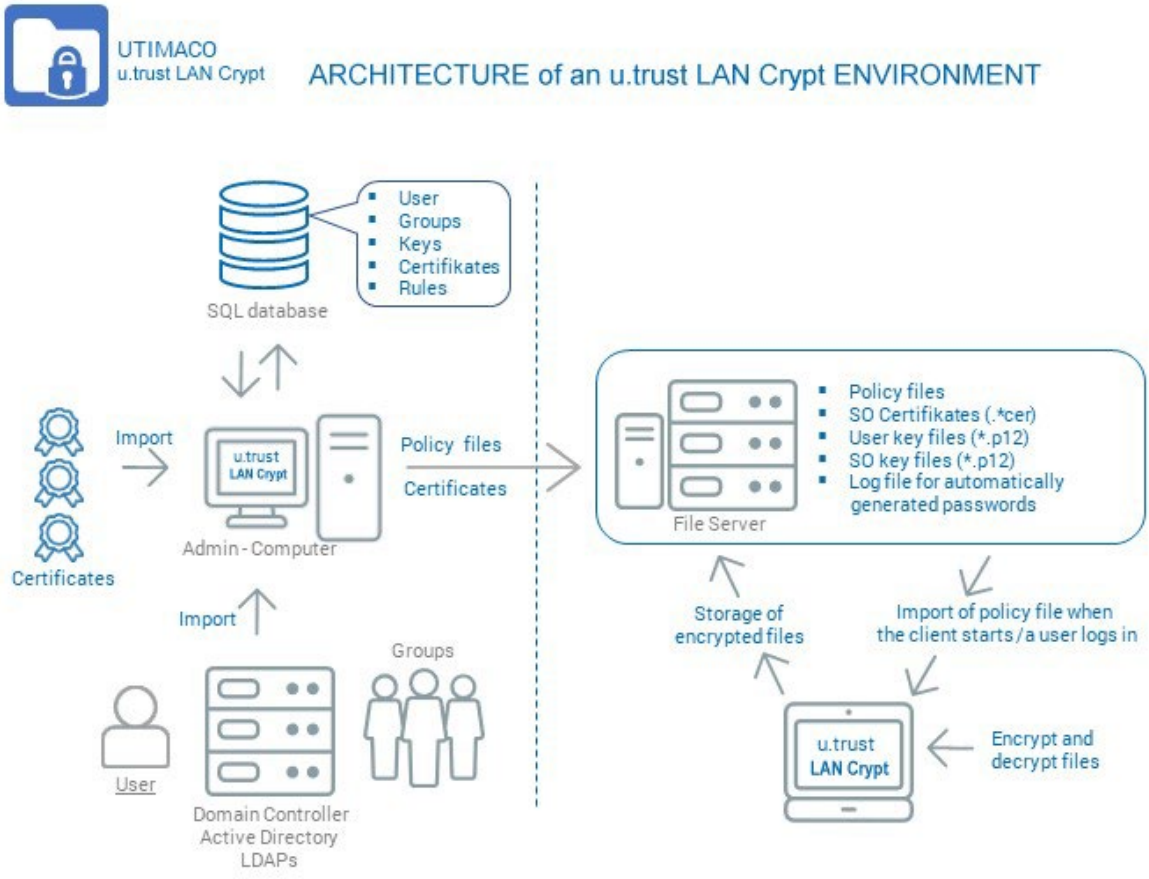
DLP 製品が暗号化が必要なデータを特定した場合、u.trust　LAN　Crypt　Client　API を使用してこれらのファイルを暗号化することができます。u.trust　LAN　Crypt 管理コンソールでは、使用する u.trust　LAN　Crypt キーを指定するさまざまな暗号化タグを定義できます。

クライアント API は、これらの定義済み暗号化タグを使用して、異なるコンテンツに特別なキーを適用することができます。たとえば、暗号化タグ<CONFIDENTIAL>を使用して、DLP 製品によって機密として分類されるすべてのファイルを暗号化することができます。

1.4 アーキテクチャ

u.trust LAN Crypt は 2 つのコンポーネントで構成されています。u.trust LAN Crypt 管理コンソールと u.trust LAN Crypt クライアントです。両コンポーネントは通常、Windows 10 (x64) または Windows 11 (x64) オペレーティングシステムを搭載した標準的なワークステーションコンピュータにインストールされます。セキュリティオフィサーは、u.trust LAN Crypt 管理コンソールを使って暗号化プロファイルを定義配布し、それをユーザーが利用できるようにします。

次の図は、各コンポーネントの相互作用と u.trust LAN Crypt が社内ネットワークにどのように統合されているかを示しています：



1.4.1 u.trust LAN Crypt の管理

管理コンポーネントには、u.trust LAN Crypt の中央管理に必要なツールが含まれており、1 人または複数のセキュリティオフィサーが使用します。インストールは通常、Windows 10 (x64) または Windows 11 (x64) をオペレーティングシステムとする 1 台以上のワークステーションコンピュータに行います。Windows Terminal Services または Citrix MetaFrame による中央管理が必要な場合は、u.trust LAN Crypt がサポートする Windows サーバーシステムへのインストールも可能です。これは特に大規模な環境、特に分散したロケーションで推奨

されます。u.trust LAN Crypt 管理コンソールシステムには、リモートデスクトップ（RDP）または独立コンピューティングアーキテクチャ（ICA）プロトコルでアクセスします。サポートされる Windows バージョンの詳細については、u.trust LAN Crypt リリースノートを参照してください。

u.trust LAN Crypt 管理コンソール機能とシステム管理機能は独立していなければ、保護すべきデータの最大限のセキュリティと機密性を保証することができないため、u.trust LAN Crypt はユーザー管理とグループ管理を分離しています。u.trust LAN Crypt が管理するユーザーとグループは、既存の Active Directory や他の LDAP ベースのディレクトリからインポートすることができます。

u.trust LAN Crypt 管理コンソールでは、設定データを保存し、u.trust LAN Crypt のユーザーとグループを管理するために SQL データベースが必要です。Microsoft SQL Server Express Edition を使用する場合、データベースは管理システムにローカルにインストールできます。複数のセキュリティオフィサーが存在する大規模なインストールでは、Microsoft SQL または Oracle サーバー形式の中央データベースシステムの使用をお勧めします。

セキュリティオフィサーは、組織で使用されるセキュリティポリシーを定義する責任があります。セキュリティオフィサーは、組織で使用されるセキュリティポリシーを定義し、そのポリシーが正しく実施、変更、遵守されるようにします。小規模の企業では、セキュリティオフィサーは通常一人です。u.trust LAN Crypt は、このような様々な階層レベルを表現し、反映させることができます。

u.trust LAN Crypt データベースが生成される際には、マスターセキュリティオフィサーが存在しなければなりません。これらのセキュリティオフィサーは最初のポリシーを定義し、セキュリティ問題に影響するアクションに 4 つの目のプリンシパルルール（認証には 2 人のセキュリティオフィサーが必要）を使用するかどうかを決定します。各セキュリティオフィサーには、基本的な権限を定義する特定の管理権限が割り当てられます。各セキュリティオフィサーの責任範囲は、アクセス制御リスト（ACL）により、いくつかのユーザーグループに限定することもできます。

u.trust LAN Crypt は、ユーザーのアクセス権を管理するために Key EnCryption Keys（KEK）を使用します。これらは暗号化されて SQL データベースに保存され、他のデータベースコンテンツと同様に、MAC とハッシュ値で変更から保護されています。管理タスクは、セキュリティオフィサーがキーの名前だけを知ることができ、実際の値を知ることができないように配置されています。つまり、キーオブジェクトを操作し、暗号化ルールを作成することができます。許可制御手順の柔軟性は、幅広いシナリオをカバーできることを意味します。例えば、セクション長がキーを定義し、フォルダを割り当てることができます。次の作業ステップでは、中央のセキュリティオフィサーが暗号化プロファイルを生成できます。その結果、キーは中央管理下に保たれます。

u.trust LAN Crypt は、自動的に生成される 2 つのキータイプ、ユーザーキーとグループキーを認識します。ユーザーキーは個々のユーザーのために生成され、ホームディレクトリやローカルフォルダ、テンポラリフォルダの暗号化など、一般的な暗号化ルールに使用できます。各ユーザーは正確に 1 つのユーザーキーを持ちます。ユーザーキーで保護されたデータを緊急に復旧する必要がある場合、セキュリティオフィサーはこの特定のキーを別のユーザーに割り当てる必要があります。このタイプの復旧には特別な管理権限が必要で、悪用されないように 4 人の目による校長ルール（2 人目の承認）とリンクさせることができます。同様のコンセプトがユーザーグループにもあります。これがグループキーです（特定キーの再割り当て参照）。

注意：マスターセキュリティオフィサーの証明書が破損した場合など、u.trust LAN Crypt 管理コンソールの緊急復旧については、3.5.10 章の復旧キータブを参照してください。

ポリシーファイルには、透過的暗号化に必要なすべてのルール、アクセス権、キーが含まれています。ユーザーがクライアントコンピュータにインストールされた u.trust LAN Crypt ソフトウェアを使用してデータを暗号化/復号化する前に、まずポリシーファイルに保存された暗号化情報にアクセスする必要があります。この場合、ポリシーファイルはファイルサーバーまたはドメインコントローラのネットログオン共有に保存されます。

注意： u.trust LAN Crypt のコンポーネントをファイルサーバーやドメインコントローラにインストールする必要はありません。しかし、u.trust LAN Crypt のユーザーグループとクライアントコンピュータの管理を容易にするために、管理用ワークステーション(RSAT)に管理コンソール付属の管理用テンプレートファイル(*.ADMX ファイル)をインストールすると便利です。これにより、u.trust LAN Crypt クライアントの最も重要な設定を簡単かつ明確に管理することができます。

ポリシーファイルは、証明書によって不正アクセスから保護されています。証明書の所有者のみが証明書に属する秘密鍵にアクセスできるため、この証明書を使用して関連する暗号化情報にアクセスできます。u.trust LAN Crypt は、スマートカード、USB トークン、または適切なハードウェアボードに保存された証明書の使用もサポートしています。

注意：スマートカードやトークンを使用しなくても、u.trust LAN Crypt を使用して証明書を保存することができます。

（ユーザーから見た）ポリシーファイルやその他の u.trust LAN Crypt 設定へのパスは、オペレーティングシステムのメカニズムによって識別されます。

u.trust LAN Crypt 信頼済みグループは、同じ暗号化プロファイルを持つ複数のユーザーで構成されます。各ユーザーのポリシーファイルは管理部で生成されます。ポリシーファイルに同じプロファイルが保存されているすべての u.trust LAN Crypt ユーザーは、認証グループのメンバーです。これらのユーザーは、暗号化やキー交換について心配する必要はありません。ポリシーファイルにアクセスできるだけで、そのファイルを閉じたり開いたりするたびに、データが透過的に暗号化または復号化されます。

1.4.2 u.trust LAN 暗号化クライアント

u.trust LAN Crypt クライアントは、暗号化を実行する Windows システム（PC、ワークステーション、ノートブック、ターミナルサーバー）にインストールします。クライアントコンポーネントには、暗号化と復号化に必要なフィルタドライバーの他に、様々なオプションコンポーネントがあります：

- 初回暗号化と明示的暗号化のためのエクスプローラ拡張機能。
- 暗号化ルールのロードと削除、暗号化の有効化と無効化のためのユーザーアプリケーション。
- クライアント上で有効なすべての設定とルールを表示するためのユーザーアプリケーション。これは例えばサポートケースにおいて重要です。
- 初回暗号化のためのユーザーアプリケーション。
- トークンサポートにより、トークンベースの証明書を使用して、保存された暗号化情報にアクセスできます。

u.trust LAN Crypt クライアントを起動すると、オペレーティングシステムのメカニズム（レジストリ設定、グループポリシー）を介して、PKCS#12 コンテナ（*.P12 ファイル）とポリシーファイルのあるフォルダにアクセスします。PKCS#12 コンテナに初めてアクセスする場合、ユーザーはセキュリティオフィサーから与えられた PIN を安全な方法で入力する必要があります。その後、ユーザー証明書はオペレーティングシステムのローカル証明書メモリに保存され、つまりロードされた Windows プロファイルにリンクされます。この証明書により、プロファイル暗号化キー - PEK を介してポリシーファイルの暗号化された部分にアクセスできます。クライアントコンポーネントがサポートするハードウェアベースのトークンに証明書が格納されている場合、トークンのロックが解除された後、暗号化と復号化にユーザーによる操作は必要ありません。

その後、u.trust LAN Crypt クライアントは、設定とキーを含むポリシーファイルをロードします。

2 はじめに

2.1 証明書

u.trust LAN Crypt は、証明書と公開キー/秘密鍵のペアを使用して、ポリシーファイルに保存された暗号化情報を保護します。証明書の所有者だけが、その証明書に属する秘密鍵にアクセスすることができ、したがって、暗号化情報にアクセスするためにそれを使用することができます。

注意：有効期間が数百年、あるいは千年を超える証明書は使用しないでください。

情報セキュリティの観点から、証明書の有効期間はできれば 5 年を超えないようにすべきです。一方、CA 証明書（認証局）については、Utimaco は最長 20 年の有効期間を推奨しています。

どの証明書が使用可能で、その証明書はどこから入手できますか：

- 企業は、独自の公開キー基盤（PKI）を持つか、トラストセンターを使用してユーザーの証明書を作成します。この場合、既存の証明書を使用できます。
- または、u.trust LAN Crypt 管理コンソールコンポーネントが自己署名証明書を生成することもできます。これらの証明書は u.trust LAN Crypt でのみ使用できます。また、証明書にはクリティカルエクステンション(OID)が付与され、アプリケーションに使用してはいけないことを示すことができます。これらは X.509 標準に準拠したシンプルな証明書（Class-1 証明書に相当）です。

u.trust LAN Crypt では、新しく生成された証明書に重要な拡張子を追加するかどうかを設定できます。

注意： 状況によっては、他のアプリケーションが u.trust LAN Crypt 証明書の Critical Extensions を無視することがあります。これにより、これらの自己署名証明書で問題が発生します。このような場合、u.trust LAN Crypt 証明書が他のアプリケーションで使用されないように、Microsoft 管理コンソールの証明書スナップインを使用して、u.trust LAN Crypt 証明書のすべての使用領域を明示的に無効にする必要があります。

注意：新しく生成された証明書に重要な拡張子を追加するように設定した場合、そのような証明書は、証明書情報を表示すると、ステータスが表示されます：証明書に未知の拡張子が含まれており、その拡張子はクリティカルと表示されます。しかし、u.trust LAN Crypt は

自身の証明書の OID（オブジェクト識別子）を知っており、有効な証明書として認識するため、この情報を無視しても問題ありません。

証明書は、u.trust LAN Crypt 管理コンソールコンポーネント内でユーザーに割り当てられます。

証明書の使用方法に関する重要な情報

- u.trust LAN Crypt は、証明書の機能に Microsoft Crypto API のみを使用します。
- u.trust LAN Crypt は、特定の標準（例えば、RSA キー長が 2048 ビット以上）に準拠するすべての暗号サービスプロバイダ（CSP）をサポートしています。この中には、Microsoft Enhanced CSP などが含まれます。

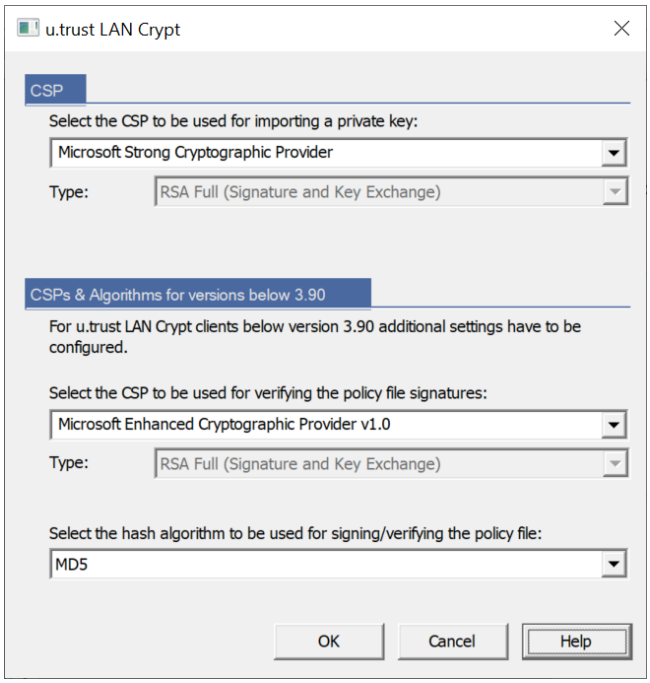
  注意：釈 Microsoft Standard CSP（Microsoft Base CSP）は使用できません。

  注意：釈 SHA-1 署名アルゴリズムは、Microsoft CSP ではサポートされなくなりました。

他の CSP との互換性に関してご質問がある場合は、サポートチームまでお問い合わせください（テクニカルサポートページ参照）。

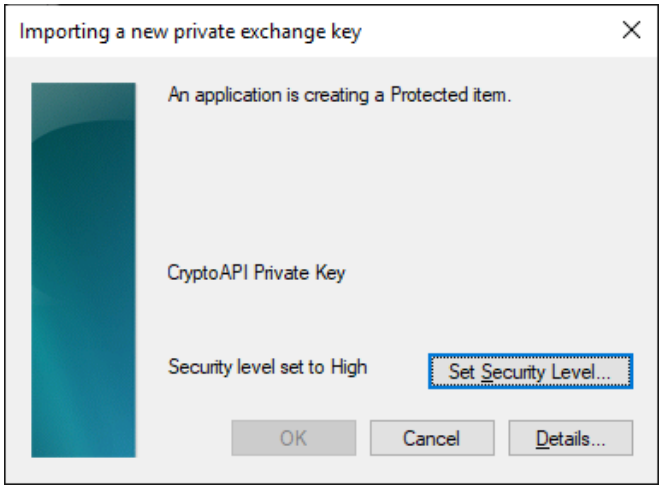
2.1.1 セキュリティレベル

u.trust LAN Crypt は可能な限り高いセキュリティを提供することを目的としているため、Microsoft Enhanced Cryptographic Provider v1.0（デフォルト設定）のような強力な CSP を使用する必要があります。これらの CSP は、大きなキー長の使用を可能にし、強力な暗号化アルゴリズムを提供するため、ポリシーファイルの確実な保護を保証します。



また、証明書のインポートウィザードを使用して証明書をインポートする場合は、以下のオプションを有効にする必要があります：強力な秘密鍵保護を有効にします。

証明書のインポート ウィザードで[終了]をクリックすると、[新規秘密鍵のインポート] ダイアログが表示されます。セキュリティレベルの設定]をクリックして、セキュリティレベルを再度設定します。



- 高

  高を選択した場合は、秘密鍵を使用していることを確認するためにパスワードを入力する必要があります。次のダイアログボックスで、新しいパスワードを入力します。

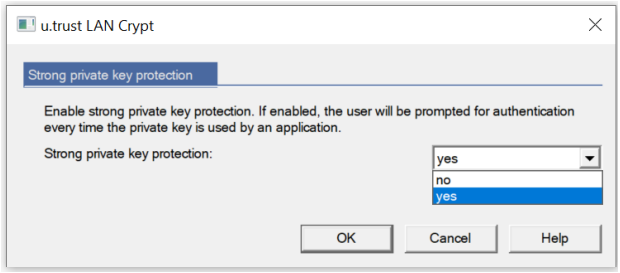
- 中

  中を選択すると、プロンプトが表示され、OK をクリックして秘密鍵の使用を確認するよう求められます。

アプリケーションで秘密鍵が使用されるたびに、セキュリティレベルの設定に応じて、パスワードの入力（高セキュリティレベル）または OK（中セキュリティレベル）のクリックを求めるプロンプトが表示されます。

自動的にインポートされる交換秘密鍵（*.p12、*.pfx）による最高レベルのセキュリティ

u.trust LAN Crypt では、証明書を自動的にインポートすることができます。これらの証明書の秘密鍵のセキュリティレベルを中または高に設定するには、u.trust LAN Crypt の設定で強力な秘密鍵保護をはいに設定する必要があります。

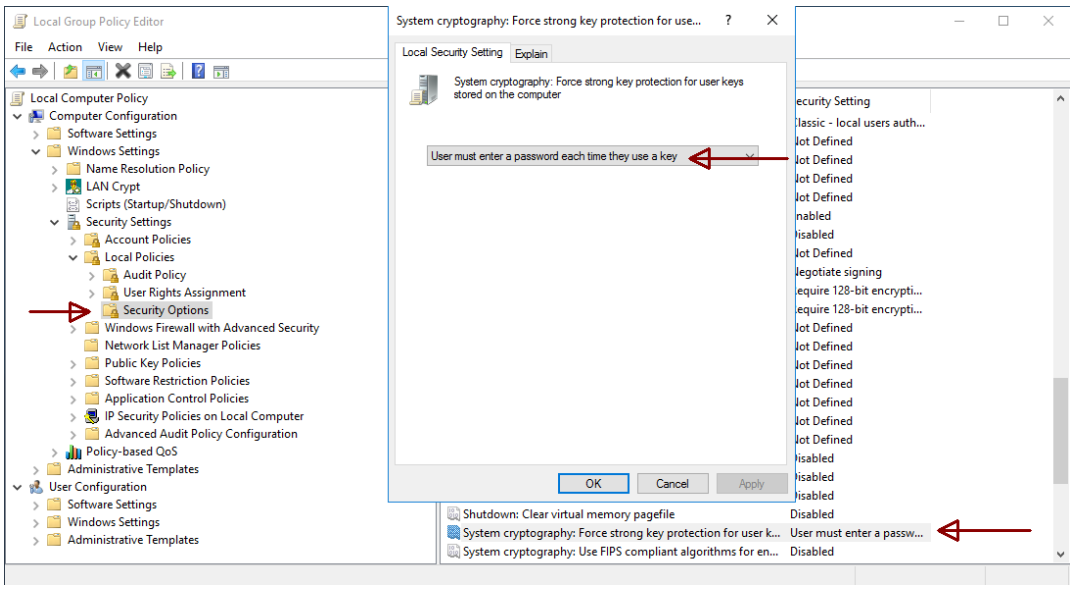


このオプションを有効にしないと、インポートされた証明書には自動的にセキュリティレベル低が使用されます。

このようにして、高いセキュリティレベルの証明書を強制的に発行し、全社的なセキュリティポリシーの中で実施できるようにすることができます。

注意：u.trust LAN Crypt のユーザーにとって、セキュリティレベルが高いということは、ログイン時と暗号化ルールが ″手動で ″ロードされる度に、秘密鍵のパスワードを一度入力しなければならないということです。

さらに、ローカルの Windows グループポリシーシステム暗号化を有効にします：また、ローカルの Windows グループポリシーシステム暗号化：コンピュータに保存されたユーザーキーの強力なキー保護を強制するを有効にし、ユーザーがキーを使用するたびにパスワードを入力する必要があるオプションを選択します。これにより、セキュリティレベルは常に高に設定されます。



スマートカード

スマートカードに保存された証明書を使用する場合、パスワードの入力は一度だけです。スマートカードがカードリーダーに収まっている限り、パスワードを再度入力する必要はありません。

注意：u.trust LAN Crypt 管理コンソールの初回起動前に、強力な秘密鍵保護オプションを有効にしておくことをお勧めします。有効にしていない場合、u.trust LAN Crypt で作成されたマスターセキュリティオフィサーの証明書は、セキュリティレベル高なしで使用されます。

注意：Windows はデフォルトで PIN を 24 時間キャッシュします。ソフトウェア証明書を使用すると、u.trust LAN Crypt 管理コンソールコンソール にログオンする際や、追加の認証が提供される際にセキュリティ上の問題が発生する可能性があります。この機能を無効にすることを強くお勧めします。

そのためには、以下の値を設定します。

″CachePrivateKeys″=dword:00000001
PrivateKeyLifetimeSeconds″=dword:00000005
″PrivKeyCacheMaxItems″=dword:00000000
PrivKeyCachePurgeIntervalSeconds″=dword:00000000

キーの場所

HKEY_LOCAL_MACHINE¥

SOFTWARE¥

Policies¥

Microsoft¥

Cryptography

値

"AllowCachePW"=dword:00000000

キーの場所

HKEY_LOCAL_MACHINE¥

SOFTWARE¥

Policies¥

Microsoft¥

Cryptography¥

Protect

この場合、PIN はキャッシュされません。

注意：CachePrivateKeys に 0、PrivateKeyLifetimeSeconds に 5 より小さい値を割り当てた場合、証明書（*.p12 ファイル）を Windows 証明書ストアにインポートする際に、（マスター）セキュリティオフィサーが PIN を 2 回入力する必要がある場合があります。

u.trust LAN Crypt で証明書を使用するための前提条件

- 証明書には公開キーが含まれていなければなりません。
- ユーザーが暗号化プロファイルにアクセスする前に、割り当てられた証明書の秘密鍵が利用可能でなければなりません。
- u.trust LAN Crypt は、個人証明書、その他の人々、Active Directory ユーザーオブジェクト証明書ストアのユーザー構成、および個人証明書証明書ストアのローカルコンピュータに保存されている証明書のみを一覧表示します。

  証明書管理コンソールのスナップインを使用して、証明書をインポートし、整理することができます。
- 証明書と u.trust LAN Crypt の暗号化情報の関連付けには公開キーのみが使用されます。秘密鍵を知る必要はありません。秘密鍵は証明書の所有者の所有物であり、暗号化情報にアクセスできる唯一の人物です。

u.trust LAN Crypt をインストールする前に、証明書を用意しておくことをお勧めします。証明書は u.trust LAN Crypt のインストール直後に証明書ダイアログに表示され、すぐに使用することができます。

注意：u.trust LAN Crypt は証明書を管理しません。しかし、企業独自の PKI インフラストラクチャを使用するか、トラストセンターを使用することで管理することができます。

2.1.2 証明書の検証

u.trust LAN Crypt は拡張証明書検証を行います。これは、証明書のチェーン全体（証明書失効リストの評価）がチェックされるまで、証明書が受理されないことを意味します。

これらの証明書については、拡張証明書検証が実施されます。

- マスターセキュリティオフィサーの作成時に提供される証明書の場合。チェックに合格した証明書のみが表示されます。
- セキュリティオフィサーに新しい証明書を割り当てるためにリカバリーキーが使用された後に作成された証明書の場合。全チェックに合格した証明書のみが表示されます。
- セキュリティオフィサーが u.trust LAN Crypt データベースにログオンするために使用する証明書の場合。証明書を確認できない場合、アクセスは拒否されます。
- 追加認証に使用される証明書の場合。

下記は、拡張証明書検証の前提条件です。

- 使用する証明書には CRL が含まれている。

  一部の PKI では、証明書自体に CRL を定義することができます。CRL が定義されている場合、そのリストが評価されます。この目的のために、ネットワークを介して発行者から CRL をダウンロードする必要がある場合があります。証明書が検証できない場合、暗号化プロファイルはロードされません。
- CRL がローカル証明書ストアにロードされている。

注意：CRL を評価するには、ネットワーク接続が必要な場合があります。この接続が確立できない場合、証明書自体は有効であっても、アクセスは拒否されます。

2.1.3 スマートカードリーダー

証明書の使用は暗号化サービスプロバイダー（CSP）を使用して処理されるため、スマートカード CSP を使用すると、スマートカードが自動的にサポートされます。そのため、スマートカードで証明書を使用することで、暗号化情報へのアクセスを処理できます。

注意：スマートカードで証明書を使用する場合は、スマートカードリーダー、関連ミドルウェア、および対応する暗号化サービスプロバイダー（CSP）が正しくインストールされ、動作していることを確認してください。

2.2 インストール

インストールは通常、Windows 10 (x64)または Windows 11 (x64)をオペレーティングシステムとする 1 台以上のワークステーションコンピュータに行います。Windows ターミナルサービスまたは Citrix MetaFrame による中央管理が必要な場合は、u.trust LAN Crypt がサポートする Windows サーバーシステムへのインストールも可能です。

注意：u.trust LAN Crypt のインストールは、Windows の管理者権限がある場合のみ可能です。

1. 解凍したインストールパッケージのインストールディレクトリに移動し、LCAdmin.msi ファイルをダブルクリックします。

u.trust LAN Crypt Admin のインストールは、インストールウィザードの案内に従って行います。次へをクリックします。

2. ライセンス契約ダイアログが表示されます。

   使用許諾契約書ダイアログで使用許諾契約書に同意します、を選択します。これを行わないと、u.trust LAN Crypt をインストールできません。次へをクリックします。

3. 宛先フォルダ］ダイアログが表示されます。

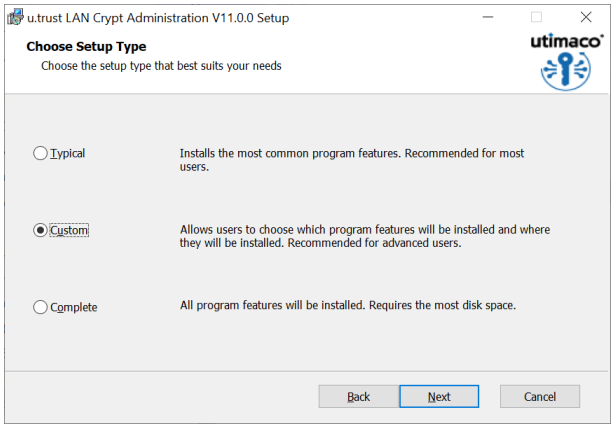
   u.trust LAN Crypt をインストールする場所を選択します。この設定を変更しない場合、インストールは以下の場所で行われます。

   <システムドライブ>:¥Program Files (x86)¥u.trust LAN Crypt¥Administration

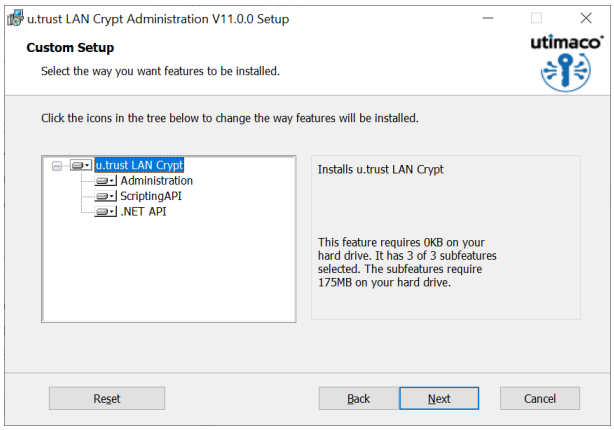
   次へをクリックします。

4. インストールタイプの選択ダイアログが表示されます。

   このダイアログで、インストールする u.trust LAN Crypt コンポーネントを選択できます。



カスタムを選択した場合は、インストールするコンポーネントを選択できます。



- 管理部門

  u.trust LAN Crypt 管理コンソール をインストールします。

- CryptAPI

製品を管理するために必要な u.trust LAN Crypt Scripting API をインストールします。

- .NET API

  .NET ベースのス Crypt またはアプリケーションを使用して製品を管理するために必要な u.trust LAN Crypt .NET API をインストールします。さらに、サンプルス Crypt もインストールされます。

  注意：.NET API を使用する際にエラーメッセージが表示される場合は、以下のパッケージリファレンスもプロジェクトに含まれているかどうかを確認してください：

  <パッケージ参照 Include="Microsoft.Win32.Registry" Version="5.0.0" />

  注意：インストールフォルダに含まれる MSI パッケージではなく、別のインストーラを使用して u.trust LAN Crypt 管理コンソールシステムをインストールする場合は、.NET API に必要なレジストリキーも設定する必要があります：

  [HKEY_LOCAL_MACHINE]
  "InstallDir"="C:¥Program Files (x86)¥Utimaco¥u.trust LAN Crypt¥Administration¥Administration¥Administration"

  InstallDir には、u.trust LAN Crypt 管理コンソールの DLL があるパスを入力します。デフォルトでは、上記のパスになります。

  u.trust LAN Crypt をデフォルトのパスにインストールしていない場合、以下の点にご注意：ください。付属のサンプルス Crypt を使用する場合、ス Crypt 内の API DLL へのパスはインストールパスの変更に合わせて調整する必要があります。

  注意：.Net SDK は、プロジェクトを使用する場合にのみ必要で、Powershell には必要ありません。StartFirstHere サンプルプログラムは、デフォルトで.NET Core 8.0 用に事前定義されています。

5. インストールするコンポーネントを選択し、［次へ］をクリックします。

   注意：通常オプションを選択した場合は、管理コンソールのみがインストールされます。Complete を選択した場合は、u.trust LAN Crypt ScriptingAPI と.NET API もインストールされます。

6. 設定を確認したら、[アプリケーションのインストールを準備]ダイアログで[インストール]をクリックします。インストールが開始されます。

7. インストールに成功すると、ダイアログボックスが表示されます。このダイアログ ボックスで、[完了]をクリックしてインストールを完了します。

2.3 無人インストール

無人インストールとは、u.trust LAN Crypt を多数のコンピュータに自動的にインストールすることです。

インストールフォルダには、無人インストールに必要な LCAdmin.msi ファイルが含まれています。

2.3.1 インストールするコンポーネント

以下の一覧は、どのコンポーネントをインストールする必要があるか、および無人インストー ルでそれらを指定する方法を示しています。

このキーワードは、ユーザー操作なしでインストールを実行する場合に、AddLocal=の個々のコンポーネントをどのように指定しなければならないかを示しています。コンポーネントの個々のキーワード名は、大文字と小文字を区別します。

AddLocal= Administration

u.trust LAN Crypt 管理コンソール のみをインストールします。

AddLocal=Administration,ScriptApi

u.trust LAN Crypt 管理コンソールに加えて、Scripting-API もインストールされます。

AddLocal=Aministration,AdminApiDotnet

u.trust LAN Crypt 管理コンソールに加えて、ス CryptAPI (.NET) もインストールされます。

例

msiexec /i lcadmin.msi /qn AddLocal=Administration

この例では、u.trust LAN Crypt 管理コンソールのみがユーザーの操作なしでインストールされます。

注意： コンポーネントを指定しないと、完全なインストールが実行されます。

注意： .NET API (AdminApiDotnet) をインストールすると、サンプル ス Crypt もインストールされます。デフォルトでは、インストールは 64 ビット版の下で行われます：

<Drive>:¥Program FilesUtimaco ¥u.trust LAN Crypt ¥Admin API PowerShell Samples

<Drive>:¥Program FilesUtimaco ¥u.trust LAN Crypt ¥Admin API Dotnet Samples

32 ビット版の場合は

<Drive>:¥Program Files (x86)¥Utimaco ¥u.trust LAN Crypt ¥Administration ¥Admin API PowerShell Samples

<Drive>:¥Program Files (x86)¥Utimaco ¥u.trust LAN Crypt ¥Admin API Dotnet Samples

注意：.NET API に関する詳細な注意：事項も参照してください。

2.3.2 コマンドライン構文

無人インストールを実行するには、特定のパラメータを指定して msiexec を実行する必要があります。

必須パラメータ

/I

インストールするパッケージを指定します。

/QN

ユーザーの操作を必要としないインストール（無人セットアップ）。

.msi ファイルの名前： lcadmin.msi

構文: msiexec /i <パス></lcadmin.msi /qn

オプションパラメータ

/L*xv <パス + ファイル名>。
<path + filename> で指定された場所にインストール手順全体をログに記録します。

例

msiexec /i C:¦Install¦cadmin.msi /qn /L*xv c:¦Log¦log.txt

これにより u.trust LAN Crypt の完全なインストールが行われます。プログラムはデフォルトのインストールディレクトリ

(<システムドライブ>:¦Program Files (x86)¦Utimaco¦u.trust LAN Crypt¦Administration)。

.msi ファイルは u.trust LAN Crypt インストールパッケージの Install フォルダにあります。

2.4 アップグレード

LAN Crypt 3.97、4.0.x、4.1.x を u.trust LAN Crypt 管理コンソールにアップグレードするには、以下の手順が必要です：

- バージョン 4.2.0 へのアップグレード
- 新バージョンのインストール
- 既存データベースのアップグレード

注意：バージョン 3.97 より古い LAN Crypt を使用している場合は、まずバージョン 3.97 にアップグレードする必要があります。

注意：アップグレード後の最初のログオンは、マスターセキュリティオフィサーが行う必要があります。

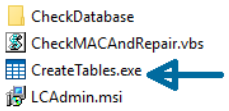
2.4.1 新バージョンのインストール

説明に従って新しいバージョンをインストールしてください。

注意：新しいバージョンをインストールする前に、LAN Crypt 管理コンソールのすべてのインスタンスが終了していることを確認してください。

2.4.2 既存の u.trust LAN 暗号データベース構造のアップグレード

コマンドラインツール CreateTables.exe を使用すると、u.trust LAN Crypt データベースのテーブル構造をアップグレードできます。このツールは、インストールパッケージの /Install フォルダにあります。



既存の u.trust LAN Crypt データベース構造のアップグレードには、高度なデータベース権限（db role: db_ddladmin）が必要なため、IT 管理者またはデータベース管理者によるアップグレードをお勧めします。CreateTables.exe によるデータベースのアップグレードでは、u.trust LAN Crypt データベースに新しいテーブルを作成し、特に DDL トリガを削除する必要があります。

注意：データベースへのログオンは、データベーススキーマの作成と変更が可能な権限で実行する必要があります。ただし、セキュリティオフィサーが u.trust LAN Crypt 管理コンソールコンソールを使用するには、データベースロール db_datareader と db_datawriter で十分です。

コマンドラインの構文

テーブルの作成 <ODBCName[.OwnerName]> <SQL 方言> <アクション>

CreateTables.exe には、その他の構成でテーブルを作成するための以下のパラメータが用意されています。

ODBCName

ODBC データソースに使用される名前。

OwnerName

データベースを正しく管理するには、Oracle データベースの場合、データベースの所有者を指定する必要があります。所有者は大文字で指定する必要があります。Microsoft SQLServer のデフォルトスキーマ が .dbo に対応していない場合は、Microsoft SQL データベースのデータベース所有者.dbo を指定する必要があります。

SQL 方言

m ...Microsoft SQL Server 2019 または 2022

o19 ... Oracle 19 以降

アクション

u ...データベース構造の更新

例 1：

テーブルの作成 SGLCSQLServer.dbo m u

例 2：

テーブルの作成 SGLCSQLServer.SGLC o19 u

注意：u.trust LAN Crypt Admin を初めてインストールする場合は、CreateTables.exe に他のパラメータを設定する必要があります。詳しくは、3.2.3 項 u.trust LAN Crypt データベースのテーブル作成を参照してください。

2.4.3 3.61 未満のバージョンのサーバーログオン資格情報

バージョン 3.97 への中間アップグレード後は、サーバーページの中央設定でログイン情報を再度入力する必要があります。Microsoft のディレクトリサービスを使用している場合は、以下のようにしてください。

- ドメインまたはサーバー名］にドメイン名を入力します。
- ユーザー名を username@Domainname と入力します。

2.5 言語設定

u.trust LAN Crypt 管理コンソールは以下の言語をサポートしています。

- 英語
- フランス語
- ドイツ語
- 日本語

u.trust LAN Crypt の言語設定は Windows の現在の言語設定に依存します。言語がサポートされていない場合、u.trust LAN Crypt はデフォルトでダイアログを英語で表示します。

または、u.trust LAN Crypt の言語を自分で設定することもできます。その場合は、u.trust LAN Crypt 管理コンソールがインストールされているコンピュータのレジストリを以下のように変更してください。

[HKEY_LOCAL_MACHINE]

"LCID"=dword:0x0409

アメリカ英語

"LCID"= dword:0x40C

フランス語

"LCID"= dword:0x0407

ドイツ語

"LCID"=dword:0x0411

日本語

その後、コンピュータを再起動してください。

手動で設定した u.trust LAN Crypt の言語は、Windows で異なる言語が設定または変更されても保持されます。

2.6 アンインストール

注意：u.trust LAN Crypt をアンインストールできるのは、Windows の管理者権限を持っている場合のみです。

1. スタート→設定→アプリを選択します。

2. インストールされているプログラムの一覧から、u.trust LAN Crypt 管理コンソールを選択します。

3. u.trust LAN Crypt 管理コンソール をアンインストールするには、［アンインストール］をクリックします。

4. u.trust LAN Crypt 管理コンソールツールをアンインストールする場合は、表示される警告メッセージを確認し、[OK]をクリックしてください。

5. システムを再起動すると、アンインストールが完了します。

注意： u.trust LAN Crypt をアンインストールしても、u.trust LAN Crypt データベースの内容は保持されます。必要に応じて、オペレーティングシステムツールまたはデータベース管理ツールを使用してデータベースを個別に削除する必要があります。また、すべてのユーザー固有の設定（レジストリキー、グループポリシー設定など）もシステムに残ります。

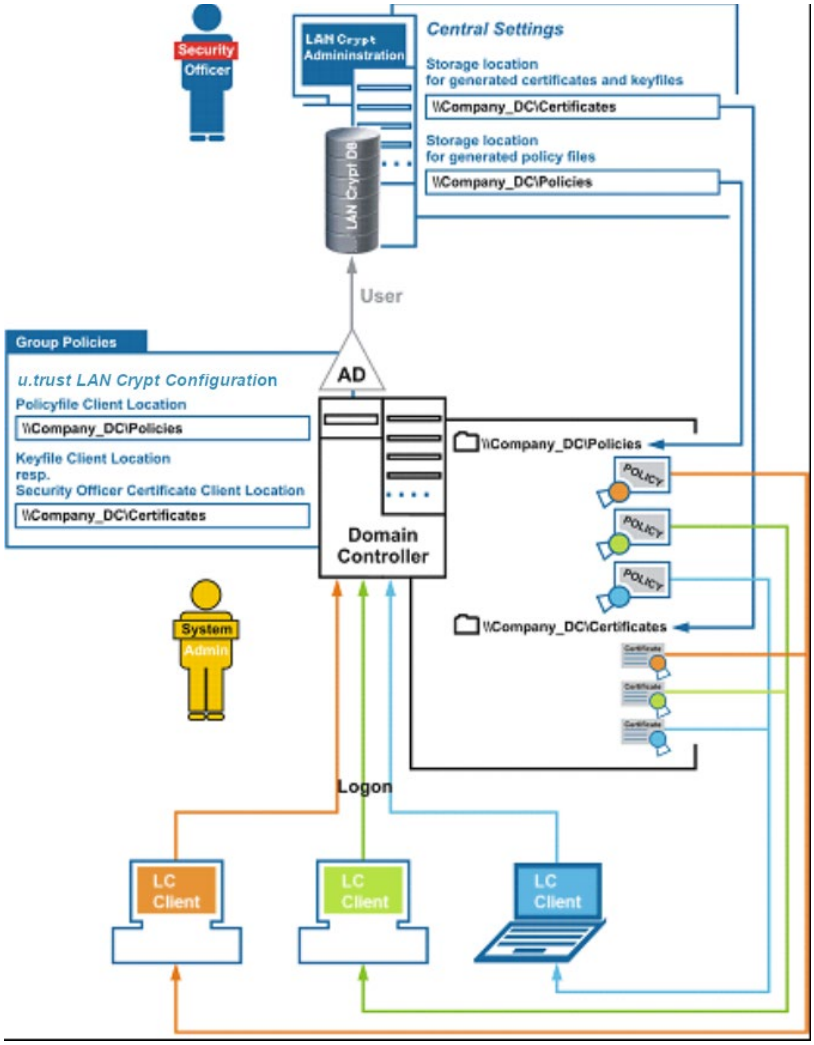
3 管理

u.trust LAN Crypt 管理コンソールは、Microsoft の管理コンソール（MMC）にシームレスに統合され、セキュリティオフィサーに典型的な MMC 機能を備えた信頼できるユーザーインターフェースを提供します。

管理コンソールは、既存の Windows レプリケーションツールを活用できるように開発されました。これは高い効率性を実現するだけでなく、総所有コスト(TCO)を削減することにもつながります。

通常、u.trust LAN Crypt 管理コンソールコンソールは別のマシンにインストールされ、そこから必要なディレクトリサービスと u.trust LAN Crypt データベースにアクセスできます。

u.trust LAN Crypt はセキュリティオフィサーのコンセプトを採用しています。最初に管理コンソールをインストールするマスターセキュリティオフィサーは 1 人です。インストール中、マスターセキュリティオフィサーは、ユーザー用に生成された証明書とキーファイル（セキュリティオフィサーの証明書のパブリック部分と、クライアントマシンにインポートされるユーザー証明書を含む*.p12 ファイル）の保存場所を指定する必要があります。インストール後、ユーザー用に生成されたポリシーファイルの保存場所を指定する必要があります。暗号化ルールを含むポリシーファイルは、ユーザーごとに生成されます。



証明書、*.p12 ファイル、ポリシーファイルは、指定されたストレージロケーションから、後の時点 でクライアントによって自動的にインポートされます。

したがって、クライアントはこれらのディレクトリにアクセスできなければなりません。マスターセキュリティオフィサーとシステム管理者は、これらのディレクトリ（通常は共有ネットワークフォルダ）を定義するために協力しなければなりません。

クライアントは、ドメインコントローラにログオンするときにグループポリシーを使用して、これらのファイルへのアクセス方法を調べることができます。システム管理者は、u.trust LAN Crypt 設定コンソールで保存場所を指定します。u.trust LAN Crypt は、ユーザーに対して有効なグループポリシーオブジェクトに設定されます。

u.trust LAN Crypt クライアントは、u.trust LAN Crypt データベースに接続する必要はありません。

証明書、*.p12 ファイル、およびポリシーファイルを見つけるために必要な情報は、ログオン時にグループポリシーで見つけることができます。これらのファイルは自動的にクライアントに転送されます。

証明書をインポートするには、ユーザーのパスワードが必要です。u.trust LAN Crypt で生成された証明書の場合、p12pwlog.csv ファイルにパスワードが含まれており、例えば PIN を作成するのに使用できます。

3.1 必要なステップ

準備：

- オプション：DBMS（Microsoft または Oracle）のインストール。新しいデータベース"LANCrypt "の作成。DBMS に追加されたデータベースは u.trust LAN Crypt には使用しないでください。
- システム DSN としてデータソース（32 ビット ODBC）を追加します（3.2.2 章参照）。
- CreateTables を使用してデータベーステーブルを作成します（または、アップグレード中にテーブルを拡張します)。
- システム管理者 u.trust LAN Crypt 設定コンソールで設定を定義します。
- マスターセキュリティオフィサーの作成
- 管理コンソールでストレージの場所を定義します。
  - u.trust LAN Crypt で生成されたユーザーキーファイルとセキュリティオフィサー証明書の場合
  - u.trust LAN Crypt によって生成されたセキュリティオフィサキーファイル用
  - 自動生成されたキーファイルのパスワードログファイル（u.trust LAN Crypt で証明書を生成した場合のみ)
  - u.trust LAN Crypt によって生成されたポリシーファイル（これらの手順を実行するには、Windows システム管理者にお問い合わせください。）

注意：Oracle データベースを使用していて、異なるマシンの Administration Consoles からデータベースにアクセスする場合は、コードページの設定も指定する必要があります（データベースタブを参照）。

- セキュリティオフィサーの増員
- オフィサーの権限の定義
- ディレクトリサービス（Active Directory など）からのオブジェクト（組織単位、グループ、ユーザー）のインポート
- u.trust LAN Crypt グループを作成し、ディレクトリサービスからインポートしたオブジェクト（ユーザー、グループ）を入れます。
- u.trust LAN Crypt グループと担当セキュリティオフィサーを各組織単位またはリージョンに割り当て、権限を定義します。
- キー作成
- 暗号化ルールの作成

  注意： u.trust LAN Crypt グループでのみ暗号化ルールを定義することをお勧めします。直接インポートされたディレクトリオブジェクトの暗号化ルールは、セキュリティ上のリスクがあり、エラーも発生しやすくなります。

- ユーザーに対する証明書の生成と割り当て
- ユーザーのポリシーファイルを生成します。

3.2 u.trust LAN Crypt を管理するための準備

インストール後、u.trust LAN Crypt の管理を開始するには、以下の手順を実行する必要があります。

- オプション：データベース管理システムのインストール

これは、u.trust LAN Crypt の管理に使用するデータベースがデータベースシステムに含まれていない場合にのみ必要です。

u.trust LAN Crypt は以下のデータベースシステムをサポートしています。

- Microsoft SQL Server 2019（Express を含む）
- Microsoft SQL Server 2022（Express を含む）
- Oracle 19 以降

  注意： Oracle データベースを使用している場合、u.trust LAN Crypt 管理コンソール機能を使用する前に Oracle クライアントをインストールする必要があります。Oracle クライアントの ″runtime ″バリアントを選択した場合、Oracle ODBC ドライバーもインストールする必要があります。

  u.trust LAN Crypt は Microsoft ODBC for Oracle をサポートしていません。

  データベースオブジェクトを生成する際には、メーカーが予約したキーワードを使用しないようにしてください。

- データソースの指定（ODBC）

  独自のデータベースシステムを使用する場合は、データソースを指定できるように、使用するデータベースのアクセスデータを知っておく必要があります。

- データベーステーブルの作成

  データソースを指定した後、ソフトウェアに付属のツール（CreateTables.exe）を使用して、データベースに u.trust LAN Crypt テーブルを作成する必要があります。

3.2.1 データベースシステムのインストール

以下の説明では、Microsoft SQL Server 2022 Express Edition について説明します。この例示的な説明では、このバージョンのデフォルト設定をできるだけ使用しています。

データベースシステムをインストールするには、次のようにします：

1. Microsoft SQL Server Express の最新バージョン（Microsoft SQL Server 2022 Express など）を Microsoft Web サイトからダウンロードします。次に、ダウンロードフォルダ内のインストールファイルをダブルクリックします。

   Microsoft SQL Server 2022 Express の場合、SQL2022-SSEI-Expr.exe になります。

   注意：64 ビットオペレーティングシステムを使用している場合は、www.microsoft.com から 64 ビットバージョンの Microsoft SQL Server 2022 Express Edition をダウンロードしてください。

2. 使用許諾契約に同意し、[次へ]をクリックします。

3. インストールファイルが解凍され、インストールウィザードが起動します。

4. インストールウィザードの指示に従って、デフォルト設定を了解します。

デフォルト設定：以下の準備手順の説明は、デフォルト設定を参照しています。変更した場合（認証方法、データベースインスタンス)、データソースの指定とデータベーステーブルの作成時にそれを考慮する必要があります。

データベース認証：デフォルトでは、Express Edition は Windows 認証を使用します。Windows 認証を使用する前提条件として、データベースにログオンするユーザーが Windows 管理者権限を持っている必要があります。

マスターデータベース：デフォルトでは、データソースを指定する際に既存のマスターデータベースが使用されます。一般的に、Express Edition や SQL Server のバージョンをアップグレードする際に問題が発生する可能性があるため、マスターデータベースを使用しないことをお勧めします。

u.trust LAN Crypt 用に別のデータベースを作成し、データソースの追加時に指定することができます。Microsoft SQL Server 2022 Express Edition の場合、コマンドラインで以下のコマンドを使用してデータベースを作成できます：

osql -E -S . ¥SQLEXPRESS -Q "CREATE DATABASE <データベース名>"

Windows 認証を使用する指定された名前のデータベースが作成されます。

例えば、パラメータ -U を使用すると、認証用のユーザー名を指定できます。すべてのパラメータを表示するには、osql -?

別のバージョンの Microsoft SQL Server Express を使用することもできます（u.trust LAN Crypt バージョン 11.0.0 は、バージョン 2019 から Microsoft SQL Server Express をサポートしています）。

また、Microsoft SQL Server Management Studio Express を無料でダウンロードし、それを使って別のデータベースを作成することもできます。

次のステップでは、u.trust LAN Crypt がデータベースシステムを使用できるように、データソースを指定する必要があります。

3.2.2 データソースの追加（ODBC）

注意：データソースは、64 ビット システムでも使用できる 32 ビット ODBC データソース アドミニストレータを使用して追加する必要があります。u.trustLANCrypt 管理コンソール(x86)を起動をクリックして、ODBC Data Source Administrator を起動します。これにより、正しいバージョンが起動されます。

u.trust LAN Crypt がデータ管理システム経由でデータベースを使用できるように、データソースを指定します。それには、ODBC データソース管理者を使用します。

ODBC（Open Database Connectivity）は、様々なデータベース管理システム上のデータにアクセスすることを可能にします。例えば、SQL データベースのデータにアクセスするプログラムがある場合、ODBC を使えば、同じプログラムを使って別のデータベースのデータにアクセスすることができます。これを行うには、システムにドライバーを追加する必要があります。ODBC は、このようなドライバーの追加や設定をサポートします。

データソースを追加するには、以下を行います。

1. StartSettings ➢Control Panel ➢Administrative Tools ➢Data Sources（ODBC）を選択します。ODBC Data Source Administrator が開きます。

2. システム DSN]タブを選択し、[追加...]をクリックします。

データソースを追加できるリストが表示され、それぞれ独自のシステム DSN（システムデータソース名）を持ちます。これらのデータソースはコンピュータにローカルに保存されますが、特定のユーザーに割り当てられることはありません。

3. データソースを作成するドライバーとして SQL Server を選択し、終了をクリックします。

注意：SQL-Server ネイティブクライアントがリストにある場合は、このエントリーを選択してください。u.trust LAN Crypt 管理コンソールと SQL サーバー間の接続を保護するため、"ODBC Driver 17 for SQL-Server "またはそれ以降のバージョンの使用をお勧めします。このドライバーは TLS 1.2 による接続の暗号化を可能にし、より高いセキュリティを提供します。https://go.microsoft.com/fwlink/?linkid=2120137 からダウンロードできます。

4. データソースを参照する SGLCSQLServer 名を入力するダイアログが表示されます。

データソース参照名は、u.trust LAN Crypt Configuration で設定します。デフォルト設定は SGLCSQLServer です。別の名前を使用する場合は、設定に入力します。

注意：ODBC ソースの名前は大文字と小文字を区別します。ここでは、u.trust LAN Crypt 設定で指定したのと全く同じ方法で名前を入力する必要があります。u.trust LAN Crypt 管理コンソールコンソールを初めて起動する前に、設定に名前を入力する必要があります。

5. サーバー］フィールドで、接続の確立に使用するサーバーを選択し、［次へ］をクリックします。

6. 次のダイアログでデフォルト設定を了解します。Windows NT 認証を使用するオプションをオンにすると、データベース システムへのログオンに Windows ユーザーのデータが使用されるように指定します。パスワードを入力する必要はありません。次へをクリックします。

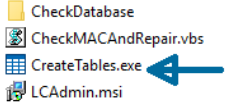
7. デフォルトのデータベースとして、u.trust LAN Crypt 用に作成したデータベース（例：LANCrypt）を選択し、確認します。

8. 次のダイアログで、デフォルト設定を了解し、終了をクリックします。

3.2.3 u.trust LAN Crypt データベースのテーブルの作成

コマンドラインツールの CreateTables.exe を使用して、u.trust LAN Crypt データベースに必要なテーブルを作成します。

このツールは、解凍したインストールパッケージの Install ディレクトリにあります。



注意：データベースへのログオンは、データベーススキーマの作成と変更を許可する権限で実行する必要があります。

データベースにテーブルを作成するには、次のようにします：

Microsoft SQL Server を使用している場合は、コマンドラインに次のように入力します：

テーブルの作成 SGLCSQLServer.dbo m c

インストール時にデフォルトを使用した場合、データベースシステムの設定はこれで完了です。これで u.trust LAN Crypt 管理コンソールを開始できます。

3.2.3.1 CreateTables コマンドラインの構文

テーブルの作成 <ODBCName[.OwnerName]> <SQL Dialect> <アクション>

CreateTables.exe には、さまざまな構成でテーブルを作成するための以下のパラメータが用意されています。

ODBC Name

ODBC データソースに使用した名前。

Owner Name

データベースを正しく管理するには、Oracle データベースの場合、データベースの所有者を指定する必要があります。所有者は大文字で指定する必要があります。Microsoft SQL Server のデフォルトスキーマが.dbo に対応していない場合は、Microsoft SQL データベースのデータベース所有者.dbo を指定する必要があります。

SQL の方言

m ...Microsoft SQL サーバー

o19 ... Oracle 19 以降

アクション

c ...すべてのテーブルを作成

例 1：

テーブルの作成 SGLCSQLServer.dbo m c

例 2：

テーブルの作成 SGLCSQLServer.SGLC o19 c

3.3 マスターセキュリティオフィサー

u.trust LAN Crypt はセキュリティオフィサーの概念を採用しています。最初はマスターセキュリティオフィサーが一人いますが、後に追加のセキュリティオフィサーを作成し、u.trust LAN Crypt の管理に関する特定の権限を割り当てることで、タスクを委任することができます。最初のマスターセキュリティオフィサーは、さらにマスターセキュリティオフィサーを作成することもできます。

ACL は、マスターセキュリティオフィサーが作成したセキュリティオフィサーに割り当てられた権限を定義するために使用されます。個々のセキュリティオフィサーは、中央管理部門の異なる組織単位に割り当てることができます。セキュリティオフィサーの権限は、割り当てられた組織ユニットにのみ適用されます。これらの権限は、他の権限が割り当てられるまで、組織階層の下層に継承されます。

データベースシステムとデータソースを設定した後、u.trust LAN Crypt 管理コンソールコンソールを初めて起動すると、次にマスターセキュリティオフィサーを作成します。

マスターセキュリティオフィサーは、常に既存のすべての権限を持っています。

注意：マスターセキュリティオフィサーの初回作成時に、u.trust LAN Crypt で生成された証明書とキーファイルの保存場所も定義する必要があります。クライアントが必要とするセキュリティオフィサーの証明書の公開部分（*.cer）もここに保存されます。ユーザー証明書（*.p12 ファイル）も後でこのディレクトリからインポートされます。システム管理者で定義したフォルダは、すでに利用可能（ネットワーク共有）になっているはずです。

マスターセキュリティオフィサーの作成時に設定した内容は、u.trust LAN Crypt 管理コンソールコンソールの中央設定で変更することができます。

3.3.1 初回マスターセキュリティオフィサー

管理機能が初めて実行され（スタート→u.trust LAN Crypt 管理コンソール→管理コンソール）、データベースにログオンすると、最初のマスターセキュリティオフィサーを作成するためのウィザードが表示されます。

初回マスターセキュリティオフィサーのデータを入力します。ここで入力した名前は、u.trust LAN Crypt で生成された証明書を使用する場合、証明書のコモンネームとして使用されます。メールアドレスとコメントは任意です。次へをクリックします。

注意：u.trust LAN Crypt で生成された証明書のパスワードログファイルにメールアドレスが追加されます。例えば、電子メールで PIN を作成する場合などに利用できます。

ウィザードの 2 番目のダイアログで、以下の保存場所を指定します。

- 生成された証明書(*.cer)とキーファイル(*.p12)
- セキュリティオフィサーの証明書
- 生成されたキーファイルの自動生成パスワードのログファイル

生成された証明書とキーファイルの保存場所

u.trust LAN Crypt は、必要に応じて自己署名証明書を生成することができます。この方法で生成されたキーファイル(*.p12)には秘密鍵と証明書が含まれています。これらは、ユーザーに証明書を割り当てる際に生成されます。関連する保存場所は、アシスタントの 2 番目のダイアログで指定する必要があります。一般的に、これはこれらのファイルがユーザーに利用可能になるネットワーク共有です。

セキュリティオフィサー証明書の公開部分（*.cer）もここに保存されます。

ユーザーは、キーファイルまたは証明書（*.p12）、ポリシーファイル、およびポリシーファイルを作成し署名したセキュリティオフィサーの証明書の公開部分（*.cer ファイル）を提供する必要があります。

u.trust LAN Crypt クライアントの設定には、グループポリシーまたはレジストリ設定を使用します（Active Directory がない場合、またはセキュリティ上の理由で使用しない場合）。

これらの設定により、クライアントは適切なアクセスパスを取得します。UNC パスと FQDN 名の使用をお勧めします。

セキュリティオフィサー証明書の公開キーを含む対応する*.cer ファイルが見つかれば、自動的にインポートされます。

注意：この機能を使用するには、u.trust LAN Crypt 設定で対応するパスを設定する必要があります。

または、ユーザーのキーファイルとセキュリティオフィサー証明書のパブリック部分を手動で配布することもできます。この場合、クライアントによって両方がインポートされていることを確認してください。

注意：ポリシーファイルを作成したセキュリティオフィサーの公開証明書は、クライアントによって常にインポートされる必要があります。

セキュリティオフィサーの公開証明書(*.cer)とユーザーのキーファイル(*.p12)が保存されているパスを変更した場合、例えばセキュリティオフィサーを追加作成した後に、これらのファイルを新しい場所にコピーする必要があります。そうしないと、u.trust LAN Crypt クライアントがセキュリティオフィサーの証明書のパブリック部分を見つけることができません。ユーザーのキーファイルも新しいパスで生成する必要があります。

作成されたセキュリティオフィサー証明書の保管場所

u.trust LAN Crypt は、セキュリティオフィサーの証明書をバックアップ用などに*.p12 ファイルに保存します。ここで、保存先のフォルダを指定できます。

注意：機密データを扱うため、不正アクセスから保護することが不可欠です。

パスワードログ用ファイル

ここでは、生成された PKCS#12 ファイルのパスワードログファイルの保存場所と名前を指定できます（デフォルト名：p12pwlog.csv）。このファイルには、生成された PKCS#12 キーファイル (*.p12)のパスワードが含まれます。これは、たとえば、PIN の作成にも使用できます。

注意： このファイルを保護し、いかなる場合でもポリシーファイルと同じフォルダに保存しないでください。

u.trust LAN Crypt を使用すると、パスワードログファイルを簡単に保護できます。そのためには、管理コンソールとクライアントを同じコンピュータにインストールします。最初のマスターセキュリティオフィサーを作成した後、パスワードログファイルを暗号化する暗号化ルールを作成し、最初のマスターセキュリティオフィサーのプロファイルを作成し、プロファイルをロードします。使用する暗号化キーは、マスターセキュリティオフィサーと証明書を作成する権限を持つセキュリティオフィサーのみが使用できます。

注意：u.trust LAN Crypt コンポーネントの管理コンソールとクライアントアプリケーションを同じコンピュータにインストールする場合は、同じバージョンである必要があります。

初回暗号化ウィザードを実行すると、パスワードログファイルが暗号化されます。ファイルが暗号化されていない間に最初のマスターセキュリティオフィサーのパスワードが漏洩して

いないことを確認するために、新しい証明書を作成し、最初のマスターセキュリティオフィサーに割り当てます。

注意：証明書を割り当てるセキュリティオフィサーが、パスワードログファイルを変更するファイルシステムの権限を持っていない場合、u.trust LAN Crypt は証明書を生成することができません。

次へをクリックします。

証明書の有効期限

ウィザードの 3 つ目のダイアログで、u.trust LAN Crypt で生成した証明書の有効期間を指定し、既存の証明書または u.trust LAN Crypt で生成した証明書をセキュリティオフィサーに割り当てます。

u.trust LAN Crypt で生成された証明書を使用する場合、その証明書は指定された期間有効です。これ以降に生成された証明書もすべてこの有効期間を持ちます。

初回セキュリティオフィサー証明書

セキュリティオフィサーのデータを保護するために使用する暗号化証明書を選択する必要があります。また、セキュリティオフィサーが u.trust LAN Crypt 管理コンソールへの認証に使用する署名証明書を選択することもできます。署名証明書を指定しない場合、暗号化証明書も認証手段として使用されます。

参照...ボタンをクリックして既存の証明書を選択するか、u.trust LAN Crypt に新しい証明書を生成させます。次のダイアログで、[新しい証明書]をクリックします。リストから新しい証明書を選択し、[OK]をクリックします。

注意：既存の証明書を使用する場合は、この証明書が利用可能である必要があります。ソフトウェア証明書を使用する場合は、証明書ストアにロードする必要があります。証明書がトークンに保存されている場合は、トークンがシステムに接続されている必要があります。証明書をインポートするには、［証明書のインポート］をクリックします。

次へをクリックします。

ウィザードの 4 番目のダイアログで、適切な接頭辞を持つリージョンを入力できます。u.trust LAN Crypt はキーを生成する際、この接頭辞をキー名の先頭に付けます。キーを生成したセキュリティオフィサーに割り当てられたリージョンの接頭辞を常に使用します。この接頭辞により、キーがどの管理単位で使用されるかが明確になります。管理コンソールの中央設定では、追加のリージョンを作成し、異なるセキュリティオフィサーに割り当てることができます。この手順は、分散環境で特に便利です。

場所を指定する必要があります。分散データベースでは、u.trust LAN Crypt データベースのロギング内でログに記録されたイベントを明確に割り当てるために場所が使用されます。

分散データベースを使用していない場合でも、場所を指定する必要があります。これにより、後でデータベースを分散させるときに、エントリーを明確に割り当てることができます。

完了をクリックすると、u.trust LAN Crypt は初回マスターセキュリティオフィサーを作成し、u.trust LAN Crypt 管理コンソール のログオンダイアログを表示します。

その後、u.trust LAN Crypt 管理コンソールデータベースにログオンする権限を持つすべてのセキュリティオフィサーがこのダイアログに表示されます。

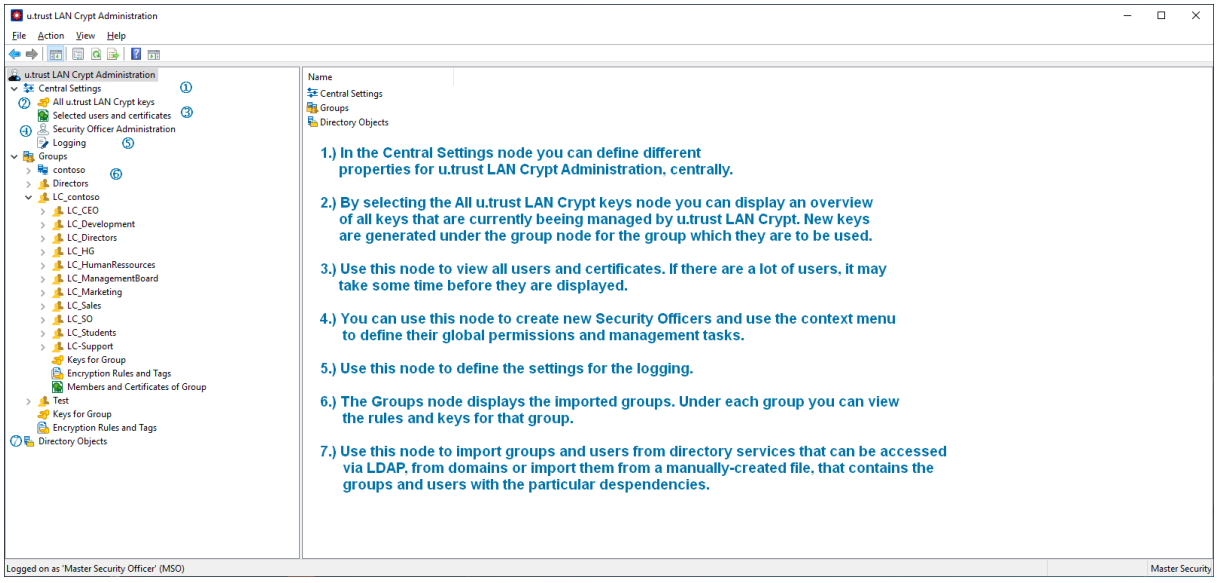
このダイアログで、新しく作成したマスターセキュリティオフィサーを選択し、[OK]をクリックします。

注意：ログオン後、リカバリーキーがまだ生成されていないことを知らせるダイアログが表示されます。復旧キーがない場合、緊急時（証明書を紛失した場合など）に管理データと暗号化されたデータがすべて失われる危険性があります。

このダイアログは、リカバリーキーが生成されるまで、マスターセキュリティオフィサーがログオンするたびに表示されます。再度警告しない］オプションを有効にすると、リカバリーキーが生成されていなくてもこのダイアログが表示されないようにできます。データ損失の可能性を避けるために、リカバリーキーを生成する必要があります。

3.4 管理コンソール：概要

u.trust LAN Crypt をインストールすると、SGLCAdmin.msc ファイルが u.trust LAN Crypt のインストールフォルダに保存されます。Windows のスタートメニュー（スタート＞u.trust LAN Crypt 管理コンソール＞管理コンソール）からこのエントリーをクリックすると、u.trust LAN Crypt 管理コンソールコンソールに必要なスナップインだけを表示する管理コンソールのウィンドウが開きます。



u.trust LAN Crypt 管理コンソールコンソールのスナップインを管理コンソールの通常ビューに追加することもできます（ファイル　スナップインの追加/削除 - u.trust LAN Crypt 管理コンソール）。スナップインを追加する場合でも、u.trust LAN Crypt 管理コンソールデータベースのパスワードが必要です。

誰がログオンしているか

ステータスバーには、現在どのセキュリティオフィサーがログオンしているかが表示されます。また、マスターセキュリティオフィサーかセキュリティオフィサーかも確認できます。

管理コンソールのツールバー

u.trust LAN Crypt の機能の多くは、管理コンソールのツールバーにアイコンとして表示されます。ツールバーの機能とアイコンの数は、その時点で選択されているタブによって異なります。

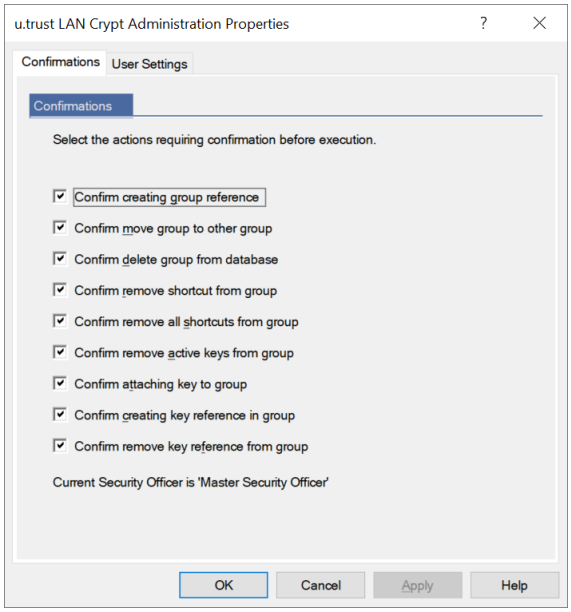
また、関連するコンテキストメニューから、これらのアイコンとして表示されるすべての機能を選択することもできます。

u.trust LAN Crypt 管理コンソールタブを右クリックしてノードのプロパティを表示し、必要に応じて変更します。これらのプロパティについては、以下のセクションで説明します。

3.4.1 確認

u.trust LAN Crypt 管理コンソールコンソールでは、実行前に確認が必要なアクションを指定することができます。これを行うには、u.trust LAN Crypt 管理コンソールルートノードのコンテキストメニューからプロパティをクリックします。

以下のダイアログは、これらのアクションを表示します：



アクションを選択した場合、実行する前に実行することを確認する必要があります。確認するまでアクションは実行されません。

この設定は、以下のアクションに対して行うことができます。

- グループ参照の作成確認

  既存のグループへの参照を作成するには確認が必要です。グループ選択＞マウス右ボタン＞コピー＞他のグループ選択＞マウス右ボタン＞ペースト＞確認

  注意：すべてのコピー、切り取り、貼り付け操作は、コンテキストメニューを使用するか、ドラッグ＆ドロップまたはドラッグ＆ドロップ＋CTRL 機能を使用して行うことができます。

- グループ移動の確認

  グループの移動には確認が必要です。

- データベースからのグループ削除の確認

  グループの削除は確認が必要です。

- グループからのショートカットの削除を確認

  グループ参照の削除は確認が必要です。

- グループからすべてのショートカットを削除することを確認します。

  別のグループにグループへの参照がある場合、例えばグループ 1 とグループ 2 にグループ 3 へのリンクがある場合、この参照の削除を確認する必要があります（グループ 3 を選択 > マウスの右ボタン > リンクの削除を選択）。

- グループからのキー削除を確認

  暗号化ルールで使用され、その後無効化されたキーの削除は、確認が必要です。使用済みのキーは管理コンソールでマークされ、グループから削除されてもデータベースに残ります。まだ使用されていないキーも、グループから削除されるとデータベースから削除されます。

- グループへのキーの取り付けを確認

  暗号化ルールで使用され、すべてのグループから削除されたキーはデータベースに保存され、中央設定/すべての LAN Crypt キーノードに表示されます。そこからドラッグ＆ドロップでグループに再割り当てできます。この操作は確認が必要です。

- グループ内でキー参照を作成することを確認

  グループ内のキーへのリンクの挿入（あるグループから別のグループへのドラッグアンドドロップなど）は、確認が必要です。キーは常にコピーされるか、キーへのリンクが挿入されます。キーをカットすることはできません。

- グループからキー参照を削除することを確認します。

  グループからキーへのリンクを削除するには、確認が必要です。

どのセキュリティオフィサーがログオンしていますか？

このダイアログには、どのセキュリティオフィサーが現在ログオンしているかも表示されます。セキュリティオフィサーの名前はダイアログの下部に表示されます。u.trust LAN Crypt 管理コンソールのステータスバーにも、どのセキュリティオフィサーが現在ログオンしているかが表示されます。

3.4.2 ユーザー設定

ユーザー設定タブでは、u.trust LAN Crypt 管理コンソールで表示される情報を設定できます。

起動

- u.trust LAN Crypt グループとドメインの関係を u.trust LAN Crypt 管理コンソールコンソール で表示するために、各グループ名にドメイン名を追加します。このオプションは、u.trust LAN Crypt を複数の異なるドメインで使用する場合に特に有効です。

- 選択されたユーザーと証明書を表示]をクリックすると、[中央設定]ノードで u.trust LAN Crypt にインポートされたすべてのユーザー（とその証明書）が表示されます。

  注意：大規模なインストールでは、すべてのユーザーと証明書を表示するのに数分かかることに注意：してください。その後、u.trust LAN Crypt 管理コンソールを再起動して、[選択したユーザーと証明書を表示]オプションで行った変更を有効にする必要があります。

  注意：u.trust LAN Crypt 管理コンソール機能をアップグレードする場合、選択したユーザーと証明書を表示するオプションを再度有効にする必要があります。

- ユーザーの親を表示をクリックすると、[グループのメンバーと証明書]ノードの下に、特定のユーザーの親グループが表示されます。これにより、u.trust LAN Crypt データベースにどのグループにも割り当てられていないユーザーが含まれているかどうかが一目でわかります。ユーザーの親を表示] で変更した内容を有効にするには、u.trust LAN Crypt 管理コンソールを再起動する必要があります。

- ユーザーリストのキャッシュを無効にします。

  パフォーマンスを向上させるため、u.trust LAN Crypt は通常バックグラウンドでユーザーリストを作成し、ユーザーが Administration で別のノードに切り替えた際にも作成し続けます。これらのリストの結果はバッファリングされ、リストが再度呼び出されたときにデータベースへのアクセスが不要になります。このため、大きなリストが含まれる場合、時間を大幅に節約できます。

  ただし、u.trust LAN Crypt の管理者（ターミナルサーバー）が複数並列に存在する環境では、メモリ要件が増加することがあります。これを防ぐには、このオプションを有効にします。その結果、リストはバッファリングされず、ユーザーがノードを離れたり、別のノードに変更したりしても、リストは作成され続けることはありません。このオプションは、実際にメモリ容量に問題がある場合にのみ使用することをお勧めします。

  同じセッションで行われたデータベースへの変更は、リストには自動的に転送されません。

  F5 キーを押すことで、いつでも変更内容を更新できます。

注意：上記の設定の変更は、データベースには保存されません。これらは、Microsoft Management Console スナップインで各ユーザーに保存される個人設定です。

3.5 中央設定

中央設定ノードでは、u.trust LAN Crypt 管理コンソール用のさまざまなプロパティを一元的に定義できます。

これを行うには、中央設定ノードのコンテキストメニューで プロパティをクリックします。または、これを選択し、u.trust LAN Crypt 管理コンソールツールバーのプロパティアイコ

ンをクリックします。その後、これらのプロパティをいくつかのタブで表示し、必要に応じて変更することができます。

注意： [追加権限]タブ、[リカバリーキー]タブ、および[リージョン]タブは、マスターセキュリティオフィサーのみが表示できます。サーバー]タブと[構成]タブは、[構成の変更]グローバル権限を持っているセキュリティオフィサーのみが表示できます。ディレクトリ]タブでパスを変更する場合も、[構成の変更]グローバル権限が必要です。アルゴリズム]タブ、[証明書]タブ、[解決ルール]タブは、マスターセキュリティオフィサーのみが変更できます。

3.5.1 アルゴリズムタブ

u.trust LAN Crypt には以下の暗号化アルゴリズムがあります。

- AES-128
- AES-256
- 3DES（非推奨）
- DES（非推奨）
- IDEA（非推奨）
- XOR（非推奨）

使用するアルゴリズムを選択します。ここで選択したアルゴリズムは、後で別のキーを生成するときに使用できます。

注意： これらの設定が後で変更された場合（例えば、3DES が使用可能なアルゴリズ ムのリストから削除された場合など）、既に生成されたキーやそのキーで暗号化されたデータは一切 影響を受けません。アルゴリズムが影響を受けると、後で新しいキーを生成するときに利用できなくなるだけです。安全でないと判断されたアルゴリズムを選択した場合、対応するセキュリティ通知が表示されます。これらのアルゴリズムを選択することは可能です。

デフォルトアルゴリズム

ここでは、ユーザーキーおよびグループキーの自動生成に使用するデフォルトアルゴリズムを選択します。キー長 256 ビットまたは 128 ビットの AES が、最もセキュリティが高いため、標準アルゴリズムとして推奨されます。

3.5.2 キータブ

u.trust LAN Crypt のインストールが、会社や部署の合併などで 1 つに統合された場合、内部キー名の重複が問題になることがあります。

このため、すべてのキーは独自のグローバルユニーク ID（GUID）で識別されます。GUID は通常 u.trust LAN Crypt によってランダムに生成され、後から変更することはできません。

ただし、u.trust LAN Crypt で暗号化したファイルを 2 社間で交換する場合は、共通のキーを生成する方法が必要です。

これは、例えば A 社の CryptOKEY キーで暗号化されたファイルを B 社が復号化できることを保証する唯一の方法です。その前に、B 社は A 社のキーと同じ設定の CryptOKEY というキーを生成しなければなりません。これは、キーの GUID と暗号化アルゴリズムにも影響します。

このような状況に対応するため、u.trust LAN Crypt には新しいキーを生成する際に GUID を手動で入力できるオプションがあります。これを有効にするには、[セキュリティオフィサーが新しく作成されたキーの GUID を定義できるようにする(デフォルトはランダム GUID)] オプションを有効にします。

キー値

オプションを有効にすることで、グローバル権限 Create Keys および Create Profiles を持つセキュリティオフィサーのみがキー（名前と値）を生成できるようにすることができます。セキュリティオフィサーがキーの作成時に値を割り当てなかった場合、キーの保存時に値が自動的に生成されます。

このオプションが有効な場合（新規インストールのデフォルト設定）、グローバルなプロファイルの作成権限を持っていないセキュリティオフィサーはキーを生成できません。

暗号化ルールにグループキー（<GROUPKEY>）を使用することも、これらのセキュリティオフィサーではできません。

注意：セキュリティオフィサーがキーの生成のみを行い、プロファイルの生成を行わない場合は、各グループの 権限で設定することができます（3.11.3 章セキュリティオフィサーにグループ処理権限を付与する。

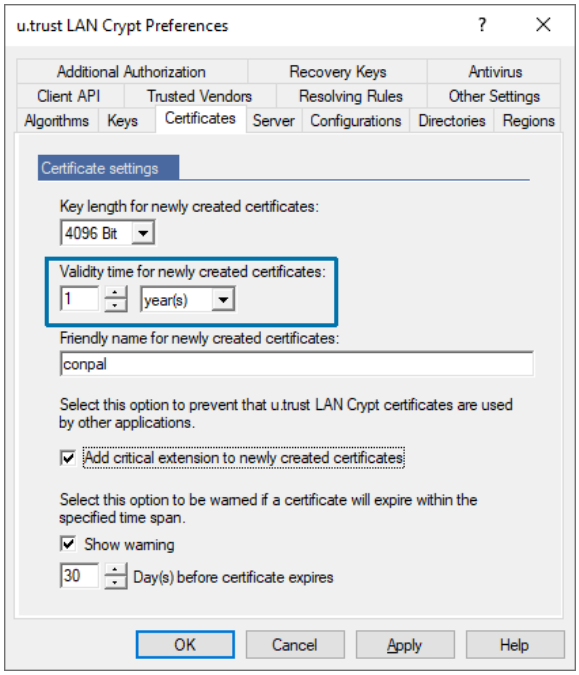
ポリシーファイルの生成時に値が生成されるグループキーの場合、暗号化ルールの作成に使用されると、値も直ちに生成されます。

注意： ″Generate profile″（プロファイルの生成）権限を持つセキュリティオフィサーのみがキーを生成できる（値のないキーは許可されない）オプションは、暗号化ルールにおけるユーザー固有のキー（<USERKEY>）の使用には影響しません。

注意：u.trust LAN Crypt は原則的に、値のないキーを作成するオプションも提供しています。このようなキーは制限なく管理で使用できます。しかし、これは分散データベースで問題を引き起こす可能性があります。キーへの参照を使用する例としては、値のないキー（値のない手動作成キー、グループキー<GROUPKEY>）を含むポリシーファイルが異なる場所でレプリケーションタイムウィンドウで生成される場合があります。ポリシー ファイルを生成するとき、キーの別々の値が各ロケーションで生成されます。その結果、2 つの異なる値を持つキーが生成されます。

3.5.3 証明書タブ

ここでは、u.trust LAN Crypt が生成する新しい証明書のキー長（1024、2048、4096 ビット）と有効期間を指定できます。新しく作成された証明書の有効期限は 1 年間です。この値はいつでも変更できます。



注意：新しく作成された証明書の有効期間は、1 日から最長 999 年の間で設定できます。ただし、情報セキュリティの観点から、有効期限はなるべく 5 年を超えないようにしてください。CA 証明書（認証局）については、最大 20 年の有効期間を推奨しています。

注意：（マスター）セキュリティオフィサーに割り当てられた証明書の有効期限は、3100 年を超えてはなりません。

新しく作成される証明書のフレンドリー名では、u.trust LAN Crypt で作成される証明書の名前を指定することができます。すべての証明書にこの名前が付けられるため、u.trust LAN Crypt の証明書であることが容易に識別できます。

新しく作成された証明書に重要な拡張子を追加するオプションを有効にすると、新しく作成された証明書に、これらの証明書を使用してはならないことを他のアプリケーションに示す重要な拡張子が追加されます。

また、警告を表示する警告期間を日数で指定することもできます（ルールがキャンセルされた場合、またはリストで証明書が黄色にマークされた場合）。たとえば、ここに 30 日と入力すると、証明書の有効期限が切れる約 1 か月前に、証明書がまもなく無効になるため更新する必要があるという警告メッセージが表示されます。

3.5.4 ルールの解決タブ

解決時に有効な証明書がないユーザーをスキップします。

ポリシーファイルを生成するときに、証明書が割り当てられていないユーザーを無視する場合は、このオプションを選択します。その結果、これらのユーザーのポリシーファイルは生成されません。

注意：ユーザーが作成され、このオプションが選択されていて、証明書がまだユーザーに割り当てられていない場合、暗号化ルールを解決（適用）するときに、このユーザーのポリシー ファイルを作成できなくても、システムは警告を表示しません。

クライアント上でのルールの順序を選択

注意：この設定はバージョン 3.90 以上のクライアントにのみ適用されます。

ここでは、3 種類のソート方法から選択できます。ソート方法 3 は、3.90 以下のクライアントバージョンで使用されるデフォルトの方法です。以前のバージョンの LAN Crypt ではソート方法を変更することができず、ソート方法 3 に対応していました。従って、ソート方法 3 はデフォルトのソート方法と見なされます。設定できるソート方法は以下の通りです。

- ソート方法 1

  1. ルール無視
  2. 除外ルール
  3. 暗号化ルール

- ソート方法 2

  1. ルール無視
  2. 除外ルール
  3. ワイルドカードなしの絶対パスで指定された暗号化ルール
  4. サブフォルダを含まないワイルドカードによる絶対パスで指定された暗号化ルール
  5. サブフォルダを含むワイルドカード付き絶対パスで指定された暗号化ルール
  6. その他のすべての暗号化ルール

  絶対パスは、UNC パス（ダブルバックスラッシュで始まる）または<ドライブ文字>: ¥

  キーへの参照の使用例：

  ¥¥or

  c: ¥confidential*.*.

- ソート方法 3（デフォルト）

  ソート方法 3 は、無視、除外、暗号化ルールを区別しません。

  ルールの並び順は以下の通り：

  1. ワイルドカードを使わないすべての絶対パス
  2. サブフォルダを含まないワイルドカードを使用したすべての絶対パス
  3. サブフォルダを含むワイルドカードを使用したすべての絶対パス
  4. その他の規則

  上記のセクション（例：並べ替え方法 3 – その他のすべてのルール）の中では、パスの定義の正確さに応じてルールが並べ替えられます。

  順番は以下の通りとなります。

  1. UNC のパス。
  2. <drive letter>で始まるパス：ここでは、ドライブ文字の後のバックスラッシュは考慮されません。
  3. 他のすべてのパス

- バックスラッシュの数が多いパスは、バックスラッシュの数が少ないパスの前に表示されます。
- ワイルドカードのないパスは、*.および*.*ワイルドカードのあるパスの前にリストされます。

注意：このオプションの変更は、新しいプロファイルが生成配布された後にクライアントで有効になります。

u.trust LAN Crypt クライアントで使用する暗号化形式を選択

u.trust LAN Crypt は以下の暗号化モードをサポートしています。

- CBC フォーマット（バージョン 3.50 以上）

  このフォーマットは、クライアントバージョン 3.50 以降で使用されます。これらのクライアントは、OFB モード（レガシー形式）で暗号化されたファイルを読み取ることができます。新しいファイルの暗号化モードは CBC です。

- XTS-AES フォーマット（バージョン 3.90 以上）

  このフォーマットは、クライアントバージョン 3.90 以降で使用できます。これらのクライアントは、OFB および CBC モードで暗号化されたファイルを読み取ることができます。新しいファイルの暗号化モードは XTS-AES です。このモードは AES キーにのみ使用されます。ファイルが他のアルゴリズムを使用したキーで暗号化されている場合、代わりに CBC 暗号化モードが使用されます。

3.90 以下のクライアントバージョンでは、以下の設定のみが有効

暗号化に CBC 形式を使用し、オプションで Legacy 形式を古い暗号化形式として使用します。それ以外の設定は、これらのクライアントでは無視されます。これらのクライアントはデフォルトで CBC または Legacy 形式を使用します。

定義された日付まで、この暗号化ファイル形式を使用

アップグレード処理中に、古い暗号化モードを設定することができます。この古い暗号化モードは、指定された日付まで有効です。この日付以降、すべてのクライアントは、設定されたファイル暗号化モードをサポートするように移行する必要があります。そうしないと、新しいクライアントは設定されたモードを使用して暗号化されたファイルを作成しますが、これらのファイルは古いクライアントでは読み取れません。

使用する暗号化形式の設定に応じて、ここで以下の形式を選択できます：

- レガシーフォーマット（バージョン 2.x、3.0x、3.1x）
- CBC フォーマット（バージョン 3.50 以上）は、暗号化ファイルフォーマットとして XTS-AES が設定されている場合にのみ使用できます。

  CBC を使用するには、クライアントのバージョン 3.50 以上が必要です。それ以前のクライアントでは、レガシー形式が選択されている場合のみ、定義された日付までこの暗号化ファイル形式を使用する設定が評価されます。

  ファイルの暗号化に旧形式を使用するまでの日付を指定する必要があります。この日付以降、またはこのオプションがクリアされると、ファイルは新しい暗号化形式で書

き込まれます。このオプションの変更は、新しいプロファイルが生成され配布された後にのみクライアントで有効になります。

すべてのクライアントがアップデートされた後、初回暗号化ツールで初回暗号化を行うことをお勧めします。これにより、新しい u.trust LAN Crypt 暗号化フォーマットのみが使用されるようになります。

この変更は、次に暗号化ルールが解決されたときに有効になります。

注意：旧式の暗号化モード OFB で作成された暗号化ファイルは、u.trust LAN Crypt バージョン 4.x.x では読み込みのみ可能で、書き込みはできません。新しいモードは書き込みや保存の際に使用されます。一般的に Utimaco は、旧式の OFB 暗号化モードで暗号化されたままのすべてのファイルを、初回暗号化を使って(AES) XTS に暗号化することを推奨します。

管理部門がバイパス規則レジストリ設定の所有権を持ちます。

バイパスルールは、特殊なシナリオで u.trust LAN Crypt の必須機能を無効にするために使用されます。このバイパス機能を有効にすると、すべてのクライアントに影響します。バイパス機能は、u.trust LAN Crypt 管理コンソールコンソール 経由のルールで、レジストリのバイパスルールの所有者を管理するオプションが有効になっている場合にのみ使用できます（バイパスを参照）。

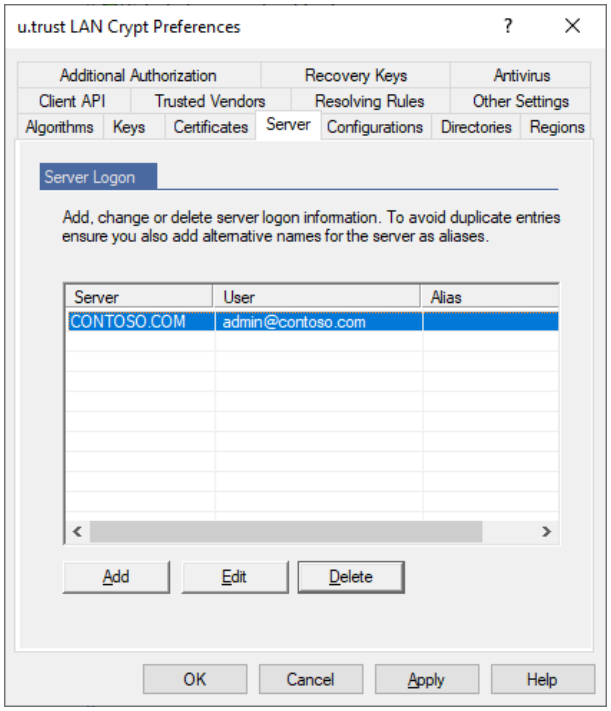
警告：ここでは細心の注意が必要です。設定を誤ると、特にファイルが破損（破壊）する可能性があります。そのため、このようなルールの導入は非常に重要であり、Utimaco のサポートと連携して行う必要があります。

注意：グループポリシーやレジストリによってバイパスルールが既に設定されている場合、この新機能はそれらを上書きまたは削除します。

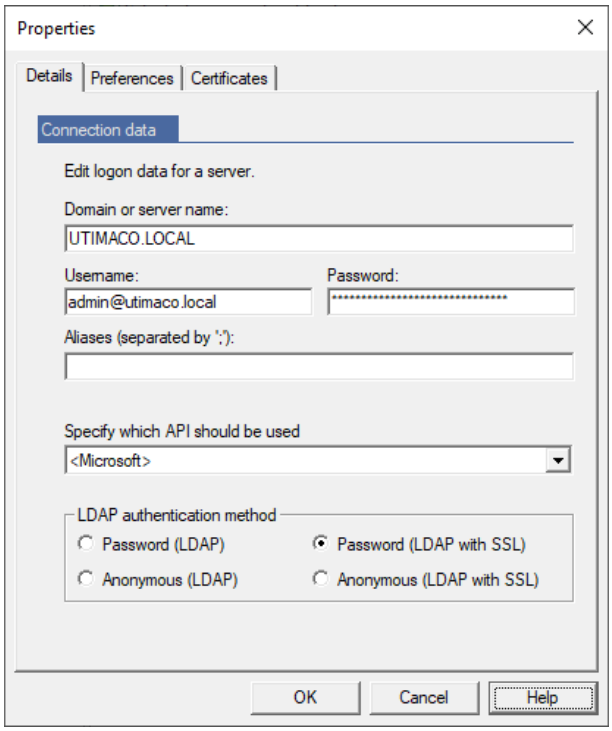
注意：この機能を無効にするのは、他のルールとの競合を避けるために、すべてのバイパスルールが設定から削除された後でなければできません。

3.5.5 サーバータブ

サーバーからグループとユーザーをインポートするには、u.trust LAN Crypt はそのサーバーのログオン情報を必要とします。



この情報は、[サーバー]タブに入力する必要があります。Add をクリックすると、3 つのタブがある別のダイアログが開きます。詳細、環境設定、証明書の 3 つのタブがあります。



サーバーの詳細パスワードログオン

1. ドメイン名またはサーバー名、ユーザー名、および適切なパスワードを入力します。重複入力を防ぐため、同じサーバーに複数の名前でアクセスできる場合に備えて、サーバーの別名として別の名前も入力してください。

   Microsoft ディレクトリサービスを使用している場合は、次のようにします：

   - ドメインまたはサーバー名] にドメイン名を入力します。

- ユーザー名を username@domain と入力します。

  注意：Microsoft 以外のディレクトリサービスからオブジェクトをインポートするには、ユーザー名を LDAP 構文（正規名）で入力する必要があります。

  例： cn=admin,ou=techops

2. 使用する API を指定します。

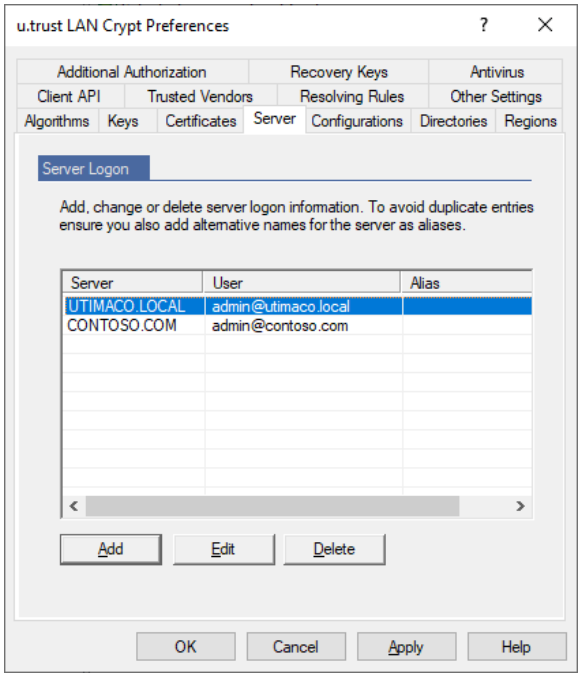
   ドロップダウンリストから<Microsoft>または<Novell>を選択します。プレースホルダの<Novell>は、Microsoft 以外のすべての API を表します。

   注意： Novell ディレクトリサービスからのインポートは LAN Crypt バージョン 3.90 以降サポートされていません。その他の Novell の機能もサポートされなくなりました。

3. サーバーへのアクセスに使用する LDAP 認証方法を指定します。u.trust LAN Crypt では、以下の方法を提供しています：
   - パスワード（LDAP）
   - パスワード（SSL 付き LDAP）

4. OK をクリックします。

サーバーは、［サーバー］タブの表に表示されます。



ログオン失敗時のエラーメッセージ

u.trust LAN Crypt がサーバーへのログオンに失敗した場合、u.trust LAN Crypt 管理コンソールコンソール にエラーメッセージが表示されます。

サーバーの詳細匿名ログオン

1. サーバー名を入力します。重複入力を防ぐため、同じサーバーに複数の名前を使用してアクセスできる場合に備えて、サーバーのエイリアスとして別の名前も入力してください。

2. 使用する API を指定します。

   ドロップダウンリストから<Microsoft>または<Novell>を選択します。プレースホルダの<Novell>は、Microsoft 以外のすべての API を表します。

   注意： Novell ディレクトリサービスからのインポートは LAN Crypt バージョン 3.90 以降サポートされていません。その他の Novell の機能もサポートされなくなりました。

3. サーバーへのアクセスに使用する LDAP 認証方法を指定します。u.trust LAN Crypt では、匿名ログオン用に以下の方法を提供しています：

   - 匿名 (LDAP)
   - 匿名 (SSL 付き LDAP)

4. OK をクリックします。

サーバーはサーバータブの表に表示されます。

ログオン失敗時のエラーメッセージ

u.trust LAN Crypt がサーバーへのログオンに失敗した場合、u.trust LAN Crypt 管理コンソールコンソール にエラーメッセージが表示されます。

環境設定

オブジェクトの識別

u.trust LAN Crypt は、Active Directory にインポートされたオブジェクトを識別するために、正確で不変の GUID (Global Unique ID) を使用します。この GUID は、データベースとディレクトリサービスの同期にも使用されます。例えば、個々の単一オブジェクトの名前が変更される可能性があるため、Active Directory の更新がデータベースに反映され、Active Directory の新しい名前のためにデータベースに新しいオブジェクトが生成されないようにします。

しかし、他のディレクトリサービスではこのタイプの ID を使用しないものもあります。この場合、u.trust LAN Crypt はオブジェクトを一意に識別する別の方法を提供します。u.trust LAN Crypt は特定の LDAP 属性を使用してオブジェクトを一意に識別するように設定できます。これらの属性は u.trust LAN Crypt 管理コンソールで設定します。

<default>と<other>の設定は常に利用可能です。通常、<default> 設定は、その設定が参照するサーバーにとって十分なものです。<standard> 設定で評価される属性は常に <default> の下に表示されます。このようにして、どの属性がデフォルト設定で評価されるかを示すことができます。また、これらの属性がすべて当該ディレクトリサービスに既に存在する場合、特定の属性を割り当てることもできます。既に表示されている属性以外の属性を指定するには<other>を使います。

注意：ここに属性を入力する場合は、オブジェクトを明確に識別できるデータが含まれていることを確認してください。

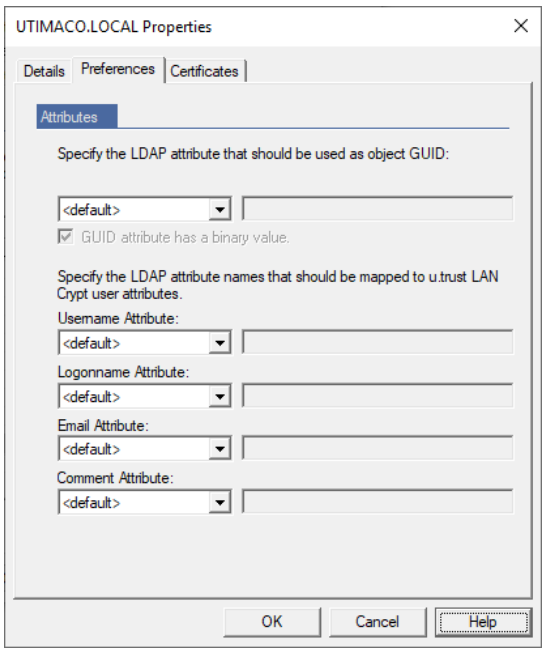
- オブジェクト GUID

  ここでは識別に使用する属性を指定します。設定を <standard> のままにすると、GUID と objectGUID の両方の属性が評価されます。

オブジェクトの識別に別の LDAP 属性を使用する場合は、objectGUID の下にある<other>を選択し、その横の入力フィールドに LDAP 属性の名前を入力します。この属性には、オブジェクトを明確に識別できるデータを含める必要があります。

- GUID 属性はバイナリ値

  このオプションは、オブジェクトのプロパティダイアログでの GUID の表示方法にのみ影響します。これらを正しく表示するには、使用する GUID がバイナリ値である場合にこのオプションを有効にします。どうしたらよいかわからない場合は、このオプションを有効にしてください。



注意：この設定はデフォルトで有効になっています。この設定を変更できるのは、<その他>を選択した場合のみです。

ユーザー属性

- ユーザー名属性

  この設定は、u.trust LAN Crypt 管理コンソールコンソールでのユーザーの表示方法にのみ影響します。ユーザーは、グループのプロパティダイアログおよびユーザーと証明書のスナップインに表示されます。

  既存の属性を選択するか、<other>を選択して LDAP 属性を入力します。<default>は（CN と SN）を評価します。

- ログオン名属性

  u.trust LAN Crypt は、ユーザーのログオン名の後にポリシーファイルを命名します。ユーザーは、ログオン名とポリシーファイル名が同じ場合にのみログオンできます。

  ここでは、どの LDAP 属性を使用してユーザーのログオン名を定義するかを指定できます。

  <default>は SAMAccountName、userPrincipalName、UID を評価します。これらの属性の 2 つまたは 3 つが既にディレクトリサービスに存在する場合、ユーザーのログオン名を定義するものを選択することができます。

ログオン名を含む他のディレクトリサービス属性を指定するには、<other>を選択します。

注意：属性の名前に@文字が含まれている場合、u.trust LAN Crypt はこの時点で名前を切り捨てます。このため、メールアドレスが使用されている場合などに問題が発生する可能性があります。

- 電子メール属性

  このメールアドレス属性は、自分で作成した証明書に追加されます。

- コメント属性

  電子メールアドレスと同様に、この属性もユーザーオブジェクトの識別に使用できます。これは、証明書の割り当て時にウィザードがオブジェクトの識別にユーザー名とログオン名を使用できない場合に特に便利です。この時点で、証明書の割り当て時にウィザードが正しいユーザーを識別するために使用する属性名を入力できます。

  注意：同期中に空の属性がインポートされた場合（AD で属性が削除された場合など）、u.trust LAN Crypt のコメントは影響を受けません。既存のエントリーは維持されます。新しい属性の内容は既存のコメントを上書きします。

  <default>を選択した場合、コメントはインポートされません。

- 証明書

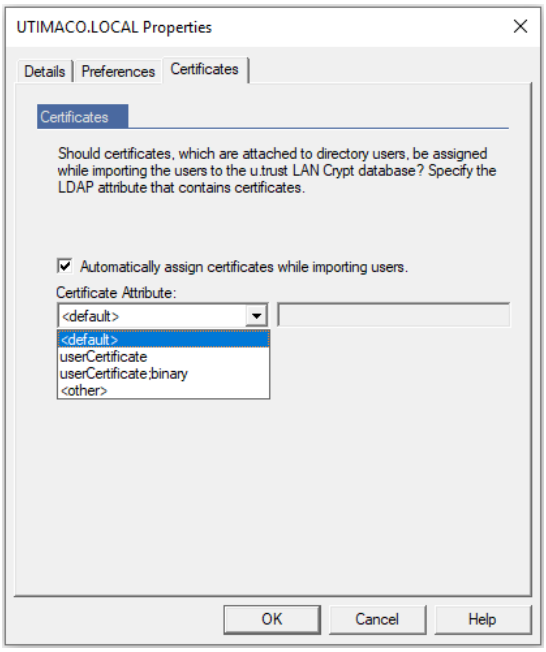
  証明書タブで、ユーザーを u.trust LAN Crypt データベースにインポートする際に、LDAP ディレクトリでユーザーに割り当てられた証明書を転送するかどうかを指定します。

  u.trust LAN Crypt 管理コンソールコンソールでこれらのユーザーに証明書を割り当てる必要はありません。ここで、ユーザーの証明書を含む属性を指定することもできます。

  注意：この方法で割り当てられた証明書はチェックされません（有効期限、CRL など）をアクティブにします。

  ユーザーのインポート時に証明書を自動的に割り当て

  オプションを使用して、LDAP ディレクトリから証明書を自動的にインポートし、u.trust LAN Crypt データベースにインポートする際にユーザーに割り当てます。



<default>は userCertificate と userCertificate;binary を評価します。

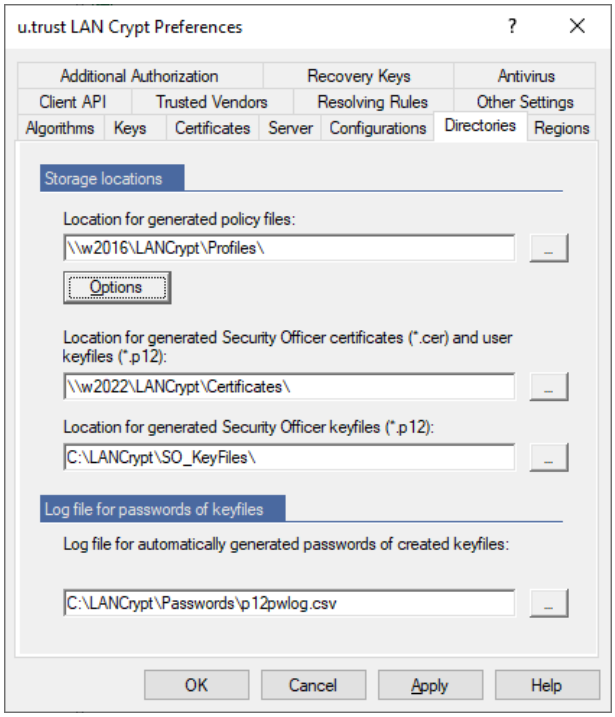
証明書を含む別の属性を指定するには、<other>をクリックします。

OK をクリックすると、u.trust LAN Crypt はサーバーリストにログオン情報を転送します。このリストでは、これらの詳細情報を編集または削除することもできます。

3.5.6 ディレクトリタブ

注意：ここで行った設定は、常にセキュリティオフィサーの現在の設定レコードに保存されます。設定レコードがまだ作成されていない場合、システムは<初回設定>設定レコードが使用されます。

注意：ディレクトリタブの中央設定ノードでは、%LOGONSERVER%などの環境変数をパス指定に使用することはできません。



生成されたポリシーファイルの場所：

ユーザー用に生成されたポリシーファイルを保存する場所を指定する必要があります。

入力フィールドに保存場所（通常はユーザーと共有されているネットワークドライブ）を入力します。

注意：ユーザーがログオンすると、生成された(ポリシー)ファイルがこのフォルダからロードまたはコピーされるため、ユーザーがこのフォルダにアクセスできることを確認してください。

注意：クライアントから見たポリシーファイルの保存場所も指定する必要があります。この設定は、u.trust LAN 暗号化設定の下にあります （ポリシーファイルクライアントの場所（を参照)。

ポリシーファイルオプション - ポリシーファイル形式の指定

異なるバージョンの LAN Crypt クライアントを使用する場合、すべての LAN Crypt クライアントが生成されたポリシーファイルを読み込めるようにする必要があります。

注意： バージョン 4 以降、u.trust LAN Crypt は古いポリシーファイル形式（*.pol.bz2 や *.pol など）をサポートしなくなりました。LAN Crypt の古いクライアントバージョンを使用している場合、バージョン 11.0.0 をインストールする前に、バージョン 3.97 にアップグレードする必要があるかもしれません。現在のポリシーファイルの形式は*.xml.bz2 です。このフォーマットはバージョン 3.90 から LAN Crypt でサポートされています。ポリシーファイルのフォーマットはあらかじめ定義されており、バージョン 4.0.0 からは変更できません。

ノベル名に基づいて追加のポリシーファイルを作成

注意：この機能は u.trust LAN Crypt ではサポートされなくなりました。

生成された証明書およびキーファイル（*.p12）の保存場所

u.trust LAN Crypt は、必要に応じて自己署名証明書（*.p12 キーファイル）を生成し、ユーザーに割り当てることができます。これらの証明書は、管理コンソールの Selected users and certificates ノードで作成割り当てられます。また、この機能はグループ/メンバーノードとグループの証明書ノードからも利用できます。

注意：管理コンソールに選択されたユーザーと証明書ノードが表示されない場合は、u.trust LAN Crypt 管理コンソールノードの下で、コンテキストメニューのプロパティをクリックした後、ユーザー設定タブに選択されたユーザーと証明書を表示するオプションが有効になっているかどうかを確認してください。

これらのファイルを保存するパスは、管理コンソールの［ディレクトリ］タブの［中央設定］ノードで指定する必要があります。クライアントは、u.trust LAN Crypt グループポリシーの設定（Keyfile Client Location）またはレジストリのエントリー（レジストリファイルなど）を介して、このアクセスパスを受け取ります。

u.trust LAN Crypt クライアントは、まずコンピュータのローカル証明書ストアで一致する証明書を検索し、次に（見つからない場合は）GPO またはレジストリ設定で定義されたパスに検索します。また、セキュリティオフィサー証明書の公開部分（*.cer）は、管理コンソールによってこのパスに保存されます（GPO 設定セキュリティオフィサー証明書クライアントの場所）。

u.trust LAN Crypt がユーザーキーファイルを自動的に認識できるように、ファイル名はユーザーのログオン名（"Logonname.p12"）と一致している必要があります。

u.trust LAN Crypt は正しいファイルを見つけると、PIN ダイアログを表示します。この PIN をユーザーに伝えるために PIN を送信する必要があります（パスワードログファイルにあります）。ユーザーが PIN を入力すると、証明書と関連キーが自動的にインポートされます。

u.trust LAN Crypt は、セキュリティオフィサーの証明書のパブリック部分を含む*.cer ファイルを見つけると、自動的にインポートします。

または、ユーザー用のキーファイルとセキュリティオフィサー証明書のパブリック部分を手動で配布することもできます。この場合、クライアントがその両方をインポートするようにしてください。

注意：クライアントは、ポリシーファイルを生成した特定のセキュリティオフィサーの証明書のパブリック部分をインポートする必要があります。セキュリティオフィサーの*.cer ファイルとユーザーの*.p12 ファイルが保存されているパスを変更した場合、セキュリティオフィサーを作成した後、その*.cer ファイルを新しい場所にコピーする必要があります。そうしないと、セキュリティオフィサーの証明書のパブリック部分が見つかりません。

ユーザーキーファイルのデフォルトパスワード

u.trust LAN Crypt では、すべてのユーザーキーファイルに統一パスワードを定義することができます。

これを行うには、必要なパスワード（最大 32 文字）を含むファイルを、パスワードログファイルを含む同じディレクトリにコピーします（次ページのキーファイルのパスワード用ログファイルを参照）。

パスワードを含むファイルは、対応するパスワードログファイル（デフォルト名：p12pwlog.csv）と同じ名前でなければなりませんが、ファイルの拡張子は ″*.pwd ″でなければなりません（パスワードログファイルのデフォルト名：p12pwlog.pwd）。システムがこのタイプのファイルを見つけると、生成されるすべてのユーザーキーファイルはこのパスワードを持つことになります。

注意：ユーザーキーファイルのデフォルトパスワードを使用している場合、生成された証明書およびキーファイル（.p12）の保存場所に、同じユーザーのキーファイル（.p12）が複数存在してはなりません。

このファイルで、キーワードとして*logonname*を入力すると、デフォルトのパスワードの代わりに、現在のログオン名がパスワードとして使用されます。

注意：セキュリティオフィサー用の ″*.p12 ″ファイルは、セキュリティが高いため、常にランダムなパスワードが与えられます。

生成されたセキュリティオフィサー証明書（*.p12）の保管場所

u.trust LAN Crypt は、セキュリティオフィサーの証明書をバックアップとして*.p12 ファイルなどに保存します。ここで、保存先のフォルダを指定することができます。

注意：機密データを扱うため、不正アクセスから保護することが不可欠です。

キーファイルのパスワード用ログファイル

ここでは、生成された PKCS#12 ファイルのログファイルの保存場所と名前を指定できます（デフォルト名：p12pwlog.csv）。このファイルには、生成された PKCS#12 ファイルのパスワードが含まれ、PIN の作成などに使用できます。

パスワードログファイルには以下の情報が含まれています（括弧内のキーワードは*.csv ファイルのカラムヘッダーを表します）。

- 生成日（CreateDate）
- 生成時刻（CreateTime）
- 有効期限（ExpirationDate）
- 有効期間が終了する正確な時刻（ExpirationTime）
- ユーザー名（名前）
- ログオン名（Logonname）
- メールアドレス（EMail）
- 生成モード（Mode）。設定可能な値は以下のとおりです。
  <GUI>-ユーザーのプロパティダイアログで証明書が生成されました。
  <SO>- セキュリティオフィサーの証明書。セキュリティオフィサーの作成時に生成されます。
  <WIZARD>-証明書は証明書割り当てウィザードを使用して生成されます。
- ファイル名（Filename）
- パスワード

注意：このファイルを保護し、いかなる場合でもポリシーファイルと同じフォルダに保存しないでください。

注意：証明書を割り当てるセキュリティオフィサーが、パスワードログファイルを変更するファイルシステムの権限を持っていない場合、u.trust LAN Crypt は証明書を生成することができません。

u.trust LAN Crypt を使用すると、パスワードログファイルを簡単に保護できます。そのためには、管理コンソール とクライアントを同じコンピュータにインストールします。最初のマスターセキュリティオフィサーを作成した後、パスワードログファイルを暗号化する暗号化ルールを作成し、最初のマスターセキュリティオフィサーのプロファイルを作成し、プロファイルをロードします。使用する暗号化キーは、マスターセキュリティオフィサーと証明書を作成する権限を持っているセキュリティオフィサーのみが使用できます。

注意：u.trust LAN Crypt コンポーネントの管理コンソールとクライアントアプリケーションを同じコンピュータにインストールする場合は、同じバージョンである必要があります。

3.5.7 リージョンタブ

u.trust LAN Crypt では、キーの管理を簡単かつ複雑にしないためにリージョンを設定することができます。各リージョンは特定のセキュリティオフィサーに割り当てられ、そのセキュリティオフィサーが責任を負います。このセキュリティオフィサーがキーを生成すると、システムは自動的にキー名の先頭にこのリージョンのプレフィックスを追加します。その結果、各キーが生成された管理単位を常に確認することができます。この方法は、特に分散環境で有用です。

中央設定ノードのリージョンタブでコンテキストメニューのプロパティをクリックすると、リージョンを定義できます。ここに表示されたリージョンは、セキュリティオフィサーの作成時にセキュリティオフィサーに割り当てることができます。追加をクリックすると、新しいリージョンを定義できます。リージョン名入力フィールドに、該当するリージョンの適切な名前（例：New York）を入力し、このリージョンのプレフィックス入力フィールドに、該当するリージョンのプレフィックス（例：NY）を入力します。OK ボタンをクリックすると、新しいリージョンが既存のリージョンリストに追加されます。

既存のリージョンを変更または削除するには、リージョンを選択し、編集または削除をクリックします。

注意：リージョンを削除できるのは、そのリージョンがセキュリティオフィサーに割り当てられていない場合のみです。

3.5.8 設定タブ

中央設定ノードの[設定]タブを使用して、各リージョンに個別の設定セットを作成できます。このように定義された設定セットは、それぞれのリージョンでのみ有効です。選択したセキュリティオフィサーをそれぞれのリージョンに割り当てると、個々のリージョンの管理を行うことができます。

設定レコードには、ディレクトリタブで入力できるすべての詳細が含まれています：

- 生成されたポリシーファイルの保存場所
- 生成された証明書とユーザーキーファイルの保存場所

- 生成されたセキュリティオフィサーのキーファイルの保存場所
- パスワードログファイルの保存場所と名前
- ポリシーファイルのオプション

設定記録は常に既存のリージョンに割り当てられます。通常、あるリージョンに割り当てられたセキュリティオフィサーは、そのリージョン用に生成された設定レコードしか使うことができません。例外は、<DEFAULT CONFIGURATION> 設定レコードで、これはすべてのリージョンで使うことができます。

1 つの組織単位（リージョン）に 1 つの特定の設定を使用することで、1 人または複数のセキュリティオフィサーに正しいパスを簡単に設定でき、すべてのセキュリティオフィサーが生成されたファイル（証明書、ポリシーファイル、パスワードログファイルなど）を保存するために常に同じパスを使用することができます。

ディレクトリタブで行った変更は、常に現在割り当てられている設定レコードに保存されます。

注意：グローバル権限構成の変更は、セキュリティオフィサーが自身の構成設定を変更することを許可されているかどうかを指定します。セキュリティオフィサーがこの権限を持っていない場合、選択したパスしか使用できません。

セキュリティオフィサーが既存の設定レコードを変更すると、その設定に割り当てられているすべてのセキュリティオフィサーの設定も変更されます。

設定レコードの生成

設定レコードを作成するには、以下の手順に従います。

1. 構成レコードを作成する既存のリージョンを選択するか、<リージョンなし>を選択して、リージョンに属していないセキュリティオフィサーを割り当てることができる構成レコードを作成します。

2. 新しい名前に新しい構成レコードの名前を入力します（例：New York）。

3. リストから既存の設定レコードを選択します。

   システムはこの構成レコードをコピーし、新しい名前で保存します。コピーをクリックします。

4. 設定レコードを編集する場合は、そのレコードを選択し、［編集］をクリックします。

5. プロパティのディレクトリダイアログと同じダイアログが表示されます。ここで、適切なパスを入力し、ポリシー ファイルのオプションを定義します。OK をクリックします。

6. これで、リストに新しい設定レコードが適切なリージョンに表示され、それを使ってさらにセキュリティオフィサーを作成することができます。既存の設定レコードの設定（およびリージョン）を変更するには、特定のセキュリティオフィサーのプロパティタブを選択します。

7. 設定レコードは必要な数だけ追加作成できます。

3.5.9 追加認証タブ

u.trust LAN Crypt では、特定のアクションに少なくともう一人のセキュリティオフィサーの追加認証が必要であることを定義できます。追加認証が必要なアクションは以下の通りです：

アクション	必要な権限
追加認証設定の変更	マスターセキュリティオフィサーのみが行うことができます。
リカバリーキーの変更	マスターセキュリティオフィサーのみが行うことができます。
以下のアクションは、操作を承認するグローバル権限を持ち、アクションを実行する権限を持つセキュリティオフィサーのみが実行できます。 重要 状況によっては、追加権限を提供するグローバル権限だけでは十分でない場合があることに注意：してください。追加権限を提供するセキュリティオフィサーは、この特定のオブジェクトに対応する権限を持っていなければなりません。	

アクション	必要な権限
グローバル設定の変更	グローバル権限「設定の変更」が必要です。 アルゴリズム]、[証明書]、[リージョン]、[ディレクトリ]、[キー]、[アンチウイルス]、[ルールの解決]、[サーバー]、[構成]、および [その他の設定] タブで変更を行うときに、システムによる認証のプロンプトが表示されます。 マスターセキュリティオフィサーのみが、アルゴリズム、証明書、キー、解決ルール、リージョン、その他の設定タブの変更を承認できます。
セキュリティオフィサーの作成	グローバルパーミッション Create セキュリティオフィサーが必要です。
アクセス制御リストの変更	グローバル権限「ACL の変更」と対応するグループまたは SO 固有の権限が必要です。
グローバル権限の変更	グローバル権限「グローバル権限の変更」と、対応するグループまたは SO 固有の権限が必要です。
証明書の割り当て	グローバル権限証明書の割り当てと、対応するグループ固有の権限が必要です。
全メンバーに証明書を割り当てる	「すべてのメンバーに証明書を割り当てる」グローバル権限と、対応するグループ固有の権限が必要です。

ユーザーまたはグループ固有のキーの使用	グローバル権限特定のキーを使用が必要です。特定のキーを使用するための追加権限を指定しても、プレースホルダー<userkey>や<groupkey>の使用には影響しません。実際の特定のキーの取り扱い（表示/使用/編集）を制限します。
グループの管理	グループの管理グローバル権限と、対応するグループ固有の権限が必要です。
ユーザーの管理	ユーザーの管理グローバル権限と、対応するグループ固有の権限が必要です。
ログの管理	ロギングエントリーの読み取りとロギングの管理のグローバル権限が必要です。
ルールの作成	これには、グローバル権限ルールの作成と、対応するグループ固有の権限が必要です。
キーの作成と移動	グローバル権限「キーの作成」と、対応するグループ固有の権限が必要です。
プロファイルの作成	プロファイルの作成］のグローバル権限と、対応するグループ固有の権限が必要です。
表示キーの値	グローバル権限「キーの読み取り」が必要です。キーのプロパティダイアログでキー値の表示オプションをチェックする場合は、追加の権限が必要です。

注意：特定のアクションの実行に追加の承認が必要な場合、この設定は密接に関連するアクションにも適用されます。

これらのアクションの 1 つに追加の承認が必要な場合、そのアクションに必要なセキュリティオフィサーの数を指定する必要があります。

これを行うには、そのアクションを選択します。選択したアクションをダブルクリックすると、必要なセキュリティオフィサーの数を指定するダイアログが開きます。OK をクリックすると、u.trust LAN Crypt は中央設定ノード内の追加認証タブのリストを更新します。

必要なセキュリティオフィサーの数が利用できないとシステムが認識した場合、メッセージが表示されます。

注意：システムは、実際に利用可能なセキュリティオフィサーの数を正確に知ることはできません。メッセージが表示されなくても、実際には必要な人数が利用できない場合があります。例えば、セキュリティオフィサーの権限がその後変更されたり、セキュリティオフィサーが削除された可能性があります。

注意：必要なセキュリティオフィサーがいないことを知らされ、必要なセキュリティオフィサーの数を定義する際に少なくとも 1 人の追加セキュリティオフィサーが必要であることを指定し、OK で設定を確定してダイアログを閉じた場合、技術的な理由によりその設定は採用されません。

これにより、必要なセキュリティオフィサーを利用できないため、追加認証が必要なアクションを実行できなくなります。追加権限設定の変更オプションにこの設定が指定されている場合、このダイアログの設定は変更できなくなります。

この設定は、リカバリーキーを生成することによってのみ変更できます（次ページの追加認証の放棄を参照）。

u.trust LAN Crypt はマスターセキュリティオフィサーがシステム内に存在することだけを保証します。

注意：追加認証にトークンを使用しない場合は、強力な秘密鍵保護をはいに設定することをお勧めします。

追加承認の提供

アクションに追加承認が指定されている場合、そのアクションが選択されると追加承認ウィザードが実行されます。このウィザードでは、少なくともう 1 人のマスターセキュリティオフィサーによる承認を求めます。ダイアログで該当するマスターセキュリティオフィサーを選択できます。

u.trust LAN Crypt がこのセキュリティオフィサーの証明書を使用して認証に成功すると、必要なアクションを実行できます。

複数のセキュリティオフィサーが同じ証明書を持っている場合、この証明書は 1 回の認証実行で 1 回のみ使用できます。この証明書が割り当てられた他のセキュリティオフィサーは、セキュリティオフィサーのリストから削除されます。

注意：セキュリティオフィサーを選択するダイアログには、特定のリージョンのセキュリティオフィサーに表示を限定できるオプションがあります。どのリージョンにも割り当てられていないセキュリティオフィサーは常にリストに表示されます。

追加承認の取り消し

あるアクションに対する追加権限は、通常、u.trust LAN Crypt 管理コンソールセッションの全期間にわたって適用されます。管理ツールバーの[現在付与されている追加権限をすべてリセット]ボタンをクリックすると、該当する情報が削除されます。

追加承認の放棄

設定によって、あるアクションの追加承認を行うセキュリティオフィサーの数が少なすぎるという状況が発生した場合、リカバリーキーを使用して、追加承認設定を変更するために必要なセキュリティオフィサーの数を 0 にリセットすることができます。

これを行うには、ログオンダイアログで証明書の割り当てをクリックします。ウィザードが実行され、追加で必要なセキュリティオフィサーの数を 0 にリセットできます。詳細は以下を参照してください。

3.5.10 リカバリーキータブ

u.trust LAN Crypt ではリカバリーキーを生成することができます。このキーは、セキュリティオフィサーが u.trust LAN Crypt データベースにログオン（証明書の割り当てボタンをクリック）した際に、証明書が破損して使用できなくなった場合などに、新しい証明書を割

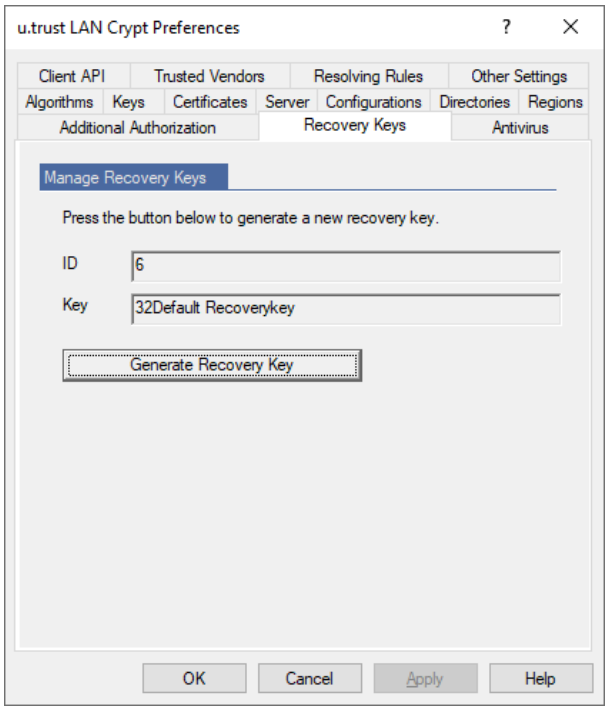
り当てるために使用します。リカバリーキーを使用すると、追加認証の設定変更に必要なセキュリティオフィサーの追加数を 0 にリセットすることもできます。

リカバリーキーはいくつかの部分に分割することができ、新しい証明書を割り当てるために必要な部分の数を指定できます。リカバリーキーの各部分は、異なるセキュリティオフィサーに配布できます。各パートの所有者は、リカバリーキーの使用時に同席し、ウィザードを使用してキーのパーツを提示する必要があります。リカバリーキーは、手動で入力するか、ファイルから読み込むことができます。

しかし、（LAN Crypt 管理コンソールバージョン 4.1.0 では）KMIP キーサーバーにリカバリーキーを保存することもできます。

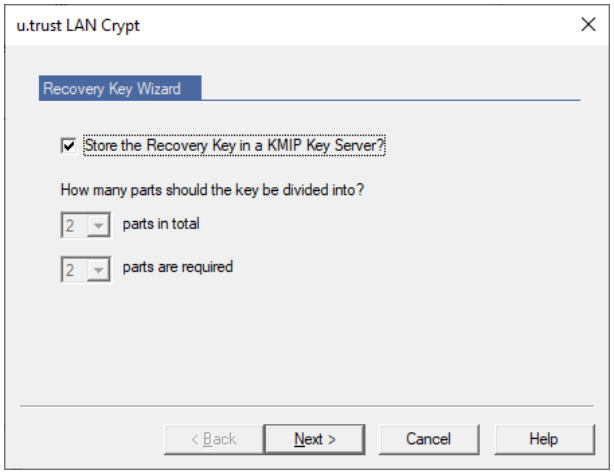
注意：KMIP キーサーバー（オプション）を使用すると、特に安全な方法でリカバリーキーを保存できます。u.trust LAN Crypt バージョン 11.0.0 は、現在 Utimaco の Enterprise Secure Key Manager (ESKM)にのみ対応しています。

リカバリーキーを生成するには、管理コンソールの中央設定ノードでコンテキストメニューを開き、[プロパティ]をクリックします。表示されるダイアログで、[リカバリーキー]タブに切り替えます。



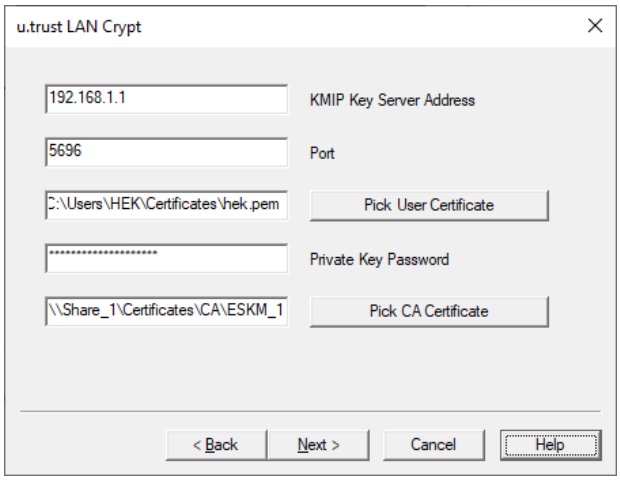
リカバリーキーの生成ボタンをクリックします。

リカバリーキーの生成に使用するウィザードを実行します。



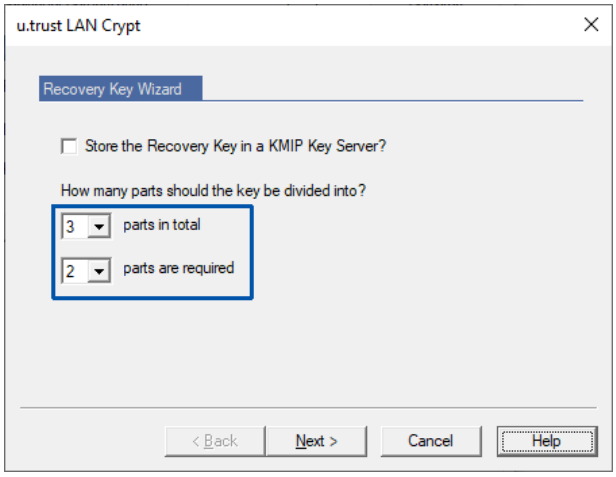
リカバリーキーを KMIP キーサーバーに保存しますかオプションを選択するか、ドロップダウンメニューを使用して、キーに含まれる部分の数と、リカバリーキーの使用に必要な部分の数を選択します。

復元キーを KMIP キーサーバーに保存しますかオプションを選択し、[次へ]をクリックした場合は、KMIP キーサーバーの接続データ（サーバーのアドレスとポート）、必要な証明書の詳細、秘密鍵のパスワードをそれぞれの入力フィールドに入力する必要があります。



次へをクリックします。KMIP キーサーバーへの接続と証明書の詳細がチェックされ、成功すると、リカバリーキーが KMIP キーサーバーにセキュア保存されます。

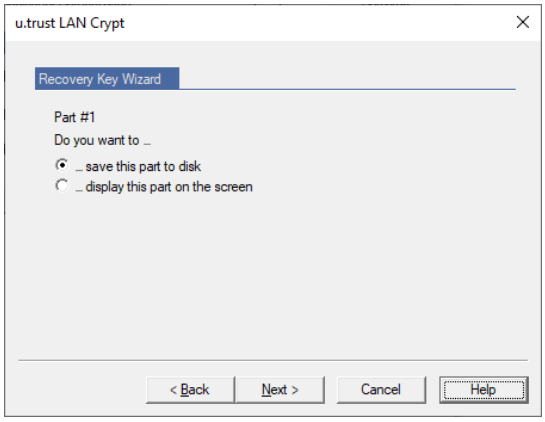
この例では、キーは 3 つの部分に分かれており、そのうち少なくとも 2 つは、ログオン時に新しいセキュリティオフィサー証明書を割り当てるために必要です。



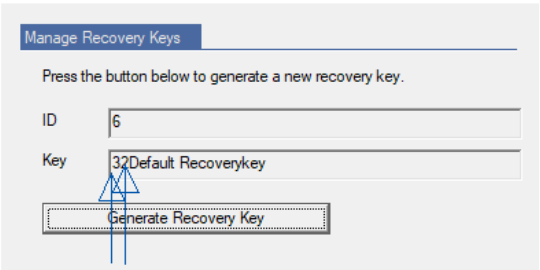
ドロップダウンメニューを使用して、キーに含まれる部分の数と、リカバリーキーを使用するために必要な部分の数を選択します。この例では、キーには 3 つの部分があり、そのうち少なくとも 2 つは、ログオン時に新しいセキュリティオフィサー証明書を割り当てるために必要です。

次へをクリックします。

キーの各部分について、ウィザードはダイアログを表示し、部分キーをファイルに保存するか、画面に表示して書き留めるかを指定できます。すべての部分が処理されると、ウィザードは閉じます。



表の一番下、デフォルトリカバリーキーエントリーのすぐ左にあるリカバリーキータブで、キーがいくつの部分で構成されているのか（前述の例では 3 つの部分）、また、そのうちのいくつの部分を使用する必要があるのか（前述の例では 2 つの部分）を確認できます。



注意：リカバリーキーのパーツを生成し配布する際には、極めて機密性の高いデータが含まれることを忘れないでください。リカバリーキーを不正アクセスから保護することが不可欠です。

注意：使用できるのは、最近生成されたリカバリーキーのみです。以前に生成されたリカバリーキーは無効となり、証明書を割り当てるために使用することはできません。

リカバリーキーの使用

u.trust LAN Crypt データベースにログオンできなくなった場合（証明書の有効期限が切れた場合など）、ログオンダイアログで証明書の割り当てをクリックし、リカバリーキーウィザードを起動します。

セキュリティオフィサーを選択した後、証明書が使用できないことを知らせるダイアログが表示されたら、そこからウィザードを開始できます。

画面の指示に従ってください。

リカバリーキーの設定（クラシックまたは KMIP キーサーバー経由）に応じて、ウィザードはマスターセキュリティオフィサーが u.trust LAN Crypt 管理コンソールに再度アクセスできるようにするための新しい証明書を作成するためのダイアログを表示します。

このウィザードには、追加承認の設定を変更するために必要なセキュリティオフィサーの数を 0 にリセットするダイアログがあります。

これにより、追加承認を行えるセキュリティオフィサーがいないために、追加承認が行えなくなるような事態は起こりえません。

このオプションを有効にすると、1 人のセキュリティオフィサーが後から追加認証の設定を変更することができます。

3.5.11 データベースタブ

注意：この設定は、異なるマシンの管理コンソールからアクセスする Oracle データベースを使用する場合にのみ必要です。この設定はマスターセキュリティオフィサーのみが行うことができます。

Oracle の言語サポート（NLS）は、文字セットが異なるために文字の数値エンコーディングが異なっていても、どの文字セットが使用されていても常に同じように表示されるように、ユーザーのためにテキストを変換します。

例　WE8MSWIN1252：ü=FC00、AL16UTF16：ü=7C00

テキストがデータベースに追加され、異なる文字セットを使用して抽出された場合、チェックサム（MAC）を計算する際にエラーが発生する可能性があります。例えば、文字がバイナリに変換された場合、バイナリデータが MAC の問題を引き起こす可能性があります。

このようなエラーを回避するには、Oracle クライアントを介してデータベースにアクセスするすべてのマシンで同一のコードページ/文字セットが使用されていることを確認してください。

データベースタブでは、データベースにアクセスするすべてのマシンで使用する文字セットを指定できます。u.trust LAN Crypt は、管理コンソールの起動時に、Oracle クライアント

の設定がデータベースの設定と一致しているかどうかをチェックします。一致しない場合は警告が表示され、管理コンソールは起動しません。

編集フィールドに、データベースへのログインを許可するために Oracle クライアントで使用する文字セットを入力します。Oracle クライアントでは、この設定はレジストリの NLS_Lan (Language.Territory.CharacterSet、例: GERMAN_GERMANY.WE8MSWIN1252)にあります。

現在のマシンの文字セットは、[データベース]タブの[INFO:]に表示されます。通常、この文字セットはデータベースにアクセスする他のすべてのクライアントでも使用する必要があります。

注意：1 文字セットのみを使用することをお勧めします。文字以上の文字セットを使用すると、チェックサム (MAC) を計算する際にエラーが発生する可能性があります。ただし、一般的には複数の文字セットを使用することは可能です。ただし、文字セットがほとんど同じで、数文字しか違わない場合にのみ、複数の文字セットを使用するようにしてください。これらの文字を識別し、データベースエントリーに使用しないようにしてください。

このチェックの無効化

u.trust LAN Crypt では、文字セットチェックを無効にすることができます。編集フィールドが空白の場合、チェックは実行されず、常に管理コンソールにログオンすることができます。この場合、チェックサム(MAC)の計算時にエラーが発生する可能性がありますのでご注意ください。

文字セット指定時のエラー（入力ミスなど）により、設定を行ったマスターセキュリティオフィサーが管理コンソールにログオンできなくなる事態を防ぐため、u.trust LAN Crypt では、適用または OK を押した際に入力されたデータをチェックします。指定された文字セットがこのマシンで現在使用されている文字セットと一致しない場合、メッセージが表示され、現在有効な文字セットが編集フィールドに追加されます。入力されたデータを確認するために、[データベース]タブが画面に表示され、必要に応じて設定を変更し、もう一度適用または OK を押します。

3.5.12 アンチウイルスタブ

ウイルススキャナが u.trust LAN Crypt で暗号化されたファイルをスキャンできるようにするには、ここでスキャナを指定する必要があります。ここに入力されたアンチウイルスソフトは、暗号化されたファイルへのアクセスが明示的に許可され、u.trust LAN Crypt で暗号化されたファイルであってもスキャン中にウイルスシグネチャを認識することができます。

ウイルス スキャナを追加するには、[追加]をクリックします。表示されるダイアログに次のデータを入力します：

- アンチウイルスソフトウェアの名前(この名前は、[製品の[アンチウイルス]タブに表示されます)。
- ウイルススキャンを実行する実行可能ファイルの名前。

ウイルススキャナが u.trust LAN Crypt クライアントポリシーファイルのロードプロセスを遅延させるのを防ぐには、クライアント暗号化ルールがロードされるときにすでにアクティブになっているか、ウイルススキャンを実行する実行ファイルへのパス (EXE ファイル名)

を含むようにアンチウイルスプロセスを設定します。パスにワイルドカードを使用することもできます。

例

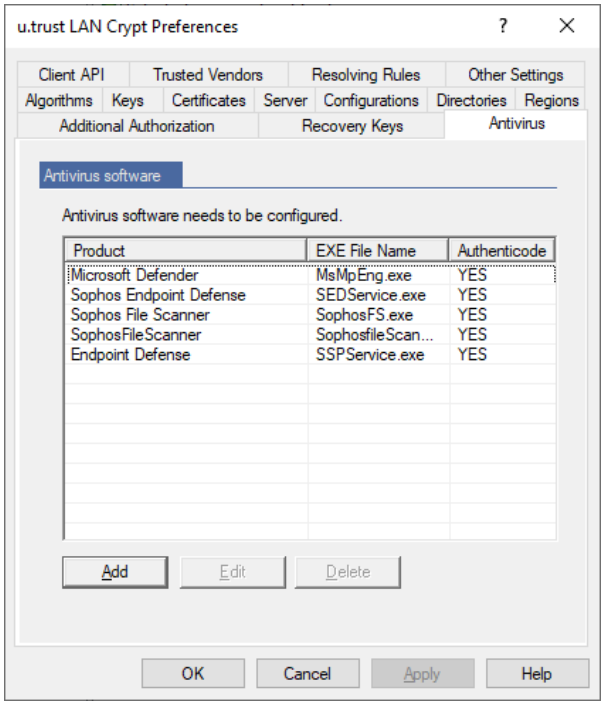
Microsoft Windows Defender

注意： この時点でパスを含めないと、ポリシーファイルの読み込み時間が長くなります。

Authenticode 検証オプションを有効にします。

注意： ここでスキャナを指定し、Authenticode の検証を有効にするには、Authenticode 署名付きウイルススキャナを使用することをお勧めします。この検証によってのみ、実行可能ファイルが本当にウイルススキャナの必要な実行可能ファイルであること、および信頼できるアプリケーションだけが暗号化されたファイルへの明示的に必要なアクセスを与えられることが保証されます（信頼できるベンダータブを参照）。

OK をクリックすると、アンチウイルスソフトウェアがリストに表示されます。さらにウイルススキャナを追加できます。



3.5.13 クライアント API タブ

u.trust LAN Crypt は、アプリケーションがファイル暗号化機能をシンプルなコマンドラインまたは COM スタイルの API で制御できるように、クライアント API を提供しています。詳細は、解凍したインストールパッケージの"api"フォルダにあるクライアント API ドキュメント(PDF)を参照してください。

注意： u.trust LAN Crypt クライアントのインストール時に API を選択する必要があります。クライアント API をクライアントで使用したい場合は、正しくインストールされていることを確認してください。

Client API タブでは、Client API の設定を指定します。

- クライアントで API を使用できるようにするには、[Enable Client API] を選択します。アプリケーションは、COM スタイルの API を介してファイル機能を制御できるようになります。
- LAN Crypt ファイル暗号化コマンドラインツールの API アクセスを有効にする を選択すると、シンプルなコマンドラインツールでファイル暗号化機能を制御できるようになります。
- API ルールが暗号化ルールより優先：デフォルトでは、u.trust LAN 暗号化管理で定義された暗号化ルールが、クライアント API 経由で実行された暗号化タスクより優先されます。API ルールを優先したい場合は、プロファイルで API ルールを暗号化ルールより優先するオプションを選択します。

> 注意：u.trust LAN Crypt の無視ルールと除外ルールは最優先され、API ルールによって優先されることはなく、同じファイル/フォルダは自動的に暗号化から除外されます（9 ページの暗号化から除外されるファイル/フォルダを参照）。

API へのアクセスは許可されたアプリケーションに制限されるため、使用を許可するアプリケーションを指定する必要があります。そのためには、下記を行います。

1. クライアント API タブの［追加］をクリックします。
2. クライアント API の使用を許可するアプリケーション名を指定します。
3. u.trust LAN Crypt Client API にアクセスする実行ファイルを指定します。
4. Authenticode 署名された実行ファイルのみで API にアクセスする場合は、[実行ファイルには Authenticode 署名が必要です]オプションを選択します。
5. 信頼できるベンダーによって署名された実行可能ファイルのみを使用する場合は、[実行可能ファイルは信頼できるベンダーによって Authenticode 署名されている必要があります]オプションを選択します。これにより、[信頼されたベンダー]タブでベンダーの署名証明書として登録されている証明書を使用して署名された実行ファイルのみが了解しられるようになります。
6. コメントを入力することもできます。

OK をクリックすると、アプリケーションがリストに表示されます。さらにアプリケーションを追加できます。

3.5.14 信頼できるベンダータブ

信頼済みベンダータブでは、クライアント API にアクセスするための実行ファイルに Authenticode 署名するベンダーを登録できます。

信頼できるベンダーを追加するには

1. 信頼できるベンダータブの[追加]をクリックします。
2. 業者名を入力してください。
3. ベンダーの署名証明書を入力します。
   クライアント API タブで選択すると、API は、この証明書を使用して Authenticode 署名された実行可能ファイルのみを了解します。

4. コメントを入力することもできます。

OK]をクリックすると、ベンダーがリストに表示されます。さらにベンダーを追加できます。

3.5.15 その他の設定タブ

セキュリティオフィサーのオプション

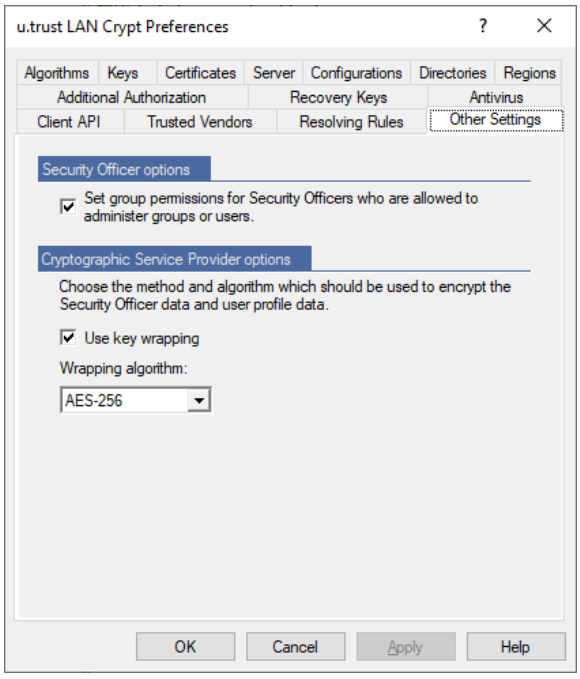
u.trust LAN Crypt は、新しく作成されたセキュリティオフィサーのルートグループの閲覧権限を持つ ACL を自動的に作成するように設定できます。要件は、セキュリティオフィサーが Administer groups または Administer users のグローバル権限を持っていることです。これにより、セキュリティオフィサーは、担当するすべてのグループにアクセス（表示および/または編集）できることが保証されます。

グループまたはユーザーの管理が許可されているセキュリティオフィサーのグループ権限を設定するオプションを選択すると、ルートグループの ACL が自動的に作成されます。

注意： グループからセキュリティオフィサーを削除する場合、ルートグループであるメインのグループノードでのみ可能です。

暗号サービスプロバイダのオプション

キーラッピングを使用する（デフォルト設定）を選択した場合、セキュリティオフィサーのデータとユーザープロファイルデータは、選択したアルゴリズム（デフォルトは AES-128）によるランダムなセッションキーを使用して暗号化されます。このセッションキーは、証明書の公開キーで再び RSA 暗号化されます。



スマートカードを使用する場合は、使用するスマートカードが選択したアルゴリズムに対応していることを確認してください。

このオプションを選択しないと、データはセッションキーなしで RSA 暗号化されます。このオプションは、スマートカードやミドルウェアではサポートされていない可能性があることに注意してください。

注意：選択したアルゴリズムがサポートされていない場合、ポリシーファイルを読み込むときにエラー　メッセージが表示されます。この場合、アルゴリズムを変更するか、使用しているスマートカードまたはミドルウェアでサポートされている適切なアルゴリズムを選択します。

3.6 すべての u.trust LAN Crypt キーの表示

すべての u.trust LAN Crypt キーノードを選択すると、u.trust LAN Crypt が現在管理しているすべてのキーの概要が表示されます。ここでは以下の情報を見ることができます。

- ロングキー名
- キーに使用するアルゴリズム
- キーが有効になっているかどうかの情報
- キーを作成した人（Creator）に関する情報
- キーを継承するかどうかの情報
- キーがどのグループのために作成されたかについての情報
- キーが使用中かどうかの情報
- コメント欄に関する情報

デフォルトの表示では、各グループで作成されたすべてのキーが表示されます。すべての u.trust LAN Crypt キーノードを右クリックすると、コンテキストメニューが表示され、既存のグループキー（<GROUPKEY>）やユーザーキー（<USERKEY>）など、特定のキーが表示されます。

列のヘッダーをクリックすると、表の内容を昇順または降順に並べ替え、必要な情報を見つけることができます。

3.6.1 キーの検索

キー情報の並べ替えだけでなく、特定のキーを検索することもできます。これを行うには、すべての u.trust LAN Crypt キーノードを右クリックし、コンテキストメニューからキーの検索を選択します。

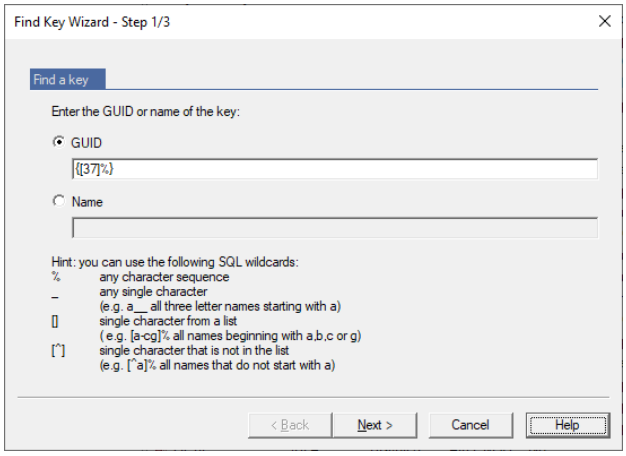
注意：キーの検索機能は、各グループのグループキーノードでも使用できます。キーをグループに追加するには、そのキーが属するグループのキーのコピーと、そのキーを追加するグループのキーの作成が必要です。

キーがどのグループにも属さない場合、キーの検索機能を使用するセキュリティオフィサーには表示されません。マスターセキュリティオフィサーだけが、そのようなキーをグループに割り当てることができます。

ウィザードが起動し、目的のキーを検索します。ステップ 1 では、キーを GUID で検索するか、名前で検索するかを指定します。これには、特定の SQL プレースホルダを使用できます。

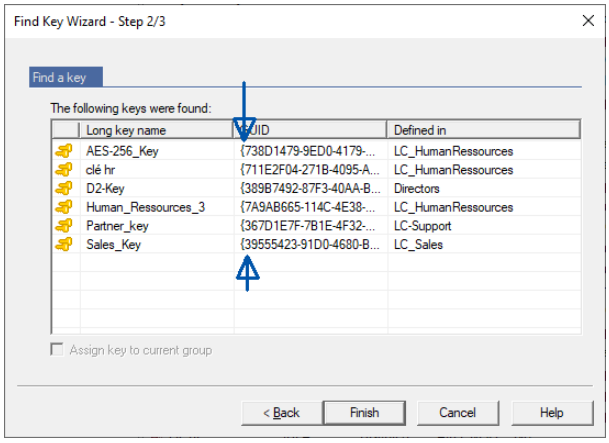
例

{37]%}は GUID が 3 または 7 で始まるすべてのキーを返します。



次に、次へをクリックして、必要なキーをデータベースから検索します。

キーが見つかった場合、ステップ 2 でキーの名前、GUID、生成されたグループが表示されます。



グループ内のグループキーノードからキーの検索機能を呼び出した場合は、現在のグループにキーを割り当てるオプションを有効にして、見つかったキーへのリンクを作成します。すると、別のグループで生成されたキーを、現在選択しているグループで使用することができます。このオプションを有効にして、[次へ]をクリックし、手順 3 で[閉じる]をクリックすると、該当する現在のグループの[グループのキー]ノードに特別なキーのアイコンが表示されます。これで、暗号化ルールでこのキーを使用できるようになります。

注意：現在のグループからキーを割り当てるオプションを選択した場合、すべての u.trust LAN Crypt キーノードからではなく、グループ内のグループのキーノードからキーの検索機能を呼び出した場合にのみ有効です。また、特定のキーを選択することはできますが、現在のグループには割り当てられません。選択したキーに特定のキーが含まれている場合、ウィザードの最終ページに対応するメッセージが表示されます。

3.7 選択されたユーザーと証明書の表示

選択されたユーザーと証明書]ノードは、u.trust LAN Crypt 管理コンソールのユーザー設定で[選択されたユーザーと証明書]を表示するオプションが有効な場合にのみ表示されます（ユーザー設定を参照）。

選択したユーザーと証明書]をクリックすると、表示するユーザーを選択するためのダイアログが表示されます。すべてのユーザーを表示するのは非常に時間がかかるため、u.trust LAN Crypt では検索条件を定義して検索プロセスをフィルタリングすることができます。

注意：システムがユーザーリストをキャッシュするように設定されている場合、新しい検索条件を入力できるようにするには、ツールバーに表示されているアイコンを使用するか、最初に F5 キーを押して表示を更新する必要があります。

検索条件を定義する入力フィールドを有効にするには、[一致するユーザーを表示] オプションを選択します。

u.trust LAN Crypt データベースから以下のユーザー情報が取得されます：

- ログオン名
- ユーザー名
- ユーザーと証明書の間の割り当て
- 証明書の請求者
- 証明書のシリアル番号
- 証明書の有効期限
- 証明書の有効期限
- 親グループ名

u.trust LAN Crypt は、検索されたユーザー属性に定義された文字列を検索します。

最初のドロップダウンリストでは、検索処理を適用する属性を選択できます。

さらに、選択された属性が入力された文字列と一致しなければならないか、または選択された属性が入力された文字列と一致しないユーザーのみが表示されるかを定義することができます。

右側のドロップダウンリストに、u.trust LAN Crypt が検索する文字列を入力します。

文字列の入力には、以下の SQL ワイルドカードを使用できます。

%	任意の文字列
_	一文字 (例: a__ は、"a" で始まる 3 文字を含むすべての名前を検索します)

[ ]	リストから 1 文字 (例: [a-cg]% は、"a"、"b"、"c"、"g" で始まるすべての名前を検索します)
[^]	リストに含まれない 1 文字 (例: [^a]% "a "で始まらないすべての名前を検索)

検索処理の条件は 3 つまで指定できます。

複数の条件を入力する場合、これらの条件をどのように組み合わせるかを定義できます（AND/OR）。

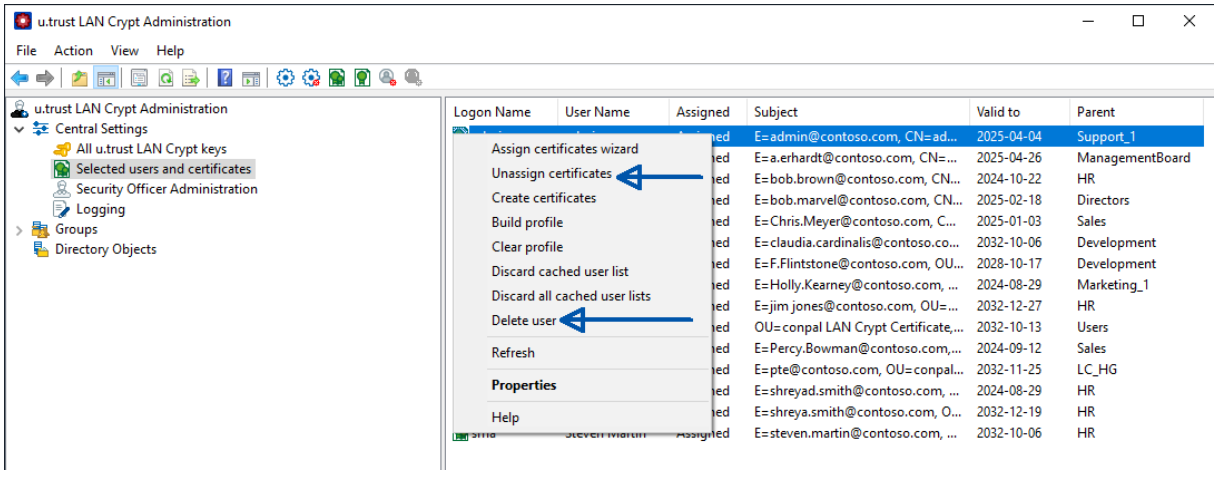
各グループで使用できる証明書スナップインのすべての機能を使用するには、[選択されたユーザーと証明書] ノードを右クリックします（証明書の割り当てを参照）。

この時点では、証明書の割り当てウィザードはマスターセキュリティオフィサーのみが利用できます。セキュリティオフィサーが適切な権限を持っている場合、プロパティメニューを使用して、特定のユーザーに証明書を割り当てることができます。

ただし、セキュリティオフィサーがこのユーザーに対する権限を持っていない場合、対応するアイコンが表示されます。

3.7.1 コンテキストメニューの証明書の割り当て解除およびユーザーの削除メニュー項目

選択したユーザーと証明書]ノードの右側のダイアログ　ボックスに表示されているユーザーについては、1 人以上のユーザーを選択すると、コンテキストメニューから[証明書の割り当ての解除]および[ユーザーの削除]機能を使用できます。ユーザーにまだ証明書が割り当てられていない場合は、そのユーザーのアイコンが灰色表示されていることで識別できます。有効な証明書を既に持っているユーザーは、ユーザーアイコンが緑色で表示されることで認識できます。



コンテキストメニューの証明書の割り当て解除メニュー項目

証明書の割り当て解除]メニュー項目は、緑、黄、または赤のユーザーアイコンが付いているユーザーに対してのみ使用できます。証明書の割り当て解除を使用すると、以前にマーク

されたユーザーの証明書の割り当てを解除できます。その後、ユーザーアイコンの色が灰色に変わります。これらのユーザーには、証明書が割り当てられなくなります。

注意：事項ユーザーアイコンの色が赤で表示されている場合は、このユーザーの証明書の有効期限が切れていることを意味します。一方、ユーザーアイコンの色が黄色の場合は、該当ユーザーの証明書の有効期限が間もなく切れる（設定された警告期間内）ことを意味します。

コンテキストメニューのユーザーの削除メニュー項目

ユーザー削除を実行すると、u.trust LAN Crypt データベースから既存のユーザーを削除できます。ユーザー削除を実行すると、そのユーザーは選択したユーザーと証明書に表示されなくなり、そのユーザーが所属していたグループにも表示されなくなります。

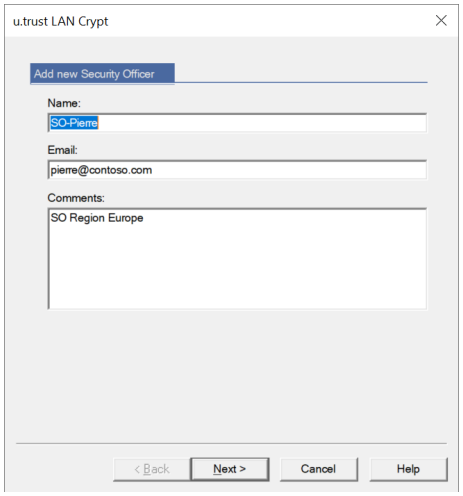
3.8 セキュリティオフィサーの作成

マスターセキュリティオフィサーと資格のあるセキュリティオフィサーは、追加のセキュリティオフィサーを作成することができます。これらのセキュリティオフィサーは、個々の組織単位に割り当てることができます。セキュリティオフィサーには、どのタスクを実行できるかを定義するグローバル権限が付与されます。セキュリティオフィサーを組織単位（u.trust LAN Crypt 管理コンソールのオブジェクト）に割り当てると、ACL を使用して、この特定のオブジェクトに合わせて権限を再度制限することができます。

注意： セキュリティオフィサーのグローバル権限で特定のアクションの実行が許可されていない場合、ACL を使用してこのアクションの権限を付与することはできません。

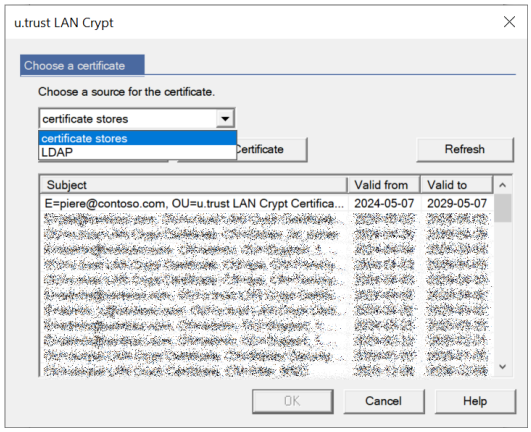
1. 新しいセキュリティオフィサー（SO）を作成するには、セキュリティオフィサー管理ノードを選択します。セキュリティオフィサーを作成するための初回ダイアログを開くには、このノードのコンテキストメニューで新規 SO の追加...をクリックするか、アクションメニューで新規 SO の追加...をクリックします。

2. このダイアログで名前、必要に応じてメールアドレス、コメントを入力します。次に次へをクリックします。



注意： メールアドレスは、u.trust LAN Crypt で生成された証明書のパスワードログファイルに追加されます。例えば、PIN を電子メールで作成する場合などに利用できます。

3. ここで、ダイアログで、新しいセキュリティオフィサーにマスターセキュリティオフィサーの権限を付与するかどうかを指定します。マスターセキュリティオフィサーは常に既存のすべてのグローバル権限を持ちます。参照...ボタンをクリックして、既存の証明書を選択するか、u.trust LAN Crypt で生成された証明書を選択します。



LDAP ソースを使用した証明書の割り当て

u.trust LAN Crypt では、Microsoft Active Directory やその他の LDAP ソースから証明書を割り当てることができます。

証明書の選択ダイアログのドロップダウンリストから[LDAP]を選択します。

LDAP ソースの URL を入力する編集フィールドが表示されます。更新]をクリックすると、LDAP ソースの内容が表示されます。角括弧内のテキスト（[Sub_OU_1]など）は、LDAP ソース内の OU を表します。OU の証明書を表示するには、その OU をダブルクリックします。

...をダブルクリックすると、1 つ上の階層に移動します。

証明書を選択し、OK をクリックします。これで証明書がセキュリティオフィサーに割り当てられました。

注意：LDAP サーバーが匿名ログオンを許可していない場合は、[中央設定]ノードの[サーバー]タブにサーバーのログオン資格情報を入力する必要があります。

注意：u.trust LAN Crypt を使用して暗号化証明書を生成する場合、このセキュリティオフィサーは、生成された *.p12 ファイルから秘密鍵をワークステーションにインポートする必要があります。

暗号化証明書が LDAP ディレクトリから割り当てられた場合は、セキュリティオフィサーのワークステー ションに関連する秘密鍵が存在する必要があります。暗号化証明書は、対称データベースキーへの暗号アクセスに使用されます。

4. または、2 番目の参照 ...ボタンをクリックして、既存の署名証明書を選択するか、u.trust LAN Crypt に新しい署名証明書を生成してもらうこともできます。

注意： u.trust LAN Crypt を使用して署名証明書を生成する場合、このセキュリティオフィサーは、生成された*.p12 ファイルから秘密鍵をワークステーションにインポートする必要があります。

署名証明書が LDAP ディレクトリから割り当てられた場合、関連する秘密鍵がセキュリティオフィサーのワークステーションに既に存在する必要があります。署名証明書は、生成されたプロファイルの署名と、拡張 API ログオン時の認証に使用されます。

5. セキュリティオフィサーにリージョンを設定している場合は、リージョンを選択することができます。

6. もし、リージョンに個別の設定レコードを作成したら、それを選択できます。

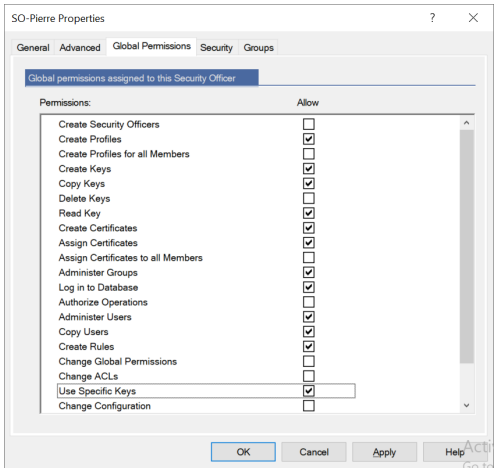
   注意：システムは、選択されたリージョンに対して生成された構成のみを表示します。

7. 次へをクリックします。

8. ウィザードの最後のダイアログで、セキュリティオフィサーが実行できるアクションを指定できます。選択したアクションに必要なグローバルパーミッションはすべて自動的に設定されます。

   これらの権限は、グローバル権限タブの セキュリティオフィサーs プロパティに表示されます（セキュリティオフィサー をダブルクリックすると表示されます）。

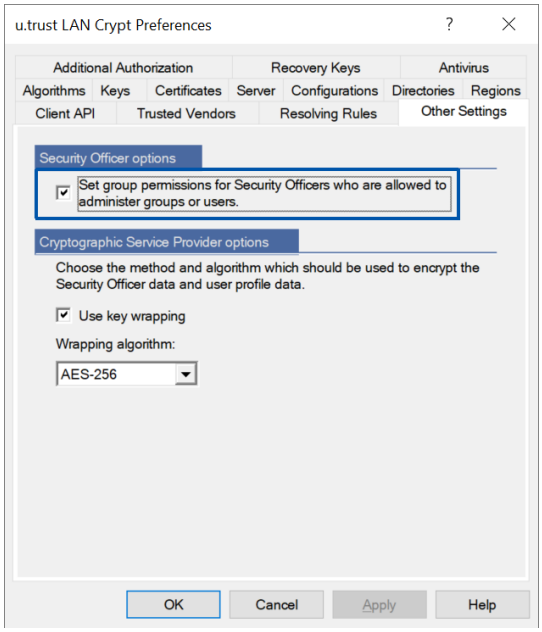
   グローバル権限はこのページで編集できます。



   このダイアログでは、セキュリティオフィサーに特定のアクションの実行を許可すると、そのアクションに必要なすべての権限が自動的に付与されます。

   注意：セキュリティオフィサーがグループを処理するには、追加のパーミッションが必要です。

   u.trust LAN Crypt は、新しいセキュリティオフィサーがこの方法でグローバル権限グループの管理またはユーザーの管理を取得した場合、グループまたはユーザーの管理が許可されているセキュリティオフィサーにグループ権限を設定するオプションが有効になっていれば、このセキュリティオフィサーのルートグループの閲覧権限を持つ ACL を自動的に作成します。これにより、セキュリティオフィサーは、担当するすべてのグループにアクセス（表示および/または編集）できることが保証されます。



グループまたはユーザーの管理が許可されているセキュリティオフィサーのグループ権限を設定する]オプションは、[中央設定]ノードの[その他の設定]タブで有効にできます。

9. 完了をクリックします。

新しいセキュリティオフィサーは、u.trust LAN Crypt 管理コンソールに表示されます。

3.8.1 グローバル権限の付与／編集

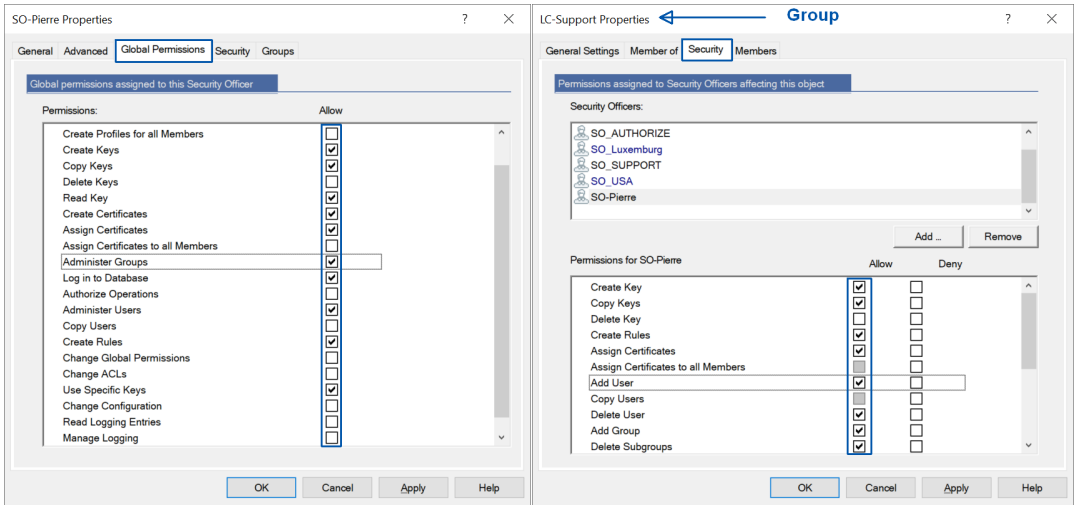
セキュリティオフィサーにはグローバル権限が付与されている必要があります。セキュリティオフィサー管理コンソールノードが選択されている場合、既存のすべてのセキュリティオフィサーが右側のコンソールペインに表示されます。セキュリティオフィサーをダブルクリックすると、セキュリティオフィサーに割り当てられたプロパティを含むタブが開きます。

グローバル権限タブでは、セキュリティオフィサーに u.trust LAN Crypt の管理に必要な基本的な権限を付与します。セキュリティオフィサーが作成されたときに、いくつかのアクションを実行する権限がすでに付与されている場合、これらの必要な権限はすでに有効になっています。

注意： セキュリティオフィサーは、特定のアクションを実行するために、その都度、彼に付与されたグローバル権限に類似した必要なグループ権限も付与されなければならないことに注意してください（セキュリティオフィサーにグループ処理権限を付与するを参照）。

例

セキュリティオフィサーがディレクトリサービスからグループとユーザーをインポートするためには、グローバル権限ディレクトリオブジェクトのインポート、グループの管理、ユーザーの管理に加えて、グループ権限グループの追加とユーザーの追加が必要です。



注意：マスターセキュリティオフィサーは、常に既存のすべてのグローバル権限を持っています。

セキュリティオフィサーには、以下のグローバル権限が付与されます。

注意：すべてのグローバル権限を一度に選択するには、[許可]をクリックします。すべてのグローバル権限の選択を解除するには、もう一度クリックします。

アクセス許可	説明
セキュリティオフィサーの作成	セキュリティオフィサーはセキュリティオフィサーを増員する権限を持っています。
プロファイルの作成	セキュリティオフィサーは、プロファイル リゾルバ を実行し、個々のユーザーのポリシー ファイルを生成するグローバル権限を持っています。このグローバル権限は、セキュリティオフィサー に特定のグループのプロファイルを作成する権限を設定するための前提条件です。プロファイルの作成を使用すると、セキュリティオフィサーは、セキュリティオフィサーがユーザーの親グループのプロファイルの作成権限を持っているユーザーのプロファイルを作成できます（ユーザーの親グループを参照）。 このパーミッションは、キーに値を割り当てるための前提条件です。キーの作成権限のみを持つセキュリティオフィサーは、値のないキーしか生成できません。
全メンバーのプロフィール作成	この権限には、プロファイルを作成する権限が設定されている必要があります。このグローバル権限は、特定のグループに[すべてのメンバーにプロファイルの作成]権限を設定するための前提条件です。すべてのメンバーのプロファイルを作成では、セキュリティオフィサーがユーザーの親グループで［プロファイルの作成］権限、またはユーザーが所属するグループの 1 つで［すべてのメンバーのプロファイルを作成］権限を持っている場合、

	セキュリティオフィサーがすべてのユーザーのプロファイルを作成できます。 注意：グローバル権限プロファイルの作成は、すべてのメンバーのプロファイルの作成の前提条件であるため、以下が適用されます： プロファイルの作成権限を非アクティブにすると、[すべてのメンバーのプロファイルを作成]権限も自動的に非アクティブになります。すべてのメンバーにプロファイルを作成]権限をアクティブにすると、[プロファイルを作成]権限が自動的にアクティブになります。
キーの作成	セキュリティオフィサーは、個々のグループでキーを生成できます。キーの作成権限を持つセキュリティオフィサーは、値のないキーのみを生成できます。管理コンソールでは、値のないキーを暗号化ルールに割り当てることができます。値自体は、ポリシーファイルの生成時に生成されます。値のあるキーを手動で生成するには、セキュリティオフィサーにプロファイルの作成権限が必要です。
キーのコピー	セキュリティオフィサーはキーのコピーを許可されています。
アクセス許可	説明
キーの削除	セキュリティオフィサーは、個々のグループからキーを削除することができます。
キーの読み取り	セキュリティオフィサーは、グループの個別キーのデータを見ることができます。
証明書の作成	セキュリティオフィサーは、ユーザーの証明書を生成できます。
証明書の割り当て	セキュリティ管理者は、ユーザーに証明書を割り当てることができます。セキュリティ管理者は、証明書を割り当てるためのウィザードを実行することができます。 このグローバル権限は、セキュリティオフィサーが特定のグループに証明書を割り当てる権限を設定するための前提条件です。 証明書の割り当てにより、セキュリティ責任者は、セキュリティ責任者がユーザーの親グループの証明書の割り当ての権限を持つユーザーに証明書を割り当てることができます（ユーザーの親グループを参照）。

証明書の割り当て メンバー	この権限には、[証明書の割り当て] 権限が設定されている必要があります。このグローバル権限は、特定のグループに対して［すべてのメンバーに証明書を割り当てる］権限を設定するための前提条件です。すべてのメンバーに証明書を割り当てる] を使用すると、セキュリティオフィサーは、ユーザーの親グループの証明書を割り当てる権限、またはユーザーが所属するグループの 1 つについてすべてのメンバーに証明書を割り当てる権限を持っているすべてのユーザーに証明書を割り当てることができます。 注意：グローバル権限証明書の割り当ては、すべてのメンバーに証明書を割り当てるの前提条件であるため、以下が適用されます。証明書の割り当て権限を無効にすると、[すべてのメンバーに証明書を割り当てる] 権限も自動的に無効になります。すべてのメンバーに証明書を割り当てる]権限をアクティブにすると、[証明書を割り当てる]権限は自動的にアクティブになります。
グループの管理	セキュリティオフィサーは、グループに変更を加えることができます。サブグループの追加、グループの移動、グループの同期、グループの削除。

アクセス許可	説明
ログインデータベース	セキュリティオフィサーは u.trust LAN Crypt データベースにログオンできます。デフォルトの設定では、この権限はアクティブになっています。 この権限により、セキュリティオフィサーは u.trust LAN Crypt データベースを簡単に変更することができます。 この権限は、他の誰かが自分の行動を承認した場合にのみ 。これにより、これらの人は確認が必要な行動しか許可できず、u.trust LAN Crypt に変更を加えることはできません。
オペレーションの承認	セキュリティオフィサーは、確認が必要な行動に参加することができます 。
ユーザーの管理	セキュリティオフィサーは、グループへのユーザーの追加、グループからのユーザーの削除、グループの同期を行うことができます。

ユーザーのコピー	セキュリティオフィサーは、グループにユーザーを追加（コピー）することができます。このグローバル権限は、セキュリティオフィサーが特定のグループにユーザーをコピー権限を設定するための前提条件です。ユーザーをグループに追加するには、セキュリティオフィサーはユーザーの親グループにユーザーをコピー権限を持っている必要があります。
ルールの作成	セキュリティオフィサーは、ユーザーの暗号化ルールを生成することができます 。
グローバル権限の変更	セキュリティオフィサーは、他のセキュリティオフィサーに付与されたグローバル権限を変更することができます 。
ACL の変更	セキュリティオフィサーはグループの ACL を変更することができます。
特定のキーの使用	セキュリティオフィサーは、暗号化ルールで特定のキーを使用したり、すべての u.trust LAN Crypt キーで特定のキーを表示したりできます。
設定の変更	セキュリティオフィサーは構成（パス）を変更できます。この権限は、中央設定の構成タブを表示するために必要です。また、セキュリティオフィサーがデータベースにログオンしている場合、ディレクトリタブで変更を行うことができます。
ロギングエントリーの読み込み	セキュリティオフィサーは、ログに使用される設定とログに記録された イベントを表示できます。

アクセス許可	説明
ログの管理	セキュリティオフィサーは、ログの設定を変更することができます。アーカイブ、削除、およびエントリーのチェックを許可されています。
ディレクトリオブジェクトのインポート	セキュリティオフィサーは、ディレクトリサービスから OU、グループ、ユーザーをインポートし、u.trust LAN Crypt データベースに追加できます。ディレクトリオブジェクトをインポートする前に、セキュリティオフィサーはグループの管理権限とユーザーの管理権限も必要です。これらはディレクトリオブジェクトのインポート権限が選択されると自動的に設定されます。セキュリティオフィサーがこの権限を持っていない場合、ディレクトリオブジェクトノード（OU、グループ、ユーザーのインポートに使用）は管理コンソールに表示されません。

グローバル権限を付与する際には、以下の点に注意してください。

- セキュリティオフィサーが変更できるのは、セキュリティオフィサーが個人的に所有している権限のみです。
- セキュリティオフィサーは、自分自身の権限を記述した ACL を変更することはできません 。
- 一部の権限は、別の権限を持っている場合にのみ付与されます。このタイプのパーミッションを選択すると、他のパーミッションが自動的に設定されます。
- u.trust LAN Crypt は、新しく作成されたセキュリティオフィサーのルートグループに対して、閲覧権限 を持つ ACL を自動的に作成するように設定できます。セキュリティオフィサーはグローバル権限管理グループまたは管理ユーザーを持っている必要があります。これにより、セキュリティオフィサーは自分が担当するすべてのグループにアクセス（閲覧、編集）できることが保証されます。

  この動作は、中央設定のその他の設定タブで有効にする必要があります。
- セキュリティオフィサーが変更され、グローバル権限管理グループまたは管理ユーザーのいずれかを受け、ルートグループの ACL を持っていない場合、その ACL が作成されます。ACL にはグループの表示権限があります。既存の ACL は変更されません。

セキュリティオフィサーに付与するグローバル権限を選択し、適用をクリックします。

OK をクリックしてダイアログを閉じます。

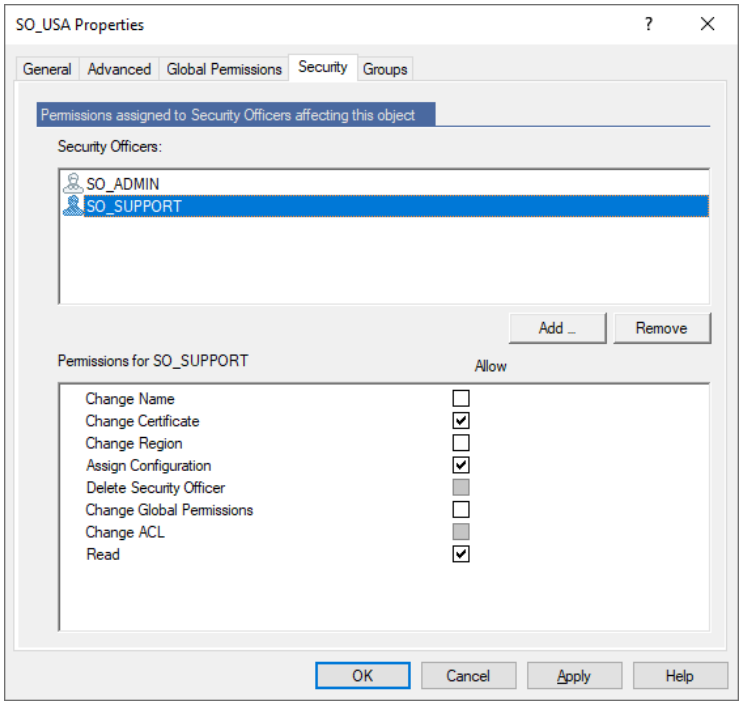
3.8.2 セキュリティオフィサーの設定変更権限

セキュリティオフィサーの設定を変更する権限は、他のセキュリティオフィサーに譲渡することができます。この権限は、セキュリティオフィサーに特別に付与する必要があります。

注意：マスターセキュリティオフィサーはいつでもこれらの設定を変更することができます。

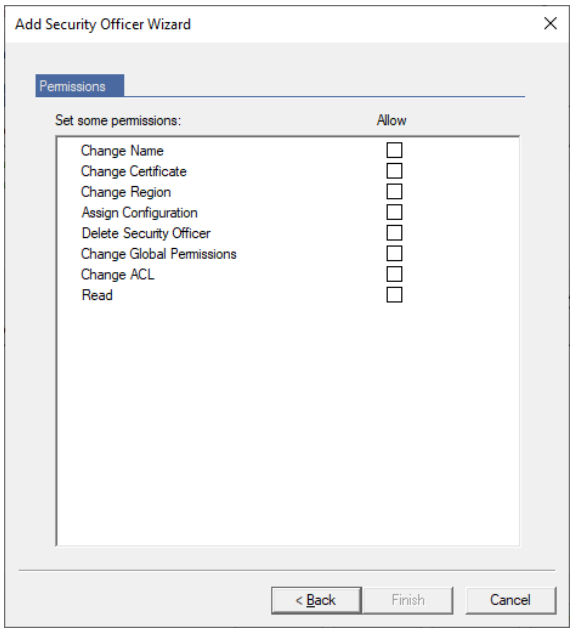
特定のセキュリティオフィサーが持つグローバル権限によって、他のセキュリティオフィサーに対して変更できる権限が決まります。さらに、ある機能を実行するために、複数の権限が必要な場合もあります。例えば、あるセキュリティオフィサーに他のセキュリティオフィサーを削除する権限を与える場合、このセキュリティオフィサーはグローバル権限 ACL の変更とセキュリティオフィサーの作成を持っている必要があります。

セキュリティタブでは、他のセキュリティオフィサーがこのオブジェクト（セキュリティオフィサー）に対して持つ権限を定義することができます。ダイアログの上部には、このセキュリティオフィサーの設定を変更する権限を持つセキュリティオフィサーが表示されます。



1. 追加をクリックして、セキュリティオフィサーを追加するウィザードを実行します。ウィザードの最初のページで、既存のセキュリティオフィサーのリストから必要なセキュリティオフィサーを選択します。

2. ［次へ］をクリックすると、このオブジェクトを変更するための現在のセキュリティオフィサー（現在設定が処理されているセキュリティオフィサー）の権限を指定するページが表示されます。

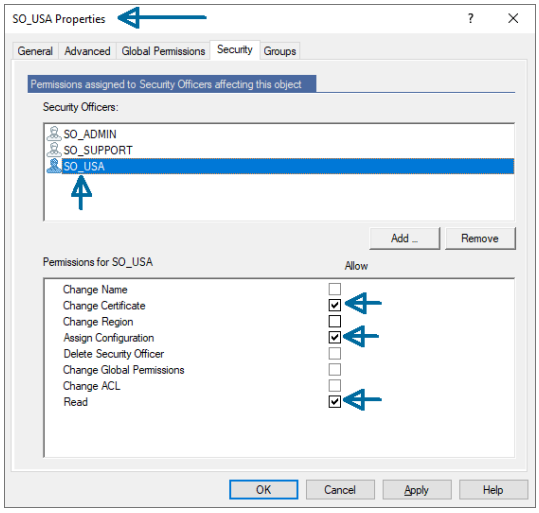


注意： すべての権限を一度に選択するには、［権限］をクリックします。もう一度クリックすると、すべてのグローバル権限の選択が解除されます。グローバル権限設定では、セキュリティオフィサーに無効な権限を付与できないように指定します。

アクセス許可	説明
名前の変更	権限の所有者が割り当てられたセキュリティオフィサーの名前の変更を許可します。
証明書の変更	権限の所有者が割り当てられたセキュリティオフィサーの証明書の変更を許可します。
リージョンの変更	権限の所有者が割り当てられているセキュリティオフィサーのリージョンプレフィックスの変更を許可します。
設定の割り当て	権限の所有者が割り当てられているセキュリティオフィサーの設定の変更を許可します。
セキュリティオフィサーの削除	権限の所有者が割り当てられているセキュリティオフィサーに削除を許可します。
グローバル権限の変更	権限所有者が割り当てられているセキュリティオフィサーのグローバル権限の変更を許可します。
ACL の変更	権限所有者が割り当てられている ACL のグローバル権限の変更を許可します。

アクセス許可	説明
読み取り	権限の所有者に割り当てられているセキュリティオフィサーが表示されます。 これは、このセキュリティオフィサーの処理を許可するすべての権限の前提条件です。 これは、そのタイプの権限が選択されると自動的に設定されます。

また、ここでプロパティが定義されているセキュリティオフィサーに、権限証明書の変更、設定の割り当て、読み取りを付与することもできます。これを実行する前に、そのセキュリティオフィサーは、このオブジェクトの権限を持っているセキュリティオフィサーのリストに存在している必要があります（この場合、特定のセキュリティオフィサー）。



読み取り

中央設定ノードで指定したセキュリティオフィサーを表示します。セキュリティオフィサーは、自分に与えられた権限を確認できます。

設定の割り当て

セキュリティオフィサーは、自分自身に異なる設定を割り当てることができます。

変更証明書

この権限の前提条件は読み取り許可です。セキュリティオフィサーが自分の証明書を変更できるようにします。

注意：チェックボックスが灰色で表示されている権限は、選択したセキュリティオフィサーに必要なグローバル権限がないため、付与できません。

3. チェックボックスをクリックしてセキュリティオフィサーに適切な権限を付与し、終了 をクリックします。これで、セキュリティページの上部ペインにセキュリティオフィサー が表示されます。ページの下部ペインには、選択したセキュリティオフィサーの権限が ACL で表示されます。

3.8.3 特定のセキュリティオフィサーのグループ/OU のすべての権限

特定のセキュリティオフィサーの権限を、そのセキュリティオフィサーが何らかの権限を持っているすべてのグループ/OU について表示するには、セキュリティオフィサー管理ノードに移動し、該当するセキュリティオフィサーをダブルクリックします。

セキュリティオフィサーのプロパティダイアログで、グループタブを選択します。このタブには、2 つのリストビューがあります。

- 上部のリストビューには、このセキュリティオフィサーが 権限を持っているすべてのグループ/OU が表示されます。
- 番目のリストビューには、選択したグループ/OU のセキュリティオフィサーの対応する権限が表示されます。

こうすることで、組織構造において、特定のセキュリティオフィサーがさまざまなグループに対して持っているすべての権限の概要を簡単に把握することができます。

注意：このビューでは、セキュリティオフィサーの権限を変更することはできません。権限の変更は、グループのプロパティダイアログでのみ可能です。

注意：セキュリティオフィサーが権限（許可または拒否）を持つグループのみが表示されます。セキュリティオフィサーが権限を継承しているグループは表示されません。

3.8.4 MSO 証明書または SO 証明書の変更または更新

(M)SO 証明書を変更または更新するさまざまな方法について、以下に説明します。

バリエーション 1：セキュリティオフィサー管理部門

1. u.trust LAN Crypt 管理コンソールを起動し、マスターセキュリティオフィサーとしてログオンします。このセキュリティオフィサーが関係するセキュリティオフィサーの証明書を変更する権限を持っている場合、セキュリティオフィサーとしてログオンすることもできます。また、セキュリティオフィサー自身が適切な権限を持ち、証明書が有効であれば、セキュリティオフィサー自身としてログオンすることもできます。

2. 中央設定ノードに切り替え、そこからセキュリティオフィサー管理コンソールノードに移動します。

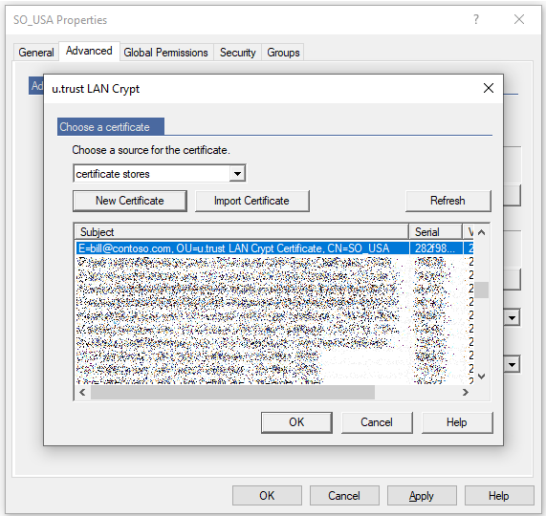
3. 該当するセキュリティオフィサーを右クリックし、コンテキストメニューからプロパティ項目を選択します。

4. 詳細タブに移動します。

5. 暗号化証明書で［参照...］ボタンをクリックして、セキュリティオフィサーの新しい暗号化証明書を選択します。

6. また、署名証明書（オプション）にアクセスし、参照...をクリックして、セキュリティオフィサーの新しい署名証明書を選択することもできます。

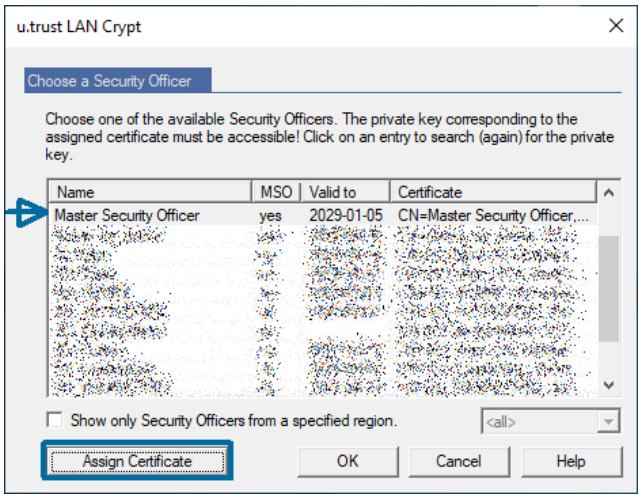
7. 希望の証明書を選択するか、新しい証明書を選択または作成します。または、既存の証明書をインポートすることもできます。セキュリティオフィサーの証明書を選択したら、［OK］をクリックします。



注意：セキュリティオフィサー の署名証明書を変更できるのは、バリエーション 1 のみで、バリエーション 2 ではできません。

バリエーション 2: 復元キーの使用

1. u.trust LAN Crypt 管理コンソール を起動します。
2. セキュリティオフィサーダイアログウィンドウで、必要な(M)SO を選択します。
3. 証明書の割り当てボタンをクリックし、リカバリーキーウィザードの指示に従います。



通常はバリエーション 1 を使うべきです。バリエーション 2 は主に代替方法を意図しており、 適切な権限を持つセキュリティオフィサーが u.trust LAN 暗号化管理にログオンできない場合に使うべきです。

注意：バリエーション 2 の前提条件は復元キーが存在することです。

どの方法を使用する場合でも、古い証明書の有効期限が切れる前に、セキュリティオフィサーによって生成されたプロファイルが再生成されるようにする必要があります。そうしないと、クライアントはプロファイルをロードできなくなります。

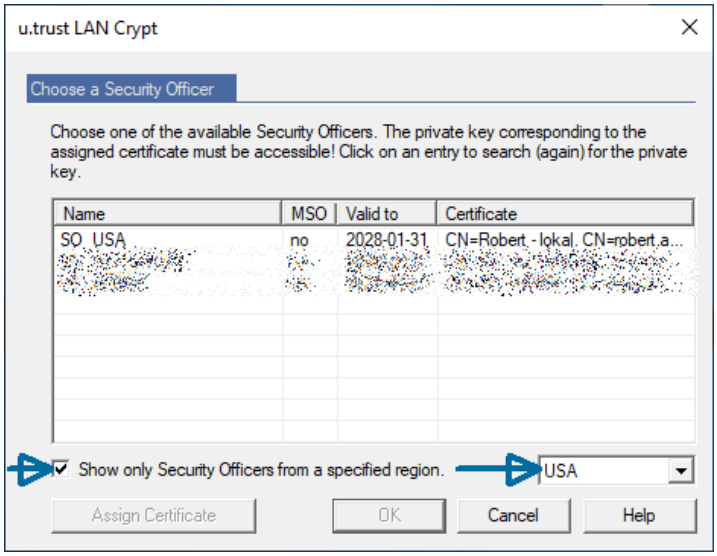
ただし、追加権限のみで証明書の割り当てを許可することもできます。このタイプの割り当ては、セキュリティオフィサーの証明書が変更されたときに影響することを覚えておく必要があります。

3.9 管理コンソールコンソールへのログオン

u.trust LAN Crypt 管理コンソールコンソールにログオンするためには、セキュリティオフィサーは データベースにログインするというグローバル権限を持っている必要があります。マスターセキュリティオフィサーは、利用可能なすべての権限が自動的に付与されるため、常にこの権限を持っています。

管理コンソール(スタート ＞ u.trust LAN Crypt 管理コンソール) を実行すると、ログオンダイアログが表示されます。

許可されたすべてのセキュリティオフィサーがリストに表示されます。特定のリージョンからのセキュリティオフィサーのみを表示オプションを選択し、そのリージョンを選択すると、そのリージョンのセキュリティオフィサーのみが表示されます。



ログオンを有効にするには、証明書に属する秘密鍵（ソフトウェア　キーまたはトークン上のキー）にアクセスする必要があります。

必要なセキュリティオフィサーを選択したら、OK をクリックして u.trust LAN Crypt 管理コンソールコンソールを開きます。

リカバリーキー

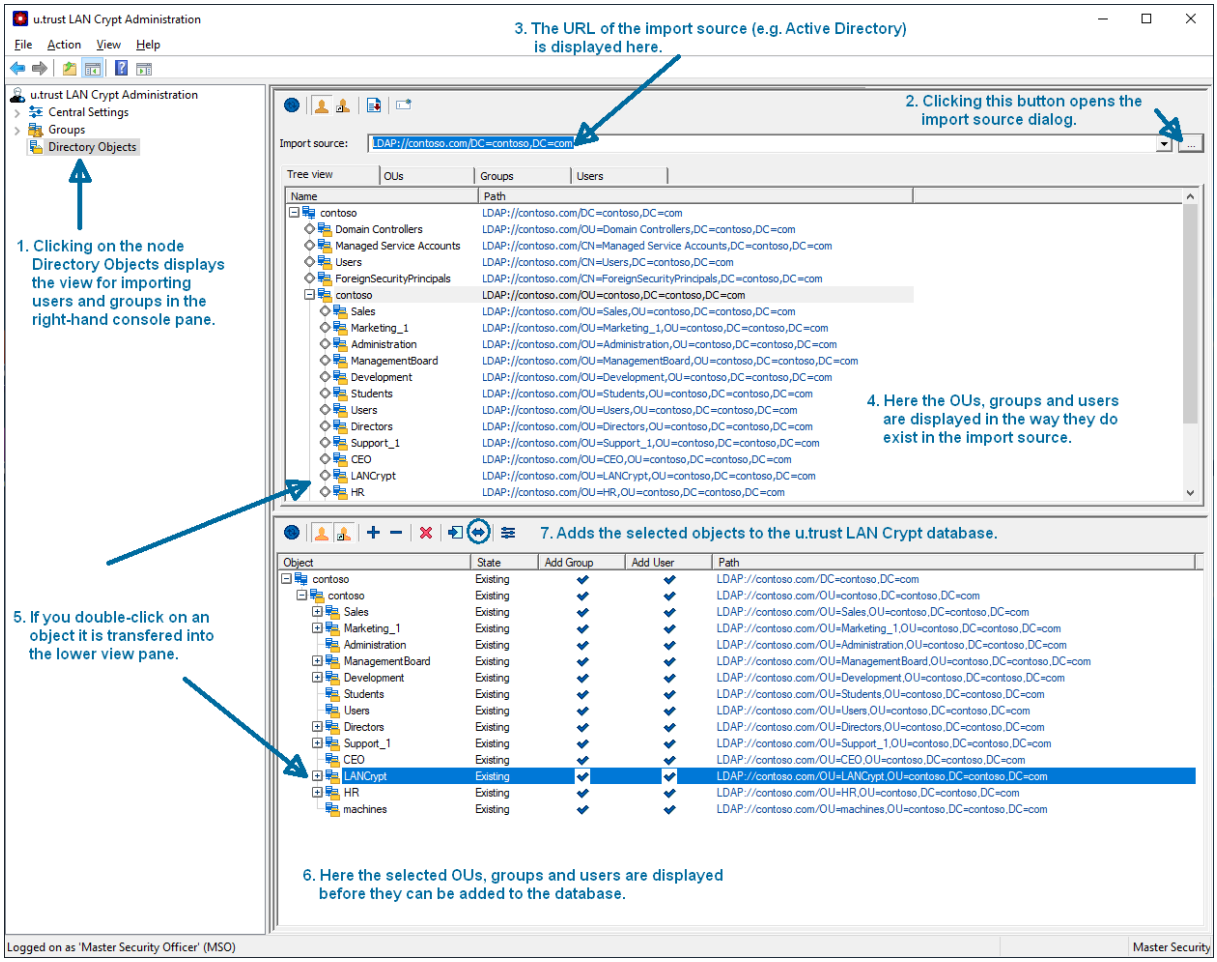
セキュリティオフィサーの証明書に属するキーの有効期限が切れた場合、または破損または紛失した場合、リカバリーキーを入力して証明書を更新します。

注意：復旧プロセス中に新しい証明書が生成された場合、この証明書（および関連するパスワード）は設定されたパスに保存されます。

3.10 グループとユーザーのインポート

u.trust LAN Crypt を使用すると、LDAP 経由で、ドメインからアクセスできるディレクトリサービスからグループとユーザーをインポートしたり、特定の依存関係を持つグループとユーザーを含む手動で作成したファイルからインポートすることができます。

ディレクトリオブジェクトをクリックすると、右側のコンソールペインに　u.trust　LAN Crypt　データベースにインポートするグループのインポートとアセンブルのダイアログが表示されます。



注意：ログオンしているセキュリティオフィサーが［ディレクトリオブジェクト］ノードを表示できない場合は、グローバル権限［ディレクトリオブジェクトのインポート］を持っていないことを意味します。このノードが管理コンソールに表示されるのは、このセキュリティオフィサーがこの権限を持っている場合のみです。

注意：パフォーマンス上の理由から、LDAP 経由でインポートソースを呼び出す場合は、常に FQDN（完全修飾ドメイン名）を使用してください。

3.10.1 ファイルからのグループとユーザーのインポート

ユーザーとグループは、特定の依存関係を持つグループとユーザーを含む手動で作成したファイルからインポートできます。インポートされたグループとユーザーは、u.trust LAN Crypt 管理コンソールコンソールのグループとディレクトリオブジェクトノードに作成されます。

ファイルからユーザーとグループをインポートするには、インポートソースダイアログのファイル検索をクリックします。検索ボタンをクリックすると、u.trust LAN Crypt ダイアログが表示されるので、インポート元のファイルを選択します。

インポートファイルはシンプルなテキストファイルで、特定のファイル拡張子はありません（ のデフォルト拡張子として*.lcg を使用することをお勧めします）。このファイルの内容は特定の要件を満たす必要があります。

インポートファイル形式

インポートファイルはいくつかのセクションで構成されています。セクションは　の任意の数の空白行で区切られます。

各セクションはユーザーまたはグループを表します。

各セクションはヘッダーと、キーワードで始まる一定の行数で構成されます。行の終わりは改行文字でなければなりません。セクション内の行と行の間に他の改行があってはなりません。

ヘッダーは角括弧で囲まれたセクション名です。セクション名は、ユーザーとグループのメンバーシップを定義するために使用されます。

キーワードは、プロパティダイアログに表示されるユーザーとグループのデータを定義します。

キーワード	説明
type=	ユーザー グループ インポートされたオブジェクトがユーザー(USER)を表すか、グループ(GROUP)を表すかを定義します。
name=	ユーザーのログオン名を定義します。u.trust LAN Crypt 管理コンソールコンソールのログオン名に表示されます。
display= 任意	ログオン名と同一でないユーザー名を定義できます。 u.trust LAN Crypt 管理コンソールコンソールのユーザー名として表示されます。 ここで名前を指定しなかった場合、u.trust LAN Crypt 管理コンソールコンソールのユーザー名には、name=に入力したログオン名が表示されます。
mail= 任意	ユーザーのメールアドレスを入力できます。これは、ユーザーのプロパティの[詳細]タブに表示されます。 注意：u.trust LAN Crypt で生成された証明書のパスワードログファイルにメールアドレスが追加されます。例えば、メールで PIN を作成する場合などに利用できます。
members=	グループが使用される場合、これはどのユーザーと他のグループが特定のグループの メンバーであるかを定義します。 メンバーを追加するには、ユーザーまたはグループ（例：U_BKA,G_Utimaco）を識別するセクション名を入力します。 各グループメンバーの名前と の間はカンマで区切ってください。

注意：行頭に // と入力すると、インポートファイルのどこでも、その行にコメントを入力することができます。

注意：インポートファイルの項目は大文字と小文字を区別しません（大文字と小文字を区別しません）。

例

```
[U_RS]
type=USER
name=RS
display=ラルフスミス
mail=ralph.smith@contoso.com
// 私のコメント
[U_PW]
type=USER
name=PW
mail=pw@contoso.com
[U_JG]
type=USER
name=JG
[U_RL]
type=USER
name=RL
[G_COMPANY]
type=GROUP
name＝Company
members=G_QA、G_NI、G_FFM、G_HG、U_RL、U_JG、U_PW、U_RS
// 私のコメント
[G_QA] type=GROUP name=QA members=U_JG, U_PW
[G_PDM] type=GROUP name=PDM members=U_RL, U_RS
```

3.10.2 管理システムのアイコン

現在のウィンドウのビューを更新します。

特定のグループに属するユーザーを表示します。

また、特定のグループに属するグループやユーザーのメンバーシップも表示します。

オブジェクトがグループに直接含まれていないメンバーシップは、灰色で表示されます。

選択したオブジェクトを下のペインに移動します。 を選択オブジェクト上でダブルクリックするのと同じ効果があります。

新しいパスとして使用します。

この設定を使用して、構造の表示方法を制限することができます。ノードが選択された状態でこのボタンをクリックすると、選択されたノードの下の構造のみが表示されます。さらに、パスがドロップダウンリストに追加されるので、この表示にすばやく切り替えることができます。

ツリー構造を表示します。

ツリー構造を閉じます。

選択したオブジェクトをビューから削除します。

右下のペインに表示されているオブジェクトを u.trust LAN Crypt データベースに追加します。

右下のペインに表示されているオブジェクトを、u.trust LAN Crypt データベースに既に存在するオブジェクト と同期させます。

転送オプションを指定するダイアログを開きます。

オブジェクトがインポート元から転送される前に、転送オプションを指定する必要があります。

3.10.3 インポートソースの選択

インポート元入力フィールドに、データを直接インポートするサーバーの URL を入力できます（例：ドメインコントローラ usw-scranton 上の Active Directory ディレクトリサービスの場合、LDAP://usw-scranton/dc=usw-scranton,dc=company,dc=us）。

検索ボタンをクリックすると、u.trust LAN Crypt がインポートソースを選択するダイアログを表示します。

LDAP://

- ドメイン

  コンピュータが Active Directory ドメインのメンバーである場合、このボタンをクリックすると、ドメインコントローラに保存されているドメインの全体の構造が表示されます。

  注意：Active Directory から組み込みグループをインポートすることはできません。そのため、ユーザーを OU（組織単位）またはグループに編成し、代わりにそれらをインポートすることをお勧めします。

- 検索コンテナ

  コンピュータが Active Directory ドメインのメンバーで、検索...を選択した場合、システムは参照...ボタンを表示し、クリックすると別のダイアログが表示されます。このダイアログで、Active Directory 構造内の特定のノードを選択できます。

WinNT://

- コンピュータ

  現在ログオンしているコンピュータのローカルグループとユーザーを表示します。通常、これらのグループとユーザーはテスト目的でのみ使用されます。

- ドメイン

  コンピューターが Windows NT ドメインのメンバーである場合、このボタンをクリックすると、ドメインコントローラーに保存されているドメインの 構造全体が表示されます。

  注意：WinNT プロトコルを使用する場合、WinNT プロトコルはユーザーオブジェクトに一意の GUID を割り当てないため、システムは同期中に名前を変更したユーザーと新しいユーザーを区別できません。

FILE://

- 検索ファイル

  ファイルからユーザーとグループをインポートするには、インポートソースダイアログのファイルの検索...をクリックします。検索ボタンをクリックして、ユーザーとグループをインポートするファイルを選択します。

  ユーザーとグループをインポートするには、インポートファイルが特定の形式である必要があります。インポートファイルの作成方法については、ファイルからグループとユーザーをインポートするページを参照してください。 87).

  インポートソースを選択したら、転送ボタンをクリックして、パスの下にソースへの URL を表示します。

  OK をクリックすると、コンソールの右上のペインに選択したデータが表示されます。このビューでは、選択したデータを OU、グループ、ユーザーごとにツリー構造で表示できます。

LDAP サーバーのみ

管理コンピュータがドメインのメンバーでない場合は、この手順を使用して、グループとユーザーをサーバーからインポートします。

1. サーバーページの中央設定に、サーバー名とユーザー名とパスワードを入力します。

2. LDAP または SSL では、<Microsoft>または <Novell>のどちらの実装を使用するかを指定します。

   注意：Novell ディレクトリサービスからのインポートは LAN Crypt バージョン 3.90 以降サポートされていません。その他の Novell の機能もサポートされなくなりました。

3. インポート元入力フィールドに、データをインポートするサーバーのアドレスを入力します。

3.10.4 u.trust LAN 暗号データベースへの転送準備

右上のコンソールペインには、インポートソースに保存されている OU、グループ、ユーザーが表示されます。

ここで、表示された OU、グループ、ユーザーのうち、u.trust LAN 暗号化データベースにインポートするものを選択できます。まず、選択したオブジェクトを下部のビューペインに移動し、再度処理します。

注意：オブジェクト（ノード）を一番下のビューペインに追加しても、データベースに追加したことにはなりません。このペインでグループ化できるのはオブジェクトだけです。オブジェクトをデータベースに転送するには、データベースに追加または同期をクリックします。

3.10.4.1 データ転送設定の定義

パフォーマンスを最適化するために、転送設定を定義できます。これらの転送設定は、下部のビューペインでの転送にのみ影響し、データをデータベースに転送するための準備を行います。

転送設定アイコンをクリックすると、3 つのオプションがあるダイアログが開きます。

- データベース内のオブジェクトのステータスを計算

  エントリーがすでにデータベースに存在する場合、つまりデータベースが 同期されている場合にのみ適用されます。このオプションを選択すると、各オブジェクトの下部のビューに以下のように表示されます。

  - データベースに既に存在するかどうか。
  - ログオンしているセキュリティオフィサーがグループを変更する権限を持っているかどうか（［グループの追加］列）。赤いチェックは、セキュリティオフィサーがグループを追加する権限を持っていないことを示します。緑のチェックは、セキュリティオフィサーがグループを追加する権限を持っていることを意味します。

- ログオンしているセキュリティオフィサーがユーザーを追加する権限を持っているかどうか（［ユーザーの追加］列）。赤い十字は、セキュリティオフィサーがユーザーを追加する権限を持っていないことを示します。緑のチェックは、セキュリティオフィサーがユーザーを追加する権限を持っていることを意味します。

■ メンバー数の計算

このオプションを選択すると、グループメンバーシップ(個々のグループの直接のメンバーではないグループとユーザー)も表示されます。直接のメンバーと区別するために、灰色のアイコンとして表示されます。

注意：システムが計算できるのは、メンバー数がデータベースに転送されるまでです。

■ オブジェクトの並べ替え

大きなグループでエントリーをアルファベット順にソートするのは非常に時間がかかるため、エントリー は通常ソートされません。オブジェクトをアルファベット順に並べ替えたい場合は、このオプションを選択します。

ビューの更新

転送にオプションが設定されていない場合、再読み込みボタンをクリックすることで、転送後にこれらのアクションを実行できます。再読み込みをクリックすると、同じオプションのダイアログが開きます。更新は、下部のビューペインのデータにのみ影響します。

3.10.4.2 下部ペインへのオブジェクトの移動

ノードをダブルクリックするか、ノードを選択して 転送ボタンをクリックすると、インポートソース構造内のオブジェクトが下のビューペインに転送されます。

オブジェクトが転送される前にダイアログが表示され、個々のコンテナやオブジェクトの転送方法を指定できます。

■ このオブジェクトのみ転送

選択されたオブジェクトをその内容なしで追加します .

■ 直接メンバーも譲渡

選択されたコンテナに存在するすべてのオブジェクトを追加します。

■ 再帰的にメンバーを転送

このコンテナに存在するすべてのオブジェクトと、別のコンテナに存在するメンバーで であるすべてのオブジェクトを追加します。メンバーは、その階層全体とともに転送されます。

必要なオプションを選択し、OK をクリックして、オブジェクトを下部のビューペインに転送し、u.trust LAN Crypt データベースに追加できるようにします。

データベースに転送する前に、このビューにさらにグループを追加し（例えば、他のソースから）、その後 1 つのステップですべてをデータベースに追加することができます。

3.10.4.3 データベースへのデータの追加またはデータの同期

オブジェクトは、下部のビューペインでグループ化され、データベースに追加または 同期ボタンをクリックするまで、u.trust LAN Crypt データベースには追加されません。

注意： 既存の構造体にオブジェクトを追加する場合は、必ずそのオブジェクトをデータベースに追加することから始めなければなりません。これを行うには、データベースに追加ボタンをクリックします。

同期が使われるのは、オブジェクト間の関係だけが変更される場合だけです。

データベースに追加をクリックすると、オブジェクトが追加され、同期プロセスが開始されます。これは、3 つのオプションを持つダイアログから始まります。

- 完全なデータベースの同期

  このオプションを選択すると、u.trust LAN Crypt データベース内のすべてのエントリーがインポートソース内のエントリーと同期されます。変更は次に示す別の画面に表示されます。

  オブジェクトが AD から削除され、 データベースからも削除する必要がある場合は、このオプションを選択します。

  注意：複雑な構造が含まれる場合、完全な同期に時間がかかることがあります。

- 表示されているエントリーのみを同期

  管理コンソールの右下ペインの選択範囲を指します。

- すべてのリレーションシップを再計算

  このオプションを選択すると、インポート元に従ってすべてのメンバー情報が再計算され、データベースに追加されます。右下のコンソールペインの表示がオフになっていても、メンバー資格は追加されます（転送設定のメンバー資格の計算オプションがオフになっている）。

- 可視リレーションシップを使う

  このオプションを選択すると、右下のコンソールペインに表示されているリレーションのみがデータベースに追加されます。非表示のメンバーシップはデータベースに追加されません（転送設定でメンバーシップの計算が無効になっています）。

  注意：同期化中にこのオプションを使用し、データベースに存在するオブジェクトのメンバーシップが右下のコンソールペインに表示されない場合、データベースに存在するメンバーシップはすべて削除されます。

オプションを選択して OK をクリックすると、同期を文書化するダイアログが表示されます。このダイアログで変更を確認する必要があります。

- すべてのエントリー

  すべての変更内容を一覧表示します。他のページのエントリー総数に対応します。

- 削除されたオブジェクト

  最後の 同期以降にインポート元（サーバー）で削除されたが、u.trust LAN 暗号データベースに残っているオブジェクトを表示します。

- ディレクトリの新しいリレーションシップ

  u.trust LAN Crypt データベースに追加されたオブジェクトとメンバーシップ、または前回の同期以降にインポート元（サーバー）で作成され、まだデータベースに転送されていない新しいオブジェクトとメンバーシップが表示されます。

- データベース内の古いリレーションシップ

  データベースにまだ存在するが、 インポート元にはもう存在しないオブジェクトとメンバシップを表示します。たとえば、グループが削除された場合や、サーバー上でメンバシップが変更された場合などです。

注意： 同期の実行では、インポート元からデータベースに少なくとも 1 回インポートされたオブジェクトのみが評価されます。

インポートソースでオブジェクトが削除された場合、[完全なデータベースを同期] オプションが選択されている場合にのみ、これらの変更がデータベースに反映されます。管理コンソールで手動で追加したグループとユーザーは、同期中に評価されないため、これらのページには表示されません。

このビューにリストされている各オブジェクトのアクションをクリックすることで、そのアクションをキャンセルすることができます（チェックを外す）。選択したアクション（チェックが付いているもの）のみが実行されます。OK をクリックして、データ同期の実行を完了します。

OU（組織単位）、グループ、ユーザーがインポートされると、それらを担当するセキュリティオフィサーを各 OU に割り当てることができます。

3.10.4.4 手動でのグループ追加

新しいグループを手動で追加するには、新しいグループを追加するノード/グループを選択し、コンテキストメニューの新規グループをクリックします。

グループ名フィールドに新しいグループの名前を入力し、[OK] をクリックします。u.trust LAN Crypt 管理コンソールコンソールにグループが表示されます。

グループの プロパティ ダイアログでは、既存のユーザーをグループに追加したり、新規ユーザーを作成したりすることができます。

インポートされたグループとは異なり、手動で作成したグループは、グループの階層内でドラッグ アンド ドロップを使用して移動できます。

3.10.4.5 グループ間のリレーションシップ

グループ間のリレーションシップを作成するには、グループをコピーして別のグループに挿入します。

この方法で挿入されたグループは、親グループのショートカットとして表示されます。その結果、挿入されたグループのメンバーは、親グループのすべてのキーと暗号化規則を継承し

ます。キーを継承するための前提条件は、これらのキーが親グループで継承可能であると定義されていることです。グループの編集権は継承されません。

このグループはショートカットとして新しい場所に挿入されるだけなので、暗号化ルール、メンバー、証明書、キーは表示されません。これらの値は、階層内の実際のグループでのみ表示されます。継承されたキーは、そこで暗号化ルールを作成するために使用することもできます。

ショートカットを使ってグループを別のグループに追加するには、下記を行います。

1. 該当するグループを選択し、コンテキストメニューを開き、コピーを選択します。

2. グループを挿入したいターゲットグループを選択し、ターゲットグループのコンテキストメニューから挿入をクリックします。CTRL キーを押しながらグループをターゲットグループにドラッグ＆ドロップしてショートカットを作成することもできます。

3. グループを追加するかどうかを確認するプロンプトが表示されます。OK をクリックして確認します。

4. このグループは他のグループの下にショートカットとして表示されます。

このようにして、あるグループの全メンバーに、別のグループのすべての権限を簡単に付与することができます。

たとえば、チーム 1 のメンバーに、チーム 2 のメンバーと同じ権限を期間限定で与えたい場合 (たとえば、チーム 1 がプロジェクトでチーム 2 をサポートできるようにする場合)、チーム 2 のグループにチーム 1 のグループへのショートカットを追加します。次に、新しいポリシーファイルを生成します。次にチーム 1 のメンバーがログオンすると、チーム 2 のデータにアクセスできるようになります。

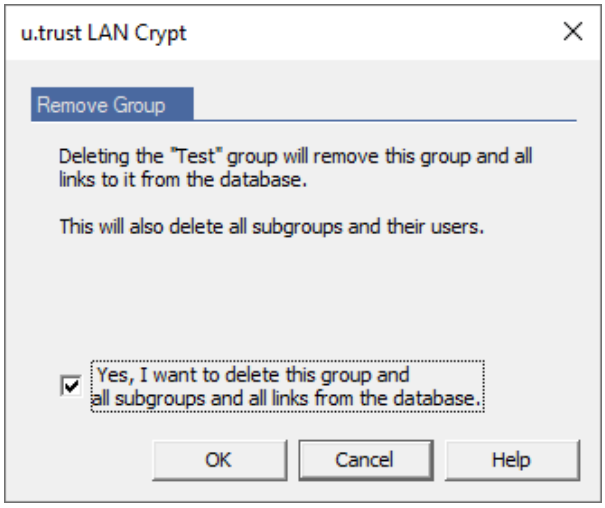
チーム 1 が余分な権限を必要としなくなったら、チーム 2 のグループからショートカットを削除して、新しいポリシーファイルを再度生成できます。チーム 1 のメンバーは、チーム 2 のデータにアクセスできなくなります。

3.10.5 グループの削除

u.trust LAN Crypt 管理コンソールコンソールでは、個々のグループ/OU、およびグループ/OU へのショートカットを削除できます。

グループを削除するには、そのグループのコンテキストメニューから削除を選択します。すべてのサブグループとユーザーのメンバーシップが削除されます。u.trust LAN Crypt 管理コンソールコンソールで OU を削除した場合のみ、ユーザー自体が削除されます。この場合、他の OU に存在するユーザーのメンバーシップも削除されます。キーは決して削除されません。u.trust LAN Crypt データベースに残ります。

グループが削除される前に、ダイアログが表示され、グループを削除することを確認する必要があります。



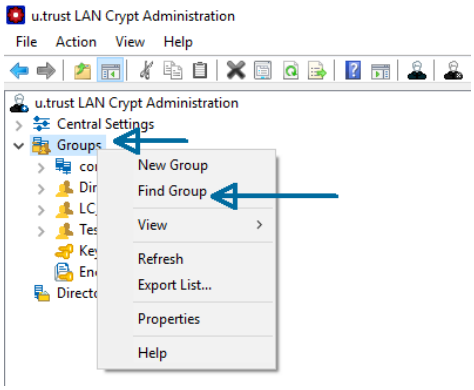
グループへのショートカットを削除するには、ショートカットのコンテキストメニューで削除をクリックします。削除されるのはショートカットだけです。グループ自体には影響しません。ショートカットを削除する前に、削除するかどうかを確認するダイアログが表示されます。

親グループのコンテキストメニューには、削除リンクという項目があり、ショートカットの削除に使用します。

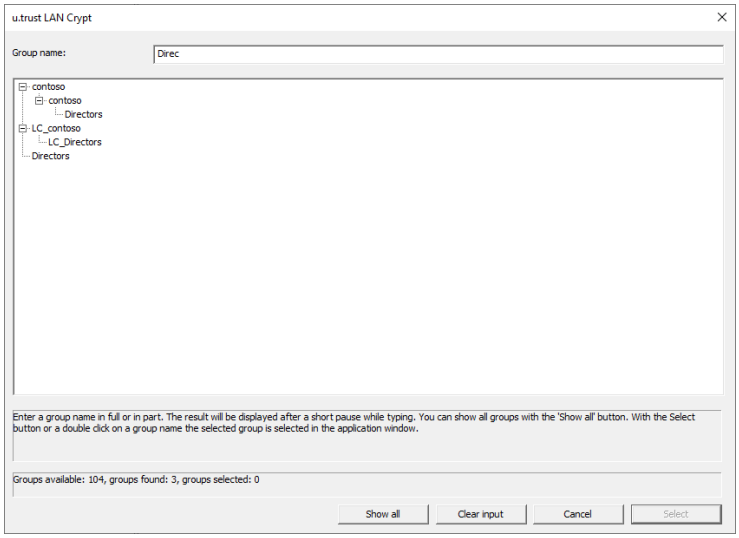
リンクを削除をクリックすると、このグループへのショートカットがすべて削除されます。グループ自体は影響を受けません。

3. 10. 6 グループの検索

グループの検索機能は、特定のグループを検索するのに役立ちます。グループノードを右クリックし、グループの検索を選択します。



以下のダイアログが表示されます。



グループ名入力フィールドに検索したいグループ名の全部または一部を入力します。入力中に少し間があいた後、アプリケーションウィンドウに結果が表示されます。すべてを表示をクリックすると、すべてのグループを表示ウィンドウに表示することもできます。探していたグループ名をハイライトして［選択］をクリックするか、アプリケーションウィンドウでグループ名をダブルクリックしてグループを選択します。

注意：グループの検索機能は、グループメインノードでのみ使用できます。ただし、この機能はその下にあるグループのコンテキストメニューには表示されません。

3.10.7 グループアイコン

u.trust LAN Crypt 管理コンソールでは、インポート元によって OU とグループが異なるアイコンで表示されます。

サーバー アイコンは、OU とグループのインポート元のアイコン

サーバーへのショートカット（コピーして作成したリンク）のアイコン

サーブからインポートされた OU のアイコン

インポートされた OU へのショートカット

サーバーからインポートしたグループのアイコン

インポートしたグループへのショートカット

ユーザーとグループがインポートされたファイルのアイコン

インポートしたファイルへのショートカット

ファイルからインポートしたグループのアイコン

インポートしたグループへのショートカット

手動で追加されたグループ

手動で追加したグループへのショートカット

3.11 セキュリティオフィサーの OU への配属

OU、グループ、ユーザーを u.trust LAN Crypt 管理コンソールにインポートした後、 マスターセキュリティオフィサーは、個々のセキュリティオフィサーを様々な組織単位に割り当てることができます。

その後、セキュリティオフィサーは、与えられた権限を使用して、割り当てられた組織単位を処理することができます。

セキュリティオフィサーが自分の担当する組織ユニットのみを編集できるように、マスターセキュリティオフィサーはこのセキュリティオフィサーから他のノードを隠すことができます。これは、ノードは表示されているが編集できないことを意味します。

セキュリティオフィサーが u.trust LAN Crypt 管理コンソールにログオンすると、自分が担当する組織構造の一部のみが表示されます。

3.11.1 ユーザーの親グループ

u.trust LAN Crypt のユーザーは複数のグループに所属することができます。

- LDAP 経由でユーザーをインポートする場合、親グループはユーザーが所属する OU になります。
- ファイルを通してユーザーをインポートする場合、親グループは、そのユーザーが所属しているグループになります。
- グループプロパティダイアログで新規ユーザーを作成する場合、親グループはグループプロパティダイアログを開いたグループです。

u.trust LAN Crypt 管理コンソールコンソールでは、親グループは 選択されたユーザーと証明書ノード、またはグループのメンバーと証明書ノードの列として表示されます（ユーザー設定タブで設定されている場合、ユーザー設定を参照）。

ユーザーの親グループは、以下の状況で権限の評価に影響します。

- ユーザーのプロパティの表示セキュリティオフィサーは、ユーザーの親グループの権限（読み取りおよび可視）がある場合、ユーザーのプロパティを表示できます。

- ユーザーのプロパティの変更セキュリティオフィサーは、グローバル権限[ユーザーの管理]と、ユーザーの親グループの権限[ユーザーの追加]および[ユーザーの削除]を持っている場合、ユーザーのプロパティを変更できます。

- プロファイルの作成プロファイルの作成: セキュリティオフィサーのグループに対してプロファイルの作成が設定されている場合、セキュリティオフィサーは、グループがグループの親オブジェクトでもあるグループの全メンバーに対して、プロファイルを作成することができます。セキュリティオフィサーは、グループのメンバーであり、別の親グループを持つユーザーのプロファイルを作成することはできません。これには、すべてのメンバーのプロファイルを作成権限が必要です。

- 証明書の割り当て証明書の割り当て: グループに対して証明書の割り当てが設定されている場合、セキュリ ティオフィサーは、グループのすべてのメンバーに証明書を割り当てることができます。セキュリティオフィサーは、グループのメンバーであり、別の親グループを持つユーザーに証明書を割り当てることはできません。これには、[すべてのメンバーに証明書を割り当てる]権限が必要です。

- ユーザーのコピー：ユーザーのコピー: セキュリティオフィサーがグループのプロパティダイアログ（メンバータブに追加ボタンがある）を使用してユーザーをグループに追加する場合、セキュリティオフィサーはユーザーの親グループに対してユーザーのコピー権限を持っている必要があります。

3.11.2 セキュリティオフィサーによるグループの閲覧と編集の許可

1. セキュリティオフィサーが管理でノードを表示できるようにするには、まず、組織構造のベースノードに 表示権を設定する必要があります。

2. これを行うには、構造内のベースノードを選択し、コンテキストメニューのプロパティをクリックして、このノードのプロパティダイアログを開きます。

3. セキュリティタブに切り替え、追加をクリックします。

   ここで、グループの処理に割り当てるセキュリティオフィサーを選択できます。

   注意：複数のセキュリティオフィサーを同じグループに割り当てることができます。

4. 次へをクリックして、このセキュリティオフィサーの権限ダイアログを表示します。ここで、可視権限を選択し、終了をクリックします。この権限はグループ階層を通じて下層に継承されます。つまり、セキュリティオフィサーはすべてのグループを表示できるようになります。

   セキュリティオフィサーがこの設定でデータベースにログオンした場合、管理構造全体を見ることはできますが、編集することはできません。

5. 次のステップでは、セキュリティオフィサーにアクセスする権限がないため、管理コンソールで表示したくないグループを非表示にすることができます。

6. これを行うには、これらのグループを選択し、プロパティダイアログを開き、セキュリティタブを選択します。

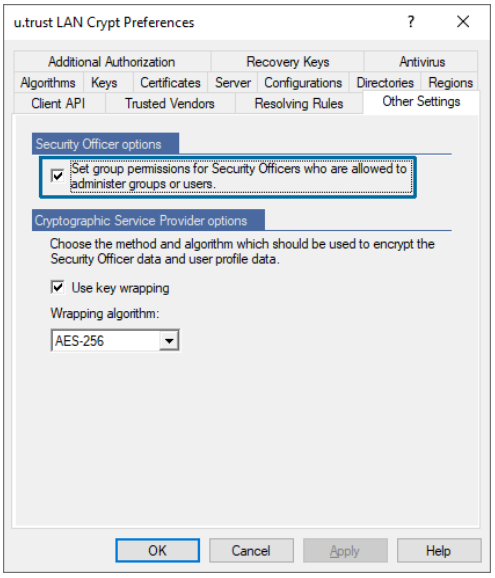
7. ここで、セキュリティオフィサーのために非表示にするグループのために、可視を拒否に設定します。

注意：セキュリティオフィサーが階層的に上位のグループに対する権限を明示的に拒否された場合、この権限を下位のグループに割り当てることはできません。従って、セキュリティオフィサーが問題を起こすことなく下位グループに権限を割り当てることができるように、セキュリティオフィサーには、階層的に上位のグループに対してのみ読み取りおよび表示権限を割り当てることをお勧めします。

注意：u.trust LAN Crypt は、新しく作成されたセキュリティオフィサーのルートグループの可視権限を保持する ACL を自動的に作成するように設定できます。セキュリティオフィサーはグループ管理またはユーザー管理のグローバル権限を持っている必要があります。これにより、セキュリティオフィサーは自分が担当するすべてのグループにアクセス（表示および/または編集）できることが保証されます。

この動作は、中央設定ノードのその他の設定タブで有効にする必要があります。

例（マスターセキュリティオフィサー）



セキュリティオフィサーがこれらの設定をしてログオンすると、このように表示されます。

セキュリティオフィサーが可視権限を持っているグループのみが表示されます。これらのグループが灰色で表示されているのは、まだセキュリティオフィサーにそのグループを処理する権限がないためです。

セキュリティオフィサーに可視権限と読み取り権限の両方が同時に割り当てられている場合、暗号化ルール、グループのメンバーと証明書、およびグループの下にあるグループキーのスナップインも表示されます。セキュリティオフィサーはスナップインの内容を見ることはできますが、変更することはできません。

読み取り権限を使用すると、グループの編集を許可せずに、他のグループに関する情報をセキュリティオフィサーに与えることができます。

注意：セキュリティオフィサーに読み取り権限も付与されている場合、グループを再び隠すには、特に再度読み取り権限を拒否する必要があります。単に可視権限を拒否するだけでは不十分です。

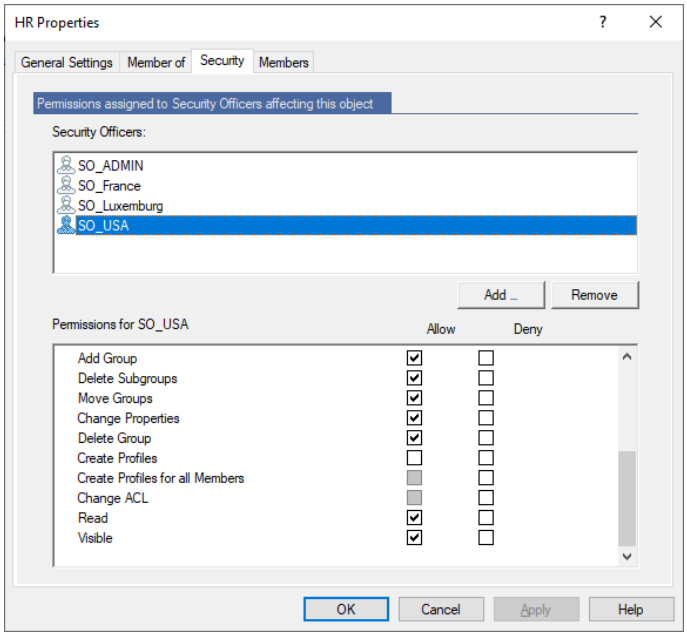
3.11.3 セキュリティオフィサーへのグループ処理権限の付与

セキュリティオフィサーが編集するグループを見ることができるように設定したら、適切なパーミッション を割り当てることができます。

これらのパーミッションは組織階層の下層に継承され、下層にある別の場所で、拒否することができます。

1. セキュリティオフィサーに権限を付与するグループを選択し、プロパティダイアログを開き、セキュリティタブを選択します。

2. セキュリティオフィサー（セキュリティオフィサー）の下には、このグループに割り当てられているすべてのセキュリティオフィサーが表示されます。 セキュリティオフィサーを選択すると、ダイアログの下部に有効な権限が表示されます。



他のグループから継承された権限は灰色のチェックで表示されます。グローバル権限の設定により許可できない権限は、チェックボックスが完全にグレーアウトされます。

注意：グローバル権限設定は、特定のセキュリティオフィサーに割り当てられる権限を定義します。グローバル権限は、セキュリティオフィサーが生成されるときに設定されます。

注意：[許可/拒否]をクリックすると、すべてのアクセス許可が許可または拒否されます。これをもう一度クリックすると、すべてのグローバル権限の選択が解除されます。すべての権限が選択されている場合、必要に応じて後で選択/選択を解除できます。グローバル権限設定では、セキュリティオフィサーに無効な権限を付与できないように定義します。

注意：グループまたはユーザーの管理が許可されているセキュリティオフィサーのグループ権限の設定も参照してください。

以下の権限を割り当てることができます。

アクセス許可	説明
キーの作成	セキュリティオフィサーはグループ内でキーの生成を許可されます。
キーのコピー	セキュリティーオフィサーはキーのコピーを許可されています。
キーの削除	セキュリティオフィサーはキーの削除を許可されています。
ルールの作成	セキュリティオフィサーは、ユーザーの暗号化ルールを生成することができます。
証明書の割り当て	セキュリティオフィサーは、ユーザーに証明書を割り当てることができます。 セキュリティオフィサーには、証明書を割り当てるためのウィザードの実行が許可されます。この権限により、セキュリティオフィサー は、グループが親グループでもあるグループ内のユーザーに証明書を割り当てることができます。
全メンバーに証明書を割り当て	この権限には、証明書を割り当てる権限が設定されている必要があります。すべてのメンバーに証明書を割り当てる]を使用すると、セキュリティオフィサーは、グループ内のすべてのユーザー(グループが親グループであるユーザーと、グループのメンバーで別の親グループを持つユーザー)に証明書を割り当てることができます。 注意：[すべてのメンバーに証明書を割り当て]を[許可]に設定すると、[証明書を割り当てる]権限は自動的に[許可]に設定されます。証明書の割り当て]を[拒否]に設定すると、[すべてのメンバーに証明書を割り当て]権限は自動的に[拒否]に設定されます。

アクセス許可	説明
ユーザーの追加	セキュリティオフィサーは、ユーザーを手動でグループに追加することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。

ユーザーのコピー	セキュリティ責任者は、このグループのユーザーを別のグループに追加する権限を持っています。これは、このグループが親オブジェクトでもあるメンバーに対してのみ許可されます。
ユーザーの削除	セキュリティオフィサーは、グループのメンバーと証明書スナップインを使用してユーザーを削除することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
グループの追加	セキュリティオフィサーは、グループのコンテキストメニューを使用して、新しいグループを追加することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
サブグループの削除	セキュリティオフィサーは、このグループのサブグループを削除することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
グループの移動	セキュリティオフィサーは、管理部で手動で作成したグループを（ドラッグ&ドロップで）移動することができます。インポートしたグループは移動できません。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
プロパティの変更	セキュリティオフィサーはグループのプロパティを変更することができます。
グループの削除	セキュリティオフィサーはグループの削除を許可されています。これは、セキュリティオフィサーが上記のグループのサブグループの削除権限を削除していることを前提としています。 この権限は、グループとユーザーをインポート/同期するための前提条件です。

アクセス許可	説明
プロファイルの作成	セキュリティオフィサーは、プロファイルリゾルバ を実行し、選択したユーザーのポリシーファイルを生成する権限を持っています。プロファイルの作成を使用すると、セキュリティオフィサーは、グループが親グ

	ループでもあるグループ内のユーザーのプロファイルを作成できます。
全メンバーのプロフィールの作成	この権限には、プロファイルを作成権限が設定されている必要があります。全メンバーのプロファイルを作成] を使用すると、セキュリティオフィサーはグループ内の全ユーザーのプロファイルを作成できます：グループが親グループであるユーザー、およびグループのメンバーで別の親グループを持つユーザー。 注意：[すべてのメンバーのプロファイルの作成]を[許可]に設定すると、[プロファイルの作成]権限は自動的に[許可]に設定されます。プロファイルの作成]を [許可しない]に設定すると、[すべてのメンバーのプロファイルを作成]権限は自動的に[許可しない] に設定されます。
ACL の変更	セキュリティオフィサーは、グループ の ACL を変更することができます（別のセキュリティオフィサーを追加するなど）。
読み取り	セキュリティ管理者にはこのグループの読み取り権限があり、スナップインの内容を確認できます。編集権限が付与されている場合は、自動的に 設定されます。
可視	セキュリティオフィサーはグループを見ることができます。ベースノードで設定され、下に継承されます。セキュリティオフィサーが拒否した場合、グループは非表示になります（読み取りも拒否に設定する必要があります）。

3. セキュリティオフィサーに割り当てる権限を選択します。適用をクリックして、設定をデータベースに保存します。

4. このグループに他のセキュリティオフィサーを割り当てている場合は、そのセキュリティオフィサーの権限も設定できます。セキュリティオフィサーに設定された権限を表示するには、セキュリティオフィサーの下にあるセキュリティオフィサーを選択します。

注意：グループのセキュリティオフィサーの権限に対する変更は、該当するセキュリティオフィサーが u.trust LAN Crypt 管理コンソールに再度ログオンした後のみ有効になります。

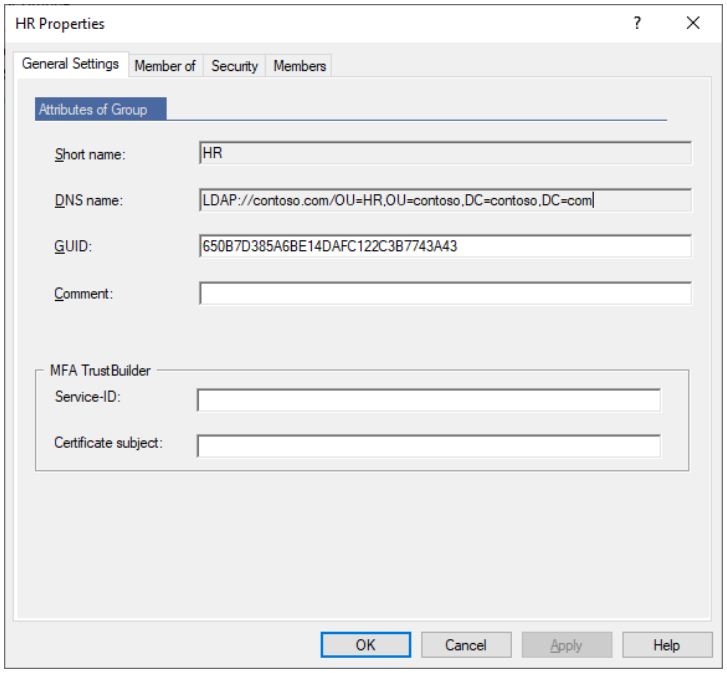
3.12 グループのプロパティ

グループのプロパティダイアログ（<グループ>/コンテキストメニュー/プロパティ）は 4 つのタブで構成されており、グループのプロパティを編集することができます。

3.12.1 プロパティタブ

プロパティタブには、下記があります。

- 略称
- DNS 名
- GUID
- コメント
- サービス ID（MFA TrustBuilder）
- 証明書サブジェクト（MFA TrustBuilder）



TrustBuilder MFA と u.trust LAN Crypt

MFA TrustBuilder セクションでは、TrustBuilder によるユーザーの多要素認証の仕様を定義します。

MFA（多要素認証）のサポートにより、ユーザーは特に安全な方法で u.trust LAN Crypt クライアントにログインできます。ログイン自体は、第 2 のデバイス（ユーザーのスマートフォンやタブレットなど）を使用して実行されます。TrustBuilder の設定は、Windows または TrustBuilder の管理者が行います。u.trust LAN Crypt の MFA TrustBuilder 設定に必要な Service-ID および証明書サブジェクトについては、管理者にお問い合わせください。

対応するフィールドに、Service-ID と証明書のサブジェクト（TrustBuilder サービスの API 証明書である "@cert.trustbuilder"）に必要な番号を入力します。

注意：このグループのユーザーが TrustBuilder MFA を使用できるようにするには、ユーザー用にプロ ファイルを新規に作成する必要があります（暗号化ルールの提供 - ポリシーファイルの生成を参照）。新しいプロファイルをロードすると、ユーザーは MFA を使用して u.trust LAN Crypt Client にログインできます。ユーザーは登録した MFA トークン（スマートフォンなど）で認証プロンプトを受信し、PIN を入力して確認します。

注意：TrustBuilder サービスの API 証明書は、u.trust LAN Crypt クライアントのユーザーの証明書ストアにインストールされている必要があります。

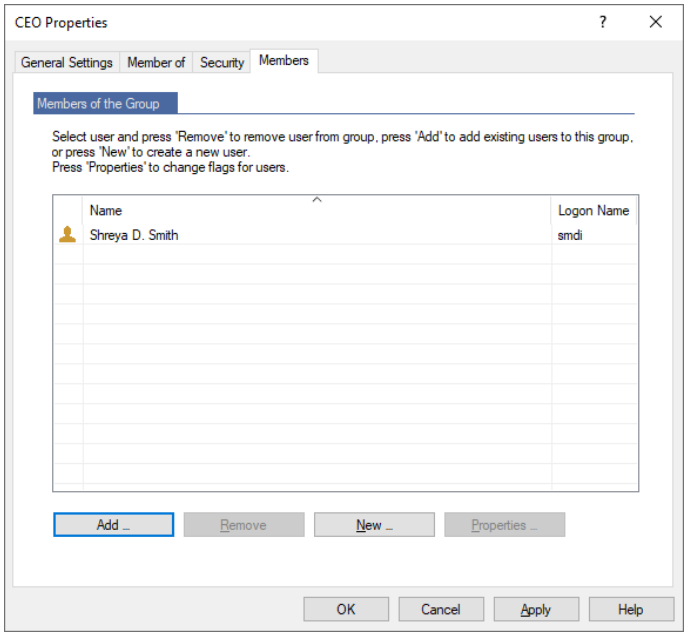
注意：グループに対して多要素認証（MFA）の仕様を定義した場合、その仕様は下位には継承されません。そのため、グループごとに個別に定義する必要があります。

3.12.2 タブのメンバー

メンバータブには、現在のグループをメンバーとして含むグループが表示されます。

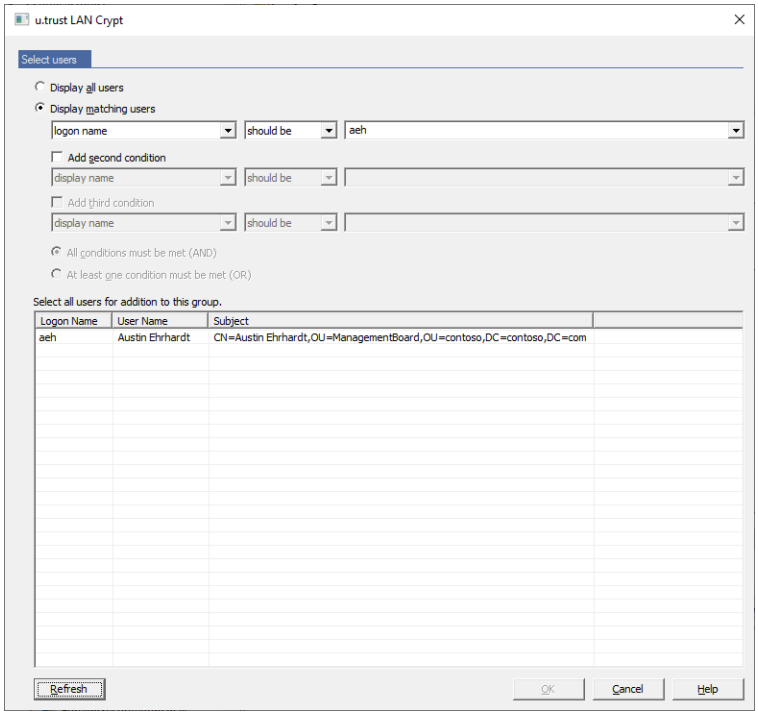
3.12.3 会員の追加／削除

[メンバー]タブでは、現在のグループにメンバーを追加できます。このリストには、このグループのメンバーである既存のユーザーとグループがすべて表示されます。このリストで変更できるのはユーザーだけで、グループは変更できません。



追加

ユーザーを選択してグループに追加するダイアログを開きます。



すべてのユーザーを表示するか、SQL プレースホルダを使用して、特定のユーザーグループまたは個々のユーザーを選択できます。

すべてのユーザーを表示するのは非常に時間がかかるため、u.trust LAN Crypt では、検索条件を定義し、検索プロセスをフィルタリングすることができます。

検索条件を定義する入力フィールドを有効にするには、オプション[一致するユーザーを表示]を選択します。

以下のユーザー情報は、u.trust LAN Crypt データベース から取得されます：

- ログオン名
- ユーザー名
- ユーザーと証明書の間の割り当て
- 証明書の請求者
- 証明書のシリアル番号
- 証明書の有効期限
- 証明書の有効期限
- 親グループ名

u.trust LAN Crypt は、検索されたユーザー属性で定義された文字列を検索します。

最初のドロップダウンリストでは、 検索プロセスを適用する属性を選択できます。

さらに、選択された属性が入力された文字列と一致すべきか、または選択された属性が入力された文字列と一致しないユーザーだけが表示されるかを定義できます。

右側のドロップダウンリストに、u.trust LAN Crypt が検索する文字列を入力します。

文字列の入力には、以下の SQL ワイルドカードを使用できます。

%	任意の文字列
_	一文字 (例: a__は a で始まる 3 文字を含むすべての名前を検索します)
[]	リストから 1 文字 (例: [a-cg]%は、a、b、c、g で始まるすべての名前を検索することを意味します)
[^]	リストに含まれない 1 文字 (例: [^a]% a で始まらない名前をすべて検索)

検索処理の条件は 3 つまで指定できます。

複数の条件を入力する場合、これらの条件をどのように組み合わせるかを定義することができます(AND/OR).

OK をクリックすると、リストで名前が選択されているすべてのユーザーが現在のグループに転送されます。

新規

新規ユーザーを作成するダイアログを開きます。

削除

現在のグループから選択したユーザーのメンバーシップを削除します。

注意： ユーザーが他のグループのメンバーでない場合、u.trust LAN Crypt データベースから削除されます。

ユーザーが複数のグループのメンバーであり、現在のグループがユーザーの親グループである場合、結果のアクションはグループのタイプに依存します。

- グループが組織単位またはルートグループで、ユーザーが別の OU またはルートグループのメンバーである場合、この OU またはルートグループがユーザーの親グループになります。ユーザーが所属する OU またはルートグループが他にない場合、ユーザーは削除されます（ユーザーが所属する OU が削除されるとユーザーが削除される Active Directory と同様）。
- グループが単純なグループ（OU でもルートグループでもない）の場合、ユーザーが所属する他のグループの 1 つが、そのユーザーの親グループになります。

プロパティ

選択したユーザーのプロパティを表示します。

注意：ユーザーは、特定のコンテナ内に一度だけ存在できます。ユーザーが既に存在するコンテナにユーザーを作成/追加しようとすると、それが不可能であることを知らせるメッセージが表示されます。

ただし、同じコンテナ内にいない限り、同じ名前の複数のユーザーをシステム内に存在させることができます。

3.12.4 セキュリティオフィサーの追加

セキュリティタブでは、（マスター）セキュリティオフィサーは、現在のグループにセキュリティオフィサーを追加し、グループに対する権限を割り当てることもできます（3.11.3 章セキュリティオフィサーにグループ処理権限を付与するを参照）。この操作の前提条件は、別のセキュリティオフィサーを追加したいセキュリティオフィサーが ACL の変更権限を持っていることです。

注意：セキュリティオフィサーがセキュリティオフィサーをグループに追加した場合、セキュリティオフィサーはそれらのセキュリティオフィサーに自分の権限（およびその権限のみ）を割り当てることができます。

セキュリティオフィサーは ACL に自分自身を追加したり、ACL 内の権限を編集したりすることはできません。

3.13 ユーザーのプロパティ

ユーザーのプロパティダイアログ （<user>/Context menu/Properties)は 4 つのタブで構成されており、ユーザーのプロパティを編集することができます。

証明書

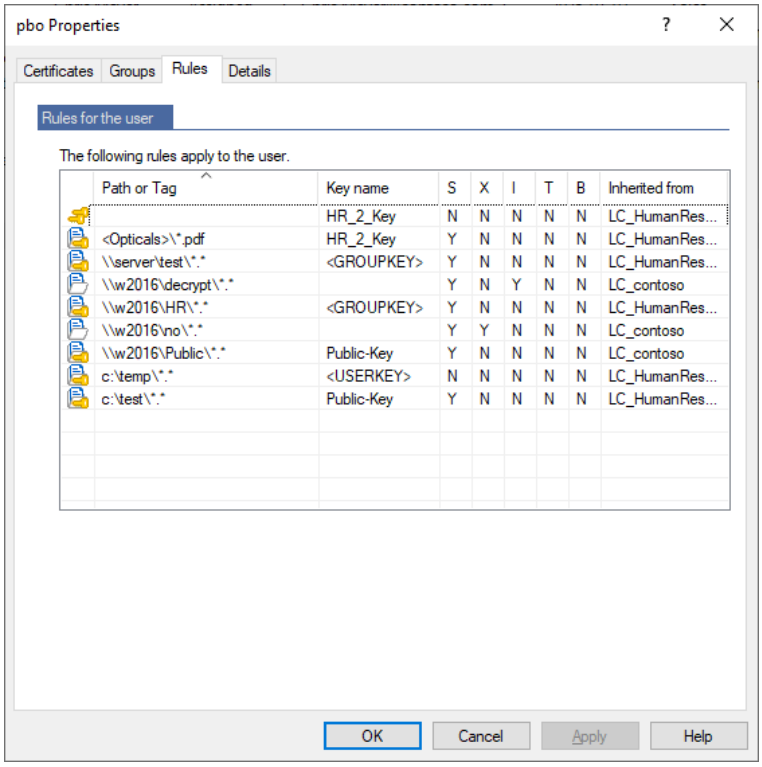
証明書タブには、ユーザーに割り当てられたすべての証明書が表示されます。このタブでは、ユーザー用の新しい u.trust LAN Crypt 証明書を作成したり、証明書ストアから証明書を追加したり、ファイルから証明書をインポートしたりすることもできます（ユーザーへの証明書の割り当てを参照）。

グループ

グループタブには、現在のユーザーがメンバーであるグループが表示されます。さらに、ユーザーのグループメンバーシップを削除したり、新しいグループメンバーシップを追加することもできます。

ルール

ルールタブには、ユーザーのすべての暗号化ルールが表示されます。これは、特定のユーザーに対して現在有効なすべての暗号化ルールの概要 を表示する便利な機能です。

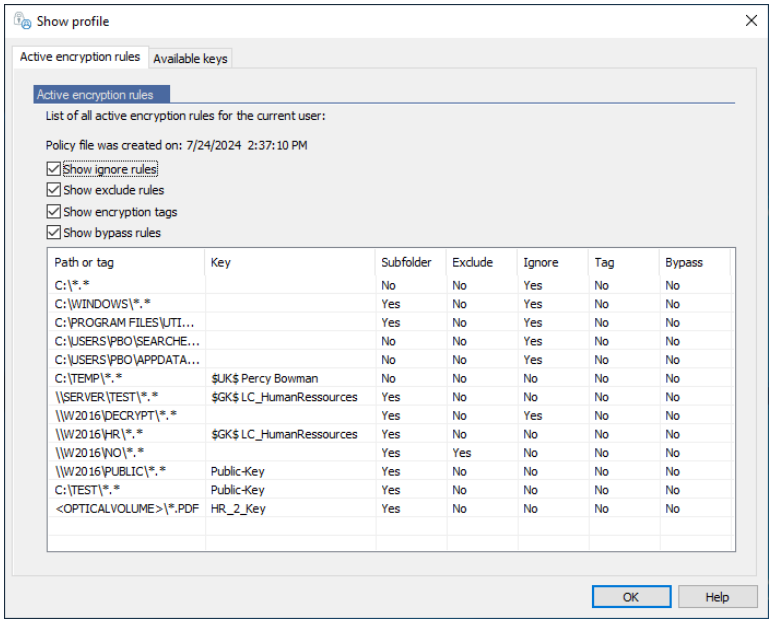


S, X, I, T, B の列は、それがどの種類のルールであるかを示しています。

- S（サブディレクトリ）：サブディレクトリも暗号化に含まれます。
- X（除外パス）：パスを暗号化から除外します。
- I（無視パス）：パスは u.trust LAN Crypt によって無視されます。詳細については、暗号化ルールの生成ページ を参照してください。
- T（タグ）：このパスは u.trust LAN Crypt Client API で定義済みの暗号化タグとして使用されます。
- B（バイパス）：パスはバイパスルールとして定義されます。詳細については、バイパスを参照してください。

[継承元]には、特定のルールの継承元グループが表示されます。

u.trust LAN Crypt クライアントのユーザーのプロファイルビューでも、同じようにこの情報を表示することができます。



詳細

ユーザーデータは 詳細タブに表示され、編集することができます。

メールアドレス入力フィールドにユーザーのメールアドレスを入力できます。このメールアドレスは、u.trust LAN Crypt で生成された証明書のパスワードログファイルに追加されます。例えば、電子メールで PIN を作成する場合などに利用できます。

注意：ユーザーのメールアドレスには、ASCII コード 127 以上の文字を使用してはいけません。文字列の最初と最後にピリオドがあってはなりません。

MFA TrustBuilder セクションでは、TrustBuilder を使用して個々のユーザーの多要素認証の仕様を定義できます。

このためには、TrustBuilder MFA の管理責任者であるシステム管理者に連絡し、必要な 情報を入手してください。サービス ID とユーザー名 ID に必要な番号、および証明書のサブジェクト（TrustBuilder サービスの API 証明書である@cert.trustbuilder）を対応するフィールドに入力します。

この詳細と、グループの全ユーザーにこの設定を定義する方法については、各グループのプロパティタブを参照してください（TrustBuilder MFA と u.trust LAN Crypt）。

注意：ユーザーデータを編集する際はご注意：ください。変更によって望ましくない副作用が発生する可能性があります。たとえば、このタブで[ログオン名]を変更した場合、クライアントはポリシーファイルを検索するために別 （古い）ログオン名を使用するため、ユーザーはポリシーファイルにアクセスできなくなる可能性があります。

3.14 セキュリティ環境の設計

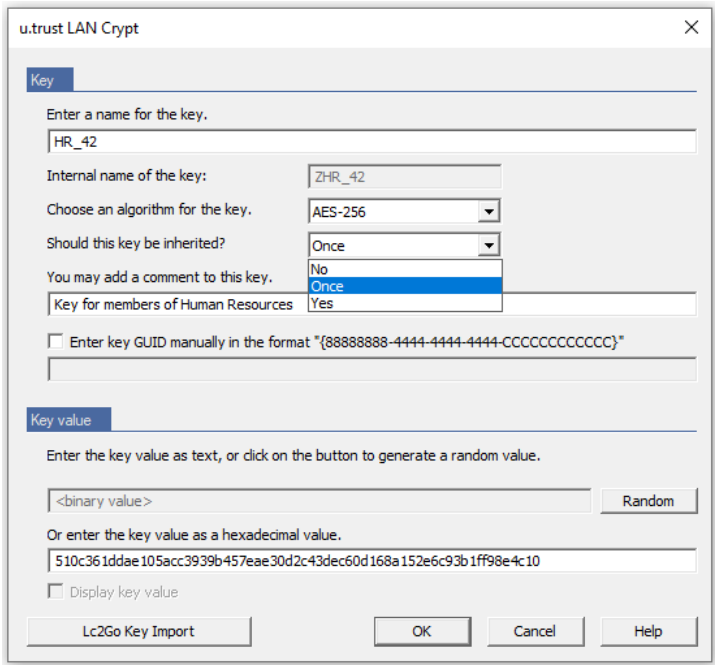
u.trust LAN Crypt の高い柔軟性は、どのような 企業のセキュリティ要件にも容易に対応できることを意味します。

それでも、u.trust LAN Crypt 環境を構築する前に、全社的なセキュリティ戦略が定義されていることが非常に重要です。

u.trust LAN Crypt システムでは通常、最初はかなり制限的なセキュリティポリシーで始めることをお勧めします。なぜなら、後でポリシーを厳しくするよりも、このポリシーを自由化する方が簡単だからです。自由なポリシーをより制限的にすると、解決するのが容易でないセキュリティ問題を引き起こす可能性があります。これを避けるためには、暗号化プロファイルを生成して配布する前に、全社的なセキュリティポリシーが定義されていることが重要です。

3.15 キーの生成

新しいキーは、使用するグループのグループノードの下に生成されます。各キーについて、グループ階層の下方に継承するかどうかを指定できます。



注意：既存のキーはすべて中央設定に表示されます。ただし、この画面では処理できません。このビューは、u.trust LAN Crypt で使用されているキーの概要です。キーは作成されたグループでのみ編集できます。

注意：キーの作成権限のみを持ち、プロファイルの作成権限を持たないセキュリティオフィサーは、キーの生成時に値を追加することはできません。値は、キーがプロファイルに送信されるときに自動的に生成されます。

u.trust LAN Crypt キーは以下のコンポーネントで構成されています。

- 名

  わかりやすくするために、ユーザーグループ名をキー名の一部にすることをお勧めします。

  u.trust LAN Crypt はキーの並べ替えもできるので、定義した名前は特に重要です。

  u.trust LAN Crypt は特定のキー名を使用して、内部で使用する 16 文字のキー名を生成します。このキー名の先頭には、該当するリージョンのプレフィックスを付けます。

- キー値

  キーの長さは、使用するアルゴリズムによって異なります。キーの値は、ANSI 文字で 、または 16 進数表記（許可される数字と文字：0123456789abcdef）で指定できます。その他の関連値は自動的に更新されます。

  キーの値を入力する必要はありません。この場合、ユーザープロファイルで初めてキーが使用されるときに、値がランダムに生成されます。

- 暗号化アルゴリズム

  AES-256、AES-128、3DES、DES、IDEA、XOR

- コメント（任意）

- キーGUID（オプション）

  キーの GUID を手動で入力することで、u.trust LAN Crypt をインストールした 2 台間で暗号化されたファイルを交換することができます。

  このフィールドが空の場合、GUID は自動的に作成されます。

新しいキーを生成するには、以下を行います。

1. キーを生成するグループの下にあるグループキーを選択します。
2. ツールバーの黄色いキーアイコンをクリックするか、右側のコンソールペインで右クリックして、コンテキストメニューを表示し、このメニューで新規キーをクリックします。
3. 上の入力フィールドに新しいキーの名前を入力します。キー名には、バックスラッシュ(¥)、スラッシュ(/)、引用符、&文字は使用できません。u.trust LAN Crypt は、この名前から内部目的で使用される一意の 16 文字のキー名を生成します。また、リージョンプレフィックス（セキュリティオフィサープロパティで指定されている場合）をこの一意の名前の先頭に付けます。内部名は、アルゴリズムを選択するドロップダウンリストの右隣に表示されます。

   キー名は後で変更できますが、そこから生成された内部名は変更できません。
4. ドロップダウンリストから暗号化アルゴリズムを選択します。

   ここでは、中央設定で利用可能にしたアルゴリズムのみを見ることができます。

   注意： XOR、IDEA、DES、3DES などの暗号化アルゴリズムはもはや安全とはみなされないため、データの暗号化には必ず AES-256 または AES-128 などの安全なアルゴリズムを選択してください。
5. グループ内でキーを継承するかどうかを指定します。
   - いいえ

     キーは継承されないため、現在のグループでのみ使用可能です。
   - 一度

     このキーは、現在のグループの次の階層レベルのグループに継承されます。
   - はい

このキーは、現在のグループより下の階層レベルにあるすべてのグループに継承され、暗号化ルールを生成するためにそこで利用できます。

6. 次の入力フィールドに、このキーのコメントを入力します。

7. 必要に応じて、[{888888-4444-4444-...}フォーマットにキーGUID を手動で入力]チェックボックスをクリックし、必要な GUID を入力します（これは、[中央設定]で[セキュリティオフィサーは新規キーの GUID を定義できる]オプションが有効になっている場合にのみ可能です）。定義済みGUID{888888-4444-4444-CCCCCCCCCC}は、ここで使用することはできません。必ず変更してください。

8. キー値の ANSI 入力フィールドに、16 進値（アルファベット A ～ F、数字 0 ～ 9）または文字列を入力します。他の関連値は自動的に更新されます。または、ランダム（推奨）をクリックすると、u.trust LAN Crypt が値を計算します。

9. OK をクリックします。

新しいキーは管理コンソールに表示されます。

3.15.1 Lc2Go キーインポート

Lc2Go で暗号化されたファイルからキーをインポートすることができます。Lc2Go キーのインポートボタンをクリックします。次に、u.trust LAN Crypt にインポートしたい Lc2Go で暗号化されたファイルを選択します。必要に応じて、ファイルエクスプローラを使用して特定のパスから Lc2Go で暗号化されたファイルを選択してインポートする場合は、参照(″...″)をクリックします。

パスフレーズ入力フィールドに、そのファイルに関連付けられたパスフレーズ（セキュアパスワード）を入力します。

インポートされた Lc2Go キーは管理コンソールに表示され、暗号化ルールに使用できます。

3.15.2 特定のキー

手動でキーを生成するだけでなく、u.trust LAN Crypt でユーザーおよびグループ固有のキーを使用することもできます。

ユーザーキー

暗号化パスにキーが割り当てられると、キーのリストには常に 1 つの<USERKEY>キーも表示されます。これは、システムが暗号化規則を解決するときに、個々のユーザーに対して自動的に生成するユーザー固有のキーのプレースホルダです。

グループキー

<USERKEY>と同様に<GROUPKEY>を使用すると、グループの全メンバーに共通のキーを生成することができます。システムは暗号化規則を解決する際にグループキーを自動的に生成します。

<USERKEY>がどのように使われるかの例としては、すべてのユーザーが U:という一つのネットワークドライブを使い、そのドライブにはユーザーごとに一つのディレクトリがあり、適切なユーザーだけがそのディレクトリにアクセスできる場合です。

u:¥*.*<ユーザーキー>

他の例としては、ローカルの一時ディレクトリを暗号化するのに<USERKEY>を使うことができます。

ユーザーおよびグループ固有のキーは、通常は必要ないため、[中央設定 、[すべての u.trust LAN Crypt キー]ノード下のデフォルトビューには表示されません。ただし、必要に応じて、マスターセキュリティオフィサーまたはグローバル権限特定のキーの使用を持つセキュリティオフィサーは、これらのキーを表示することができます。

必要に応じて、これらの特定のキーの値は、それぞれのキーのプロパティダイアログ（コンテキストメニュー/プロパティ）で表示することもできます。

特定のキーを表示するには、キーリストのコンテキストメニューから、特定キーの表示をクリックします。これで、特定のキーのみが表示されます。デフォルトの表示に戻るには、もう一度特定キーの表示をクリックします。

注意：特定のキーは、所属するユーザー/グループが削除されてもデータベースから削除されません。このキーはデータベースに残り、コンテキストメニューの特定のキーを表示をクリックすることで、中央設定のすべての u.trust LAN Crypt キーノードに表示することができます。

特定のキーの再割り当て

状況によっては、ユーザーまたはグループ固有のキーをユーザーまたはグループに再割り当てする必要があります。

例ユーザーが Active Directory から u.trust LAN Crypt 管理コンソールコンソールにインポートされます。このユーザーにはユーザー固有のキーが生成されます。u.trustLAN Crypt 管理コンソールコンソールでユーザーが所属するグループを削除し、再度インポートすると、u.trustLAN Crypt はユーザーのポリシーファイルを生成する際に自動的に新しいユーザー固有キーを生成します。

すると、ユーザーは古いユーザー固有キーで暗号化されたデータにアクセスできなくなります。

このような状況を克服するために、u.trust LAN Crypt を設定して、削除されたユーザー/グループから特定のキー を再割り当てできるようにすることができます。

これを行うには、DWORD-ValueShowUserKeyPage を Windows レジストリに追加し、キーの下にデータ値 1 を追加します。

hkey_local_machine

SOFTWARE¥

Policies¥

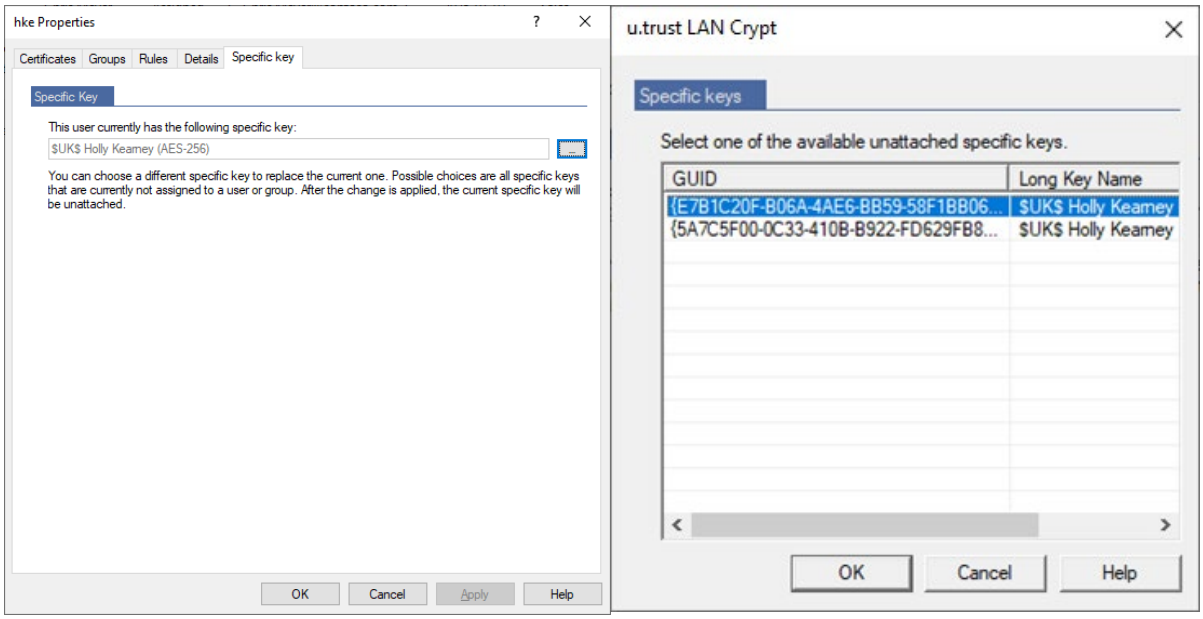
Utimaco¥

SGLANCrypt

このエントリーは、Windows レジストリの下記で作成できます。

hkey_current_user....

この値が Windows レジストリで見つかった場合、タブ固有のキーがユーザーとグループのプロパティダイアログ（<ユーザー/グループ>/コンテキストメニュー/プロパティ）に追加されます。



特定のキーがユーザーまたはグループに割り当てられている場合、そのキーは[特定のキー]タブに表示されます。特定のキーが表示されていない場合は、現在のキーを別の特定のキーに置き換えるか、新しいキーを割り当てることができます。データベースに存在し、まだユーザーまたはグループに割り当てられていないキーを使用できます。

注意：変更を行うには、セキュリティオフィサーに特定のキーを使用するパーミッションが必要です。そうでない場合は、読み取り権限しかありません。

参照...ボタンをクリックすると、使用可能なすべてのキーのリストが表示されます。キーを選択し、OK をクリックします。

特定のキータブで、OK をクリックします。

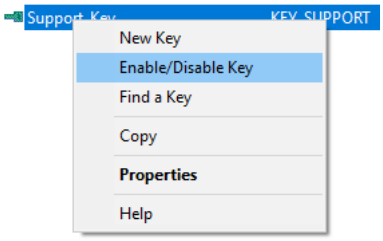
現在の特定のキーが別のキーに置き換えられた場合、そのキーは非割り当てキーとしてデータベースに残ります。

3.15.3 キーのアクティブ化／非アクティブ化

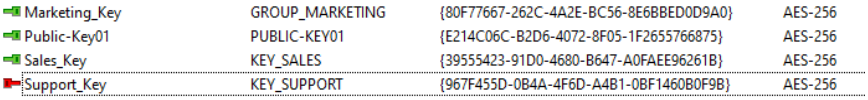
u.trust LAN Crypt では、既存のキーを非アクティブに切り替えることができます。これを行うと、暗号化ルールを定義する際にこのキーは利用できなくなります。

ただし、すでに使用中の暗号化ルールでこのキーを使用することはできます。このキーは管理データベースに保存されたままであり、必要に応じて再度アクティブ化することもできます。

キーを非アクティブからアクティブ（またはその逆）に切り替えるには、そのキーを選択し、コンテキストメニューのキーの有効化/無効化をクリックします。



パッシブキーは、行頭に赤いキーのアイコンが付いているので分かります。



3.15.4 キー間のリレーションシップ

キーを使用するグループ用にキーを生成するだけでなく、別のグループのキーとのリレーションシップ（ショートカット）を作成することで、グループ内のユーザーが 。

例あるチームのメンバーに、限られた期間だけ別のチームのメンバーと同じ権限を与えたい場合、一方のグループのキーへのショートカットをもう一方のグループに追加します。このキーへのショートカットを使用して、暗号化ルールを作成できます。

もしキーへのショートカットが使えなければ、この単純なデータ交換を可能にするために、新しいグループを作成し、両方のグループのユーザーを新しいグループに追加し、新しいキーと暗号化ルールを作成しなければなりません。キーへのショートカットは、迅速で簡単なデータ交換の方法を提供します。

ショートカットを使って別のグループにキーを追加するには、あるグループの、グループのキーノードから、関連するグループのノードにキーをドラッグします。また、コピー元のグループのキーをコピーして、コピー先のグループにペーストすることもできます。

この方法でインポートされたキーは、ショートカットとして表示されます。



セキュリティオフィサーは、キーにショートカットを挿入する前に、これらのグローバル権限を持っている必要があります。

- キーの作成
- キーのコピー

送信元グループでは、グループ固有の権限も必要です。

- キーの作成
- キーのコピー

ショートカットを削除するには、セキュリティオフィサー がグローバルおよびグループ固有のキーの削除権限を持っている必要があります。

ショートカットとして挿入されたキーには、以下のプロパティがあります。

- これらは継承されませんので、作成されたグループ内でのみ利用可能です。サブグループでは使用できません。
- オリジナルキーが削除されると、すべてのショートカットも削除されます。

注意：通常のグループキーの場合と同様に、参照を削除しても、そのキーが使用されていたルールが無効になるわけではありません。データへのアクセスを削除するには、対応する暗号化ルールを削除し、新しいポリシーファイルを生成する必要があります。ユーザーがこのデータにアクセスできないようにするには、クライアントが新しいポリシーファイルを初めて読み込む必要があります。

3.15.5 グループからのキーの削除

キーを削除できるのは、キーが生成されたグループからのみです。キーを削除する前に非アクティブにする必要があります。

使用中のキーを削除すると、グループから削除されますが、未割り当てのキーとしてデータベースに残り、[中央設定]/[すべての u.trust LAN Crypt キー]に表示されます。

再びキーを追加

このキーが後で必要になった場合（例えば、古いデータの暗号化されたバックアップにアクセスする場合など）、すべての u.trust LAN Crypt キーのリストから該当するグループにドラッグするだけで、再び使用することができます。セキュリティオフィサーは、キーの作成権限を持っているグループにキーを追加することができます。ショートカットではありません。

注意：暗号化ルールで一度も使用されたことのないキーを削除すると、実際にデータベースから削除されます。このキーは、[すべての u.trust LAN Crypt キー]の下に表示されなくなります。

3.15.6 データベースからのキーの削除

以下の条件下では、データベースからキーを実際に削除することができます（すべての u.trust LAN Crypt キーノードの下）。

- マスターセキュリティオフィサーとしてログオンしている必要があります。
- キーは暗号化ルールで使用してはいけません。
- キーはどのグループにも存在してはいけません。
- このキーは、ユーザーやグループに割り当てられた特定のキーであってはなりません。
- キーを解除する必要があります。

3.15.7 キーの編集

キーを生成した後、その名前、そのキーに指定された継承のタイプ、コメントを変更することができます。

キーが既に使用されているかどうかは、コンソールの使用済み列で確認できます。

キーを変更するには、キーが生成されたグループに移動し、該当するキー名をダブルクリックします。キーを変更できるダイアログが表示されます。

注意：すべての u.trust LAN Crypt キーノードでキーの継承設定を変更することはできません。

プロパティダイアログ

プロパティダイアログには、選択したキーに関する情報が表示されます。このダイアログでは、ロングキー名と、キーを継承するかどうかを定義する設定を変更できます。u.trust LAN Crypt で生成された内部用の 16 文字の一意のキー名は変更できません。

注意： キーを編集するには、セキュリティオフィサーは、キーが生成されたグループに対して、グループ固有のキーを作成権限を持っている必要があります。特定のグループに属さないキーは変更できません。

キーをダブルクリックすると、プロパティが表示されます。

プロパティダイアログは 3 つのタブで構成されています。

- キータブには、キーのデータが表示されます。このタブでは、ロングキー名と、そのキーを継承できるかどうかを定義する設定を変更できます。キーの値を表示するには、キー値の表示をクリックします。
- グループタブには、キーが利用可能なすべてのグループが表示され、暗号化ルールの作成に使用できます。
- ルールタブには、キーが使用されるすべての暗号化ルールが表示されます。

注意：グループとルールタブは情報のみです。ここでは変更はできません。

3.16 暗号化ルール

u.trust LAN Crypt ルールは、各キーで暗号化できるデータを正確に定義します。暗号化ルールは暗号化パスとキーで構成されます。

注意：暗号化ルールのパス指定に加えて、ファイルパターンも下のフィールドに指定する必要があることに注意してください。ここではワイルドカード（*.*など）を使用することもできます。

グループに定義された暗号化ルールは、1 つの u.trust LAN Crypt 暗号化プロファイルを構成します。

グループの暗号化プロファイルには、それぞれ異なる暗号化ルールを含めることができ、 、特定のタイプのデータを暗号化するために使用されます。

ドライブ全体、リムーバブルメディア（USB フラッシュドライブなど）、光学ドライブ、ネットワーク共有、フォルダ（サブフォルダを含む）、特定のファイルタイプ（ファイル拡張子で識別）、および個々のファイル（ファイル名またはファイル名の一部で識別）を暗号化できます。

個々の暗号化ルールを生成すると、グループ内に存在するすべてのキーが表示されます。u.trust LAN Crypt セキュリティオフィサーは、ユーザーがアクセスできるデータを定義するために適切なキーを割り当てることができます。

暗号化ルールは常にグループごとに生成されます。暗号化ルールはパスとキーで構成され、暗号化ルールとタグノードで作成されます。同じダイアログでパスの詳細を入力し、キーを選択し、異なるオプションを選択するため、暗号化ルールを生成するのは簡単です。

パス、キーの選択、さまざまなオプションがダイアログにまとめられているため、暗号化ルールを簡単に作成できます。暗号化ルールは必要に応じて後で変更することができます。たとえば、以前に選択したキーのアルゴリズムが必要なセキュリティ要件を満たさなくなった場合などです。この場合、以前に使用したキー（たとえば IDEA アルゴリズム）を、より高いセキュリティアルゴリズム（たとえば AES-XTS 256 ビット）を使用した新しいキーに置き換えることができます。最初の暗号化を実行した後、すべての既存ファイルを新しいキーと高いセキュリティアルゴリズムで暗号化します。

注意： 既存の暗号化ルールのために、以前に使用したキーを別のキーに置き換える場合、古いキーはユーザーが所有したままでなければなりません。古いキーは、このキーで暗号化された既存の暗号化データの再暗号化に必要です。そのためには、古いキーをパスなしキーとして各ユーザーに割り当てます。

注意： Utimaco では一般的に、すべてのデータをキー長 256 ビットの AES で暗号化することを推奨しています。古いアルゴリズム（DES、3DES、IDEA、XOR など）で暗号化されたままのデータは、セキュリティ上の理由から、できるだけ早く AES 256 ビットに再暗号化する必要があります。

暗号化ルールは常に下位グループに継承されます。

注意：インターネット一時ファイルフォルダには暗号化ルールを定義しないでください。

3.16.1 暗号化パス

暗号化パスは、どのデータを暗号化するかを定義します。暗号化パスは、関連するグループノードの下にある EnCryption Rules and Tags ノードで定義します。そして、そのグループに存在するすべてのユーザーに適用されます。

注意：*.zip ファイルや圧縮フォルダへのパスは暗号化パスとして使用できません。

注意：暗号化パスは 259 文字以下でなければなりません。

相対パス

u.trust LAN Crypt は相対パス定義に対応しています。相対パス定義は、関係するディスクドライブを特定しないディレクトリまたはファイル、または階層内の次の最上位ディレクトリへのパス を指定します。相対パス定義を選択すると、システムはそのパス定義に一致する各ディレクトリを暗号化します。

相対パスは 2 つの方法で使用できます。

- エントリー¥my_data*.*

  ROOT ディレクトリ内のすべての ″my_data ″フォルダを暗号化します。

  例えば、以下のようなフォルダです：

  C:„*.*.
  D:¥my_data*.*

F:¥my_data*.*
Z:¥my_data*.*.

- エントリー： my_data*.*

  my_data ″フォルダを暗号化します。

  例

  C:¥company¥my_data¥*.*.

  Z:¥Department¥Development¥Team¥*.*.

どちらの場合も、″my_data ″フォルダ内のファイルはすべて暗号化されます。

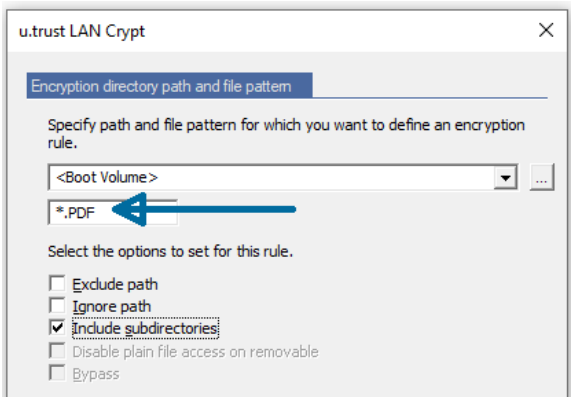
ディレクトリパスがバックスラッシュで始まる場合、相対パスの定義はルートディレクトリにのみ適用されます。

ブートボリューム

<Boot Volume>オプションを選択すると、システムドライブ（Windows もインストールされている）にあるファイルを暗号化できます。このオプションを選択すると、入力フィールドに定義済みのエントリー ″*.*″（これはすべてのファイルに適用されます）をカスタマイズすることもできます。（これはすべてのファイルに適用されます）を入力フィールドでカスタマイズすることもできます。

例

例えば、ブートボリューム上で PDF ファイルのみを暗号化する場合は、入力フィールドの項目を以下のように変更してください。



また、ブートボリューム上の他のファイルタイプや特定のファイル（confidential.txt など）だけを暗号化することもできます。これを行うには、別の新しいルールを作成し、入力フィールドのエントリーを上記と同じ方法で変更します。

ローカルボリューム

<Local Volumes>オプションを使用すると、すべてのローカルドライブにのみ適用されるルールを作成できます。例えば、（複数の）内蔵ハードディスク、リムーバブルメディア、あるいは光学ドライブなどです。

光学機器

<Opticals>オプションを使用すると、光学メディアのみに適用されるルールを作成できます。例えば、CD、DVD、Bluray に書き込まれたデータは常に u.trust LAN Crypt によって自動的に暗号化されます。対応するキーを所有するユーザーだけが、このデータを後で読んだり、お互いに共有したりすることができます。

ネットワーク共有

<Network Shares>オプションを選択すると、ユーザーがアクセスできるすべてのネットワーク共有に適用するルールを作成できます。ネットワーク共有がドライブ文字か UNC パスかは関係ありません。

リムーバブル

<Removables>オプションを選択すると、すべてのリムーバブルデバイスに適用するルールを作成できます。

注意：<Removables>は、外部に接続されたすべてのストレージメディア（USB スティック、外付けハードディスクなど）を指すことに注意してください。これは、外部に接続された光学ドライブにも当てはまります。さらに、リムーバブルデバイスもローカルボリュームに属します。

デフォルトフォルダ

ユーザー固有のフォルダの暗号化を容易にするため、u.trust LAN Crypt は Windows によって事前に定義されたデフォルトディレクトリをサポートしています（例：マイドキュメント、共通ドキュメントなど）。u.trust LAN Crypt は、該当するデフォルトディレクトリから正しい言語の正しいユーザー固有のパスを決定し、そのディレクトリに保存されているファイルを暗号化します。

注意： Windows 10 のバージョン 1709 では、インターネットクッキーを Windows のインターネットクッキー用の事前定義ディレクトリのファイルに保存しなくなったことに注意：してください。そのため、バージョン 1709 以降の Windows では、インターネットクッキーの暗号化はサポートされなくなりました。

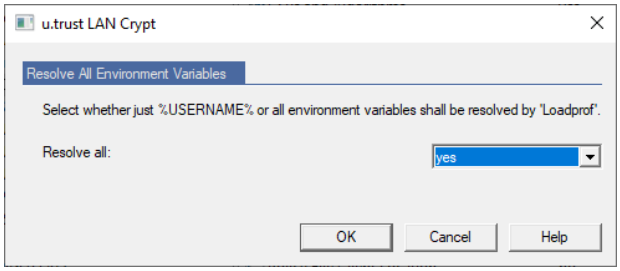
環境変数

u.trust LAN Crypt はパス定義でローカル環境変数 %USERNAME%の使用をサポートしています。パス定義のローカル環境変数%USERNAME%は、u.trust LAN Crypt によって自動的に解決されます。

u.trust LAN Crypt では、環境変数を入力することで追加のフォルダを指定することができます：

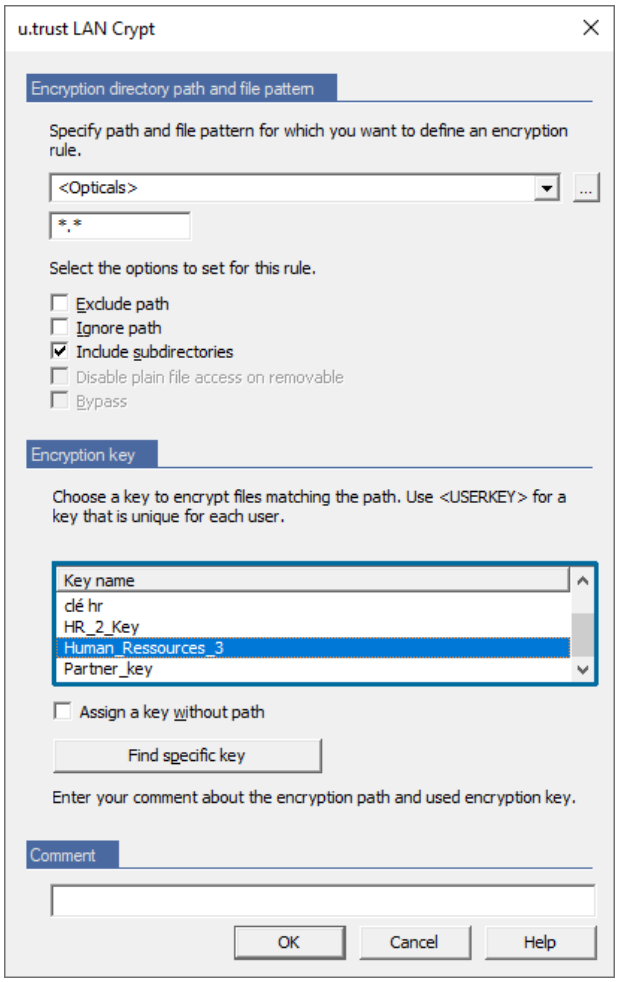
環境変数：	例
すべてのユーザープロファイル	C:¥ProgramData
%APPDATA	C:¥Usersers¥Username¥AppData¥Roaming
ローカル APPDATA	C:¥Users¥Username¥AppData¥Local
パブリック	C:¥Users¥Public
ユーザープロファイル	C:username

u.trust LAN Crypt クライアントでこれらの環境変数を解決するには、u.trust LAN 暗号化設定で設定する必要があります。



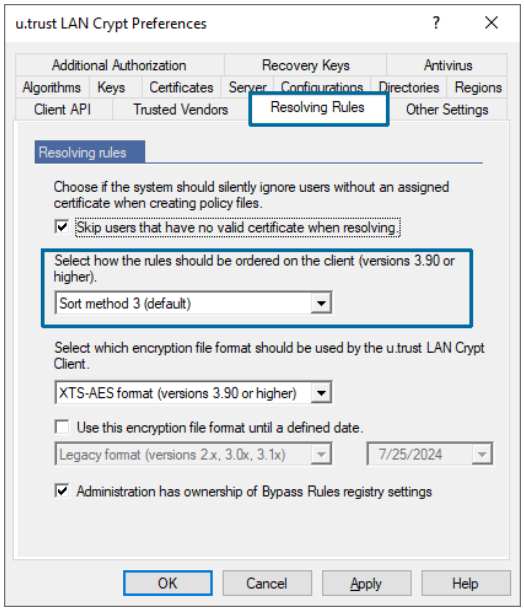
3.16.2 キー

暗号化ルールを作成する前に、データの暗号化に使用するキーを作成します。暗号化ルールを作成するダイアログには、関連するグループで使用可能なすべてのキーが表示されます。



3.16.3 一連の暗号化規則

ポリシーファイルをクライアントに読み込むと、u.trust LAN Crypt はルールの解決タブで選択した方法に従って暗号化ルール をソートします（ソートの方法参照）。

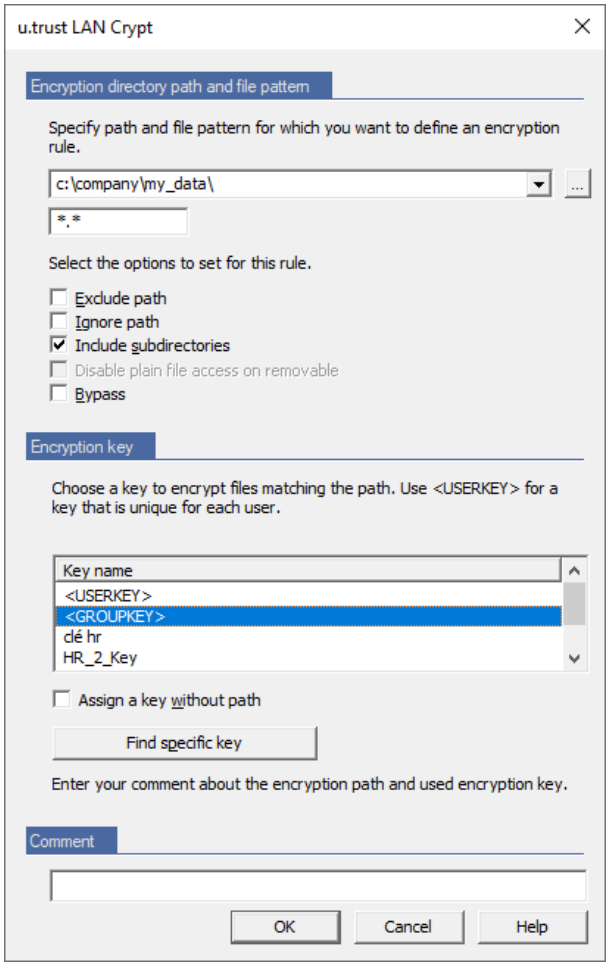


3.16.4 暗号化ルールの生成

暗号化ルールは常にグループごとに生成されます。パスとキーで構成され、暗号化ルールとタグノードで作成されます。特定のグループを探している場合は、グループ検索機能を使用することもできます。

1. 該当するグループノードの下にある暗号化ルールとタグを右クリックし、コンテキストメニューの［新規暗号化ルール］をクリックします。

   また、右側のコンソールペインで右クリックして表示されるコンテキストメニューから、新しい暗号化ルールコマンドにアクセスすることもできます。右側のコンソールペインでは、生成されたすべての暗号化ルールを見ることができます。



2. 暗号化パスの入力フィールドに相対パスまたは絶対パスを入力するか、定義済みのテンプレートから 1 つを選択します。

3. 選択したパス内のすべてのファイルに新しい暗号化ルールを適用したい場合は、下の入力フィールドにファイルパターンとして*.*を入力します。一方、新しい暗号化ルールを特定のファイルタイプにのみ適用する場合は、ファイルパターンとして *.docx（Word ファイルのみ）または*.txt（テキストファイルのみ）などを入力します。ファイル名にジョーカー（*）とワイルドカード（？）を使用できます（パスの残りの部分には使用できません）（例：″*.d?″または ″*.d*″）。必要に応じて、参照ボタン（″...″）をクリックしてパスを選択します。

   または、リストボックスに含まれる Windows デフォル フォルダ（マイ キュメントなど）、ローカルドライブ、ネットワーク共有、またはドライブの種類（リムーバブル、光学式など）の定義済みパスのいずれかを選択することもできます。選択された定義済みパスは、入力フィールドに表示されます。

相対パスと、8.3 記法のみによるファイルまたはパス指定をサポートするプログラム

8.3 記法でしかファイルやパスを指定できないプログラムを使用していて、8 文字以上のファイル名の暗号化ファイルや 8 文字以上のフォルダ名の暗号化ファイルにアクセスしたい場合は、8.3 記法で暗号化パスを指定する必要があります。

これらの暗号化ルールを追加で定義する必要があります。そうしないと、32 ビットプログラムは動作しなくなります。

長いファイル名の正しい 8.3 名を表示するには、dir /x コマンドを使用します。

4. 暗号化ディレクトリパスとファイルパターンの下に 5 つのオプションが表示されます：
   - 除外パス
   - 無視パス
   - サブディレクトリを含む
   - リムーバブルファイルの平文アクセスを無効にします。
   - バイパス

サブディレクトリを含む

サブディレクトリまたはサブフォルダは、指定しない限り暗号化に含まれません。すべてのサブディレクトリまたはサブフォルダを暗号化に含めるには、［サブディレクトリを含める］オプションを選択します。

例

Entry: c:¥companymy_data¥*.* Include subdirectories

この暗号化ルールは、すべてのファイルを暗号化します。

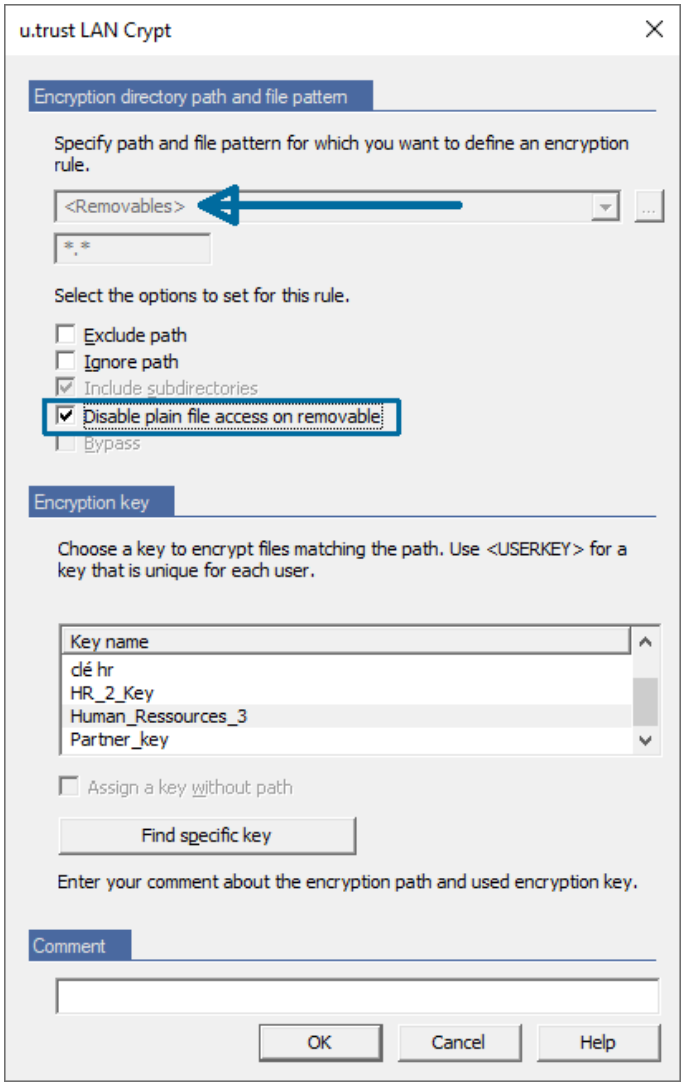
C:¥company ¥my_data

C:¥company ¥my_data ¥project X

C:¥company ¥my_data ¥project Xdemo

リムーバブルファイルの平文アクセスを無効にします。

このオプションは、事前定義パスに<Removables>が設定されている暗号化ルールでのみ使用できます。リムーバブルに平文ファイルアクセスを無効化オプションを設定すると、暗号化ルールが存在するリムーバブルメディア(外付けハードディスク、USB メモリなど)に保存された暗号化されていないファイル(平文ファイル)へのアクセスが拒否されます。暗号化ルールが存在するリムーバブルメディア (外付けハードディスクや USB メモリなど)に保存された暗号化されていないファイル(平文ファイル)へのアクセスが拒否されます。



リムーバブルの平文ファイルアクセスを無効にする）オプションを設定すると、USB メモリなどのリムーバブルメディアから不正なソフトウェアがインストールされるのを防ぐことができます。

注意：このオプションを有効にすると、暗号化ルールの［サブディレクトリを含める］オプションも自動的に設定されます。

注意：この暗号化ルールにはキーを割り当てる必要があります。

除外パス

ここで、このデータを暗号化から除外する暗号化ルールを定義する必要があります。これを行うには、[暗号化ルール］ ダイアログで[除外パス]オプションを選択します。その結果、暗号化ルールで指定されたファイルは暗号化されません。デフォルトでは、このオプションは選択されていません。

このオプションを暗号化ルールで使用すると、すでに暗号化ルールが存在するパスの個々のファイル、ファイルタイプ、またはサブフォルダを暗号化から除外できます。これは、新しい暗号化ルールダイアログで ［除外パス]オプションを有効にすることで実現できます。つまり、暗号化ルールで指定されたファイルは暗号化されません。既存の暗号化ルールをダブルクリックで選択するか、[プロパティ]コンテキストメニューを使用して、既存の暗号化ルールに対してこのオプションを変更することもできます。

例

ファイル拡張子が*.TXT のファイルはすべて暗号化から除外されます。

1 行目：

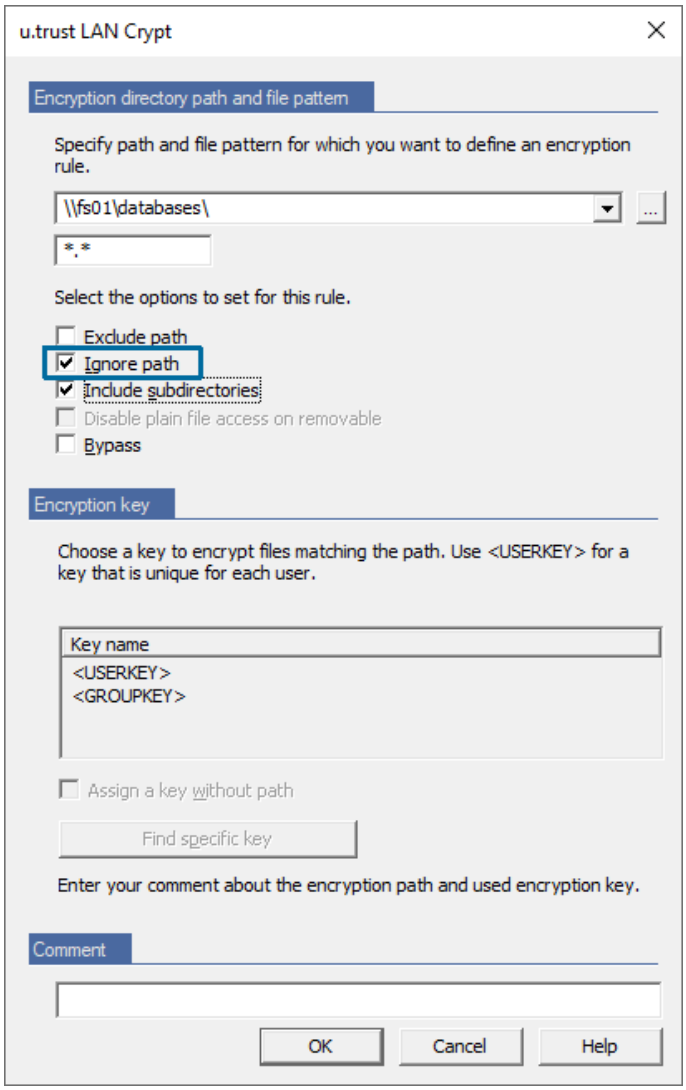
エントリー　C:¥MYDIR*.TXT，除外パス，キーなし，MYDIR フォルダ内の拡張子.TXT を持つすべてのファイルを暗号化から除外します。

2 行目：

エントリー　C:¥MYDIR*.*，除外パス，選択なし，指定されたキーで MYDIR フォルダ内のすべてのファイル（*.TXT ファイルを除く）を暗号化します。

無視パス

u.trust LAN Crypt には無視パスオプションがあります。u.trust LAN Crypt はこのタイプの暗号化ルールの影響を受けるファイルを単に無視します。



パスの除外オプションとは対照的に、これはこれらのファイルに対するアクセス制御がないことも意味します。ファイルを開いたり（暗号化された内容が表示されます）、移動したり、削除したりすることができます。にもかかわらず、システムは暗号化から除外されたフォルダ内のファイルをチェックし、実際に暗号化されているかどうかを確認します。このようにして、u.trust LAN Crypt はこの種のフォルダ内のファイルが暗号化されているかどうかを検出することができます。暗号化されたデータにアクセスすることはできません。u.trust LAN Crypt は、パスを無視するオプションが選択されたフォルダ内のファイルを単に無視します。u.trust LAN Crypt はそれらをチェックしないので、ユーザーは暗号化されたファイルにアクセスすることができます。

注意：u.trust LAN Crypt Client では、レガシーフィルタドライバーとミニフィルタドライバーの動作が異なることがあります。フォルダの無視パスルールは、ミニフィルタ暗号化ドライバーが有効な場合、ファイルのアクセス保護も解除されることを意味しますが、レガシーフィルタ暗号化ドライバーが有効な場合（古い LAN Crypt クライアントのみ）、ファイルのアクセス保護はそのようなフォルダにも存在します。

このオプションは主に、アクセス頻度が非常に高く、特に暗号化する理由がないファイルに使用します。これにより、システムのパフォーマンスが向上します。u.trust LAN Crypt のインストール先や Windows 自体のインストール先も暗号化によって無視されます。原則として、パスを無視するオプションが選択された場所にあるファイルは暗号化も復号化もできません。これらのファイルは u.trust LAN Crypt によって完全に無視されます。

バイパス

このオプションを使用すると、u.trust LAN Crypt にバイパスルールを作成できます。このようなルールが存在するすべてのパスは、u.trust LAN Crypt ミニフィルタドライバーによって完全に無視されます。このようなパスにあるファイルは暗号化も復号化もできません。パス無視オプションと比較すると、バイパスルールが適用されるパスでのファイルアクセスはミニフィルタドライバーによって全く監視されません。

注意：この機能は、[中央設定]ノードの[ルールの解決]タブで[管理部門にバイパスルールのレジストリ設定の所有権がある]オプションを有効にしている場合にのみ、この時点で使用できます（管理部門にバイパスルールのレジストリ設定の所有権があるを参照）。

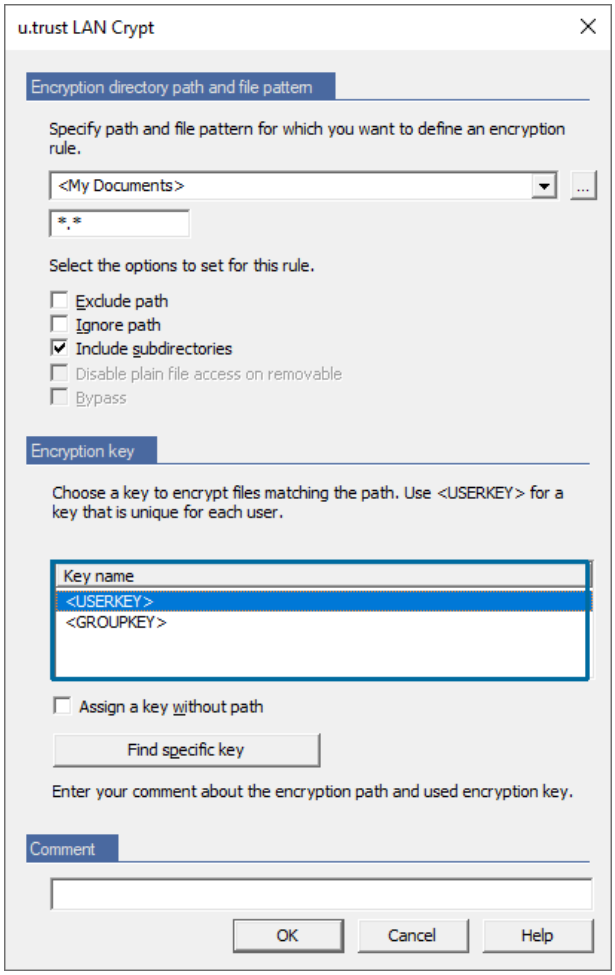
注意：このオプションを有効にすると、暗号化ルールの［サブディレクトリを含める］オプションも自動的に設定されます。

警告: このオプションは、Utimaco のサポートスタッフから依頼された場合のみ有効にしてください。

注意：バイパスルールを設定または削除した後は、クライアントコンピュータを再起動する必要があります。

キー付きの暗号化ルールを作成する場合は、以下の追加手順を実行します。

リストからキーの選択します。



注意：デフォルトのビューでは、<USERKEY>と<GROUPKEY>のプレースホルダとセキュリティオフィサーが作成したキーだけが表示されます。特定のキーの検索ボタンを使用すると、特定のキーを検索して表示することができます。

暗号化パスとキーは、u.trust LAN Crypt 暗号化ルールを形成します。ユーザー/グループに対して定義した暗号化ルールは、合計でユーザー/グループの暗号化プロファイルを形成します。

ユーザーキー

キーリストには常に 1 つの<USERKEY>キーも含まれます。これはユーザー固有のキーのプレースホルダで、システムが暗号化規則を解決するときに、個々のユーザーごとに自動的に生成します。

グループキー

<USERKEY>と同じように、<GROUPKEY>を使ってグループの全メンバーに共通のキー を生成することができます。

注意：<USERKEY>を使用する場合、このキーが割り当てられたユーザーのみがデータにアクセスできるようにしてください。他のユーザーはこのデータを復号化できません。

例<USERKEY>の使用例: すべてのユーザーが同じネットワークドライブ U:で作業しています。適切なユーザーだけがそのディレクトリにアクセスできます。

これを指定する暗号化ルールは次のようになります。

u:„*.*<ユーザーキー>

他の例としては、ローカルの一時ディレクトリを暗号化するのに<USERKEY>を使うことができます。

パスのないキーの割り当て

定義された暗号化パスのリストには、パスなしでキーを割り当てるというプレースホルダも含まれています。

これは、暗号化パスが存在しないデータを暗号化するために使用できるキーをユーザーに与えるために使用されます。例えば、暗号化されたファイルが、暗号化ルールが定義されていない（暗号化が解除されている）場所にコピーされた場合などに起こります。その場合、このキーを使って適切なキーでファイルにアクセスすることができます。パスのないキーは通常、データの再暗号化にも必要であり、常にこの（古い）キーの暗号化ルールがなくなった場合に必要です（暗号化ルールの注釈も参照してください）。

パスのないキーが割り当てられた場合、システムは自動的に新しいプレースホルダを作成し、パスのない他のキーを生成できるようにします。

1. 該当するオプションを選択してください。
2. ［コメント］には、作成した暗号化ルールの説明や情報を入力できます。
3. OK をクリックします。

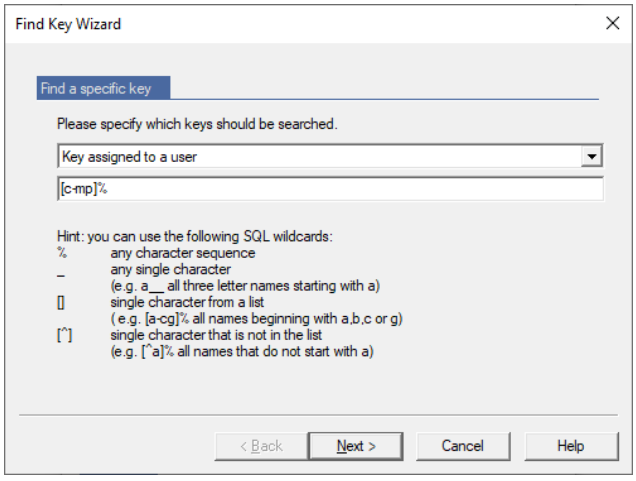
新しい暗号化ルールが u.trust LAN Crypt 管理コンソール に表示されます。

既存の暗号化ルールを編集するには、そのルールを選択し、コンテキストメニューの Properties をクリックします。該当するエントリーをダブルクリックすることもできます。

注意：暗号化ルールは、作成されたグループでのみ変更できます。

3.16.5 特定のキーの検索

特定のキーを検索］ ボタンを押すと、特定のキーを検索するためのウィザードが起動します。ウィザードで選択したキーがキーリストに追加され、暗号化ルールに使用できるようになります。キーは一時的に追加されます。ウィザードを再度実行して別のキーを選択すると、前に追加したキーはリストから削除されます。



最初のページでは、検索条件を定義できます。ドロップダウンリストから以下の条件を選択できます：

- ユーザーに割り当てられたキー

  ユーザーに割り当てられたすべての特定のキーを検索します。編集フィールド（検索条件）にユーザー名またはログオン名を入力します。ワイルドカード検索を実行するには、SQL ワイルドカードを使用します。例えば、"Peter%"は、ユーザー名またはログオン名が "Peter "で始まるユーザーに割り当てられたすべてのキーを検索します。）

- グループに割り当てられたキー

  グループに割り当てられているすべての特定のキーを検索します。グループ名を入力してください。

- キー名

  特定の名前のキーをすべて検索します。キーの長い名前または短い名前を入力します。

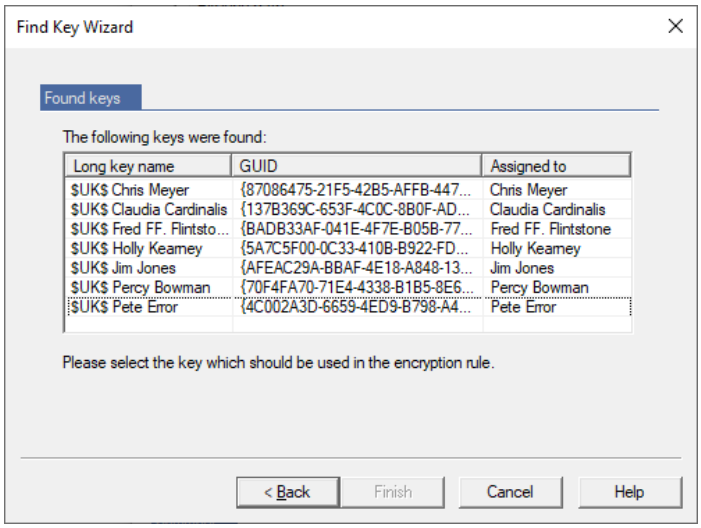
- キーGUID

  特定の GUID を持つ特定のキーをすべて検索します。キーの GUID を入力してください。

- 現在、キーは割り当てられていません。

  現在ユーザーまたはグループに割り当てられていないすべてのキーを表示します。

検索結果は 2 ページ目に表示されます。



キーが現在割り当てられている場合、ユーザー名またはグループ名が割り当て先の下に表示されます。リストには、特定のキーだけが表示されます。

キーを選択し、［完了］をクリックすると、暗号化ルールの作成ダイアログのリストにキーが追加されます。

3.17 暗号化タグ

DLP 製品が暗号化が必要なデータを特定した場合、u.trust LAN Crypt Client API を使用してこれらのファイルを暗号化することができます。u.trust LAN Crypt 管理コンソールでは、使用する u.trust LAN Crypt キーを指定するさまざまな暗号化タグを定義できます。

Client API は、これらの定義済み暗号化タグを使用して、異なるコンテンツに特別なキーを適用することができます。 たとえば、暗号化タグ<CONFIDENTIAL>を使用して、DLP 製品によって機密に分類されるすべてのファイルを暗号化することができます。

キーへの参照の使い方の例は次の通りです。

SGFEAPI enCrypt /Tag:CONFIDENTIAL c:¥documentsfinancial-figures.docx

〈CONFIDENTIAL〉 タグに関連付けられているキーを使用して、c: ¥documents フォルダ内の financial-figures.docx ファイルを暗号化します。

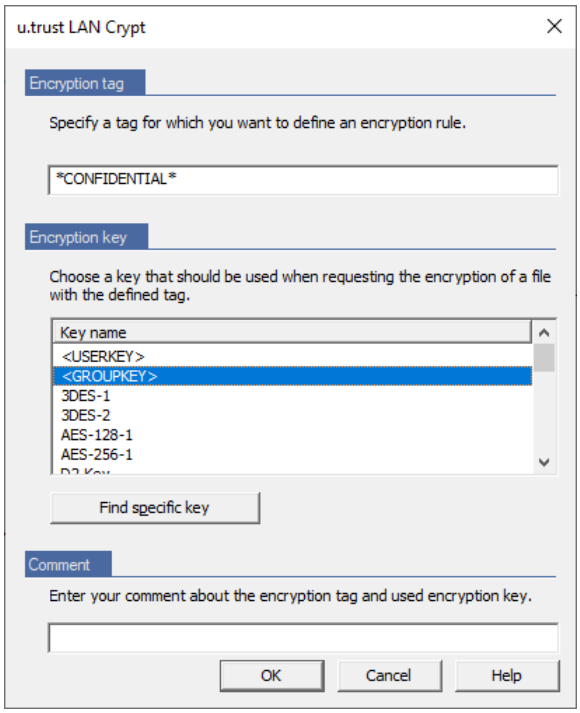
暗号化タグを生成するには、以下を行います。

1. 該当するグループノードの下にある暗闘化ルールとタグを右クリックし、コンテキストメニューの新規暗号化タグをクリックします。

   また、右側のコンソールペインで右クリックすると表示されるコンテキストメニューから、新規暗号化タグコマンドにアクセスすることもできます。右側のコンソールペインでは、生成されたすべての暗号化ルールを見ることができます。

2. 暗号化タグの下の入力フィールドに暗号化タグの名前を入力します。

3. キーを選択します。



詳しくは、解凍したインストールパッケージの¥api フォルダにあるクライアント API ドキュメントをご覧ください。

注意： デフォルトのビューでは、<USERKEY>と<GROUPKEY>のプレースホルダとセキュリティオフィサーが作成したキーだけが表示されます。特定のキーを検索ボタンを使用すると、特定のキーを検索して表示することができます。

ユーザーキー

キーリストには常に 1 つの<USERKEY>キーも含まれます。これはユーザー固有の キーのプレースホルダーで、システムが暗号化規則を解決するときに、個々のユーザーごとに自動的に生成します。

グループキー

<USERKEY>と同じように、<GROUPKEY>を使ってグループの全メンバーに共通のキー を生成することができます。

注意：<USERKEY>を使用する場合、このキーが割り当てられたユーザーのみがデータにアクセスできるようにしてください。他のユーザーはこのデータを復号化できません。

4. コメントの下に、作成された暗号化タグの説明や情報を入力することができます 。

5. OK をクリックします。

新しい暗号化タグが u.trust LAN Crypt 管理コンソールに表示されます。

既存の暗号化タグを編集するには、タグを選択し、コンテキストメニューのプロパティをクリックします。該当するエントリーをダブルクリックすることもできます。

3.18 証明書の割り当て

各プロファイルは所有者の公開キーで保護されています。この公開キーは、u.trust LAN Crypt 管理コンソールで、証明書を介してユーザーに割り当てる必要があります。

u.trust LAN Crypt 管理コンソールにより、各ユーザーに証明書（*.p12 ファイル）が割り当てられます。このファイルには秘密鍵も含まれています。u.trust LAN Crypt は対応する暗証番号をパスワードログファイル(p12pwlog.csv)に書き込みます。このファイルは不正アクセスから常に保護されている必要があります。これを実現するには、u.trust LAN Crypt 管理コンソール部門の（マスター）セキュリティオフィサーが u.trust LAN Crypt クライアントアプリケーションをインストールし、パスワードログファイルの暗号化ルールを作成します。

注意：u.trust LAN Crypt コンポーネントの管理コンソールとクライアントアプリケーションを同じコンピュータにインストールする場合は、同じバージョンである必要があります。

または、PKI からの証明書を使用することもできます。証明書の割り当てを開始する前に、証明書ストアまたはディレクトリ（LDAP など）で証明書がすでに使用可能になっていることをお勧めします。標準の Windows ツールを使用して、証明書を関連する証明書ストアにインポートできます。

u.trust LAN Crypt には、証明書を自動的に割り当てる証明書割り当てウィザードがあります。

注意：証明書を作成するセキュリティオフィサーが、ファイルシステムのパスワードログファイルを変更する権限を持っていない場合、u.trust LAN Crypt 証明書を生成することはできません。

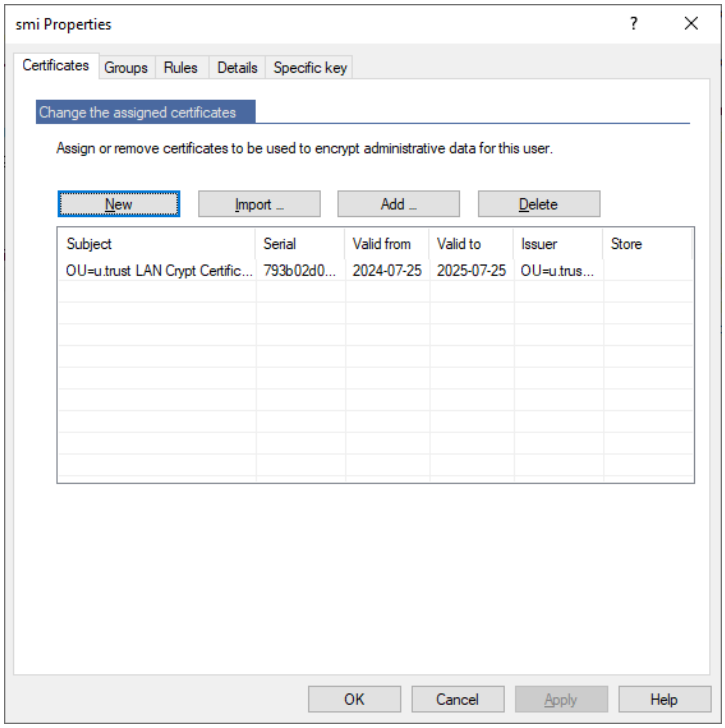
3.18.1 ユーザーへの証明書の割り当て

証明書を割り当てるには、以下の手順に従います。

1. 該当するグループノードで、グループのメンバーと証明書を選択します。右側のコンソールペインに、全ユーザーのリストが表示されます。

2. ユーザーをダブルクリックするか、ユーザーを右クリックし、コンテキストメニューからプロパティを選択します。プロパティダイアログが表示されます。

3. このダイアログでは、以下のオプションのいずれかを選択して、1 つまたは複数の証明書をユーザーに割り当てます。



- 新規
  u.trust LAN Crypt に新しい証明書を生成させたい場合は、新規をクリックします。利用可能な証明書がない場合、u.trust LAN Crypt 管理コンソールコンソールで証明書を生成することもできます。ただし、これらの証明書を使用するのは u.trust LAN Crypt だけです。

  生成された証明書は、デフォルトのディレクトリに PKCS#12 ファイルとして保存されます（中央設定ノードのディレクトリタブを参照）。

  注意：このようにして生成された証明書は、適切なユーザーに配布する必要があります。そうしないと、そのユーザーは暗号化プロファイルにアクセスできません。

■ インポート...

必要な証明書がまだ証明書ストアに存在しない場合、利用可能な証明書のリスト（ ）には表示されません。

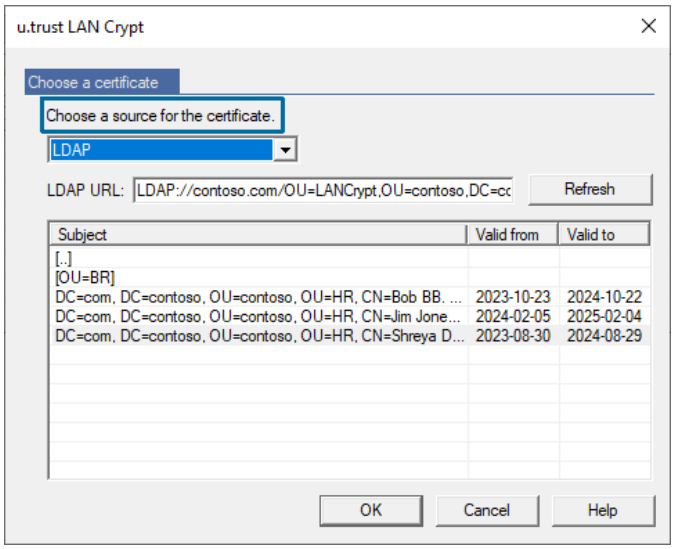
この場合、[インポート...] をクリックします。ダイアログが開き、必要な証明書を選択できます。OK をクリックすると、証明書がユーザーに割り当てられます。

インポート証明書は、他の人という証明書ストアに自動的にインポートされます。

注意：*.cer、*.crt、または *.der 形式の証明書ファイルのみインポートできます。*.p12 または*.pfx ファイルはインポートできません。

■ 追加...

証明書のソースを選択します。



証明書ストアからの証明書の割り当て

既存の証明書をユーザーに割り当てるためのダイアログを開きます。このダイアログには、証明書ストアに存在するすべての証明書のリスト が表示されます。

LDAP ソースを使用した証明書の割り当て

u.trust LAN Crypt では、LDAP ソースから証明書を割り当てることができます。

これを行うには、[証明書のソースの選択]ダイアログのドロップダウンリストから LDAP を選択します。

LDAP ソースの URL を入力する編集フィールドが表示されます。再読み込みをクリックすると、LDAP ソースの内容が表示されます。

角括弧内の用語（[Sub_OU_1]など）は、LDAP ソース内の OU を表します。OU の証明書を表示するには、その OU をダブルクリックします。

...をダブルクリックすると、1 つ上の階層に移動します。

証明書を選択し、OK をクリックします。これで証明書がセキュリティオフィサーに割り当てられました。

注意：LDAP サーバーが匿名ログオンを許可していない場合、サーバーのログオン資格情報は、中央設定のサーバータブで識別名（例：CN=John Doe,OU=Sales）として入力する必要があります。

注意：LDAP ディレクトリから割り当てられた証明書がある場合、この証明書に属する秘密鍵がユーザーのワークステーションで利用可能である必要があります。

4. 説明されているオプションのいずれかを使用して証明書を選択し、OK をクリックします。

システムは、右側のコンソールペインでユーザーの横に証明書を表示します。コンソールペインには、使用されている証明書に関する情報(有効期間、シリアル番号、発行者)が表示されます。

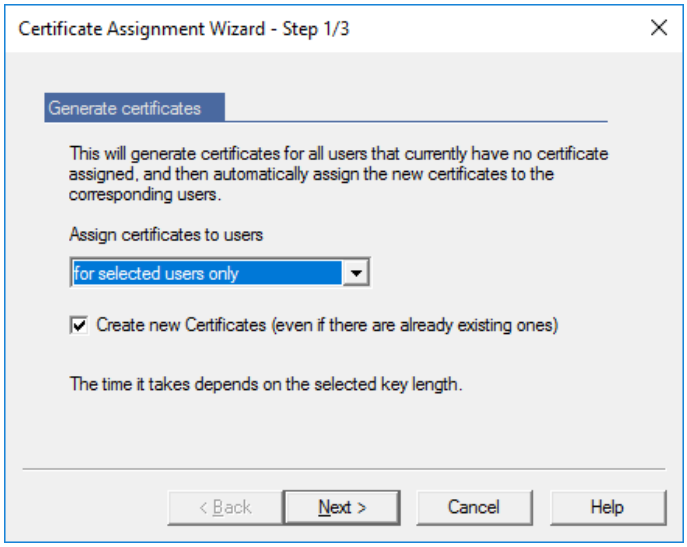
注意：証明書スナップインは、各ユーザー/グループノードの下にあります。ここでは、関連するグループのメンバであるユーザーのみが表示されます。

3.18.2 u.trust LAN Crypt 証明書の生成と割り当て

このウィザードを使用して、証明書がまだ割り当てられていないすべてのユーザー用の証明書を生成し、これらの証明書をユーザーに自動的に割り当てます。

このウィザードを開くには、グループノードの各メンバーと証明書のコンテキストメニューで 証明書の作成 をクリックするか、ツールバーの該当するアイコンをクリックします。

次のダイアログで、証明書をこのグループのみで生成して割り当てるか、このグループとすべてのサブグループで生成して割り当てるか、または選択したユーザーに対してのみ生成して割り当てるかを指定します。



新しい証明書を作成する（既存の証明書が既に存在する場合でも）オプションをオンにすると、選択したすべてのユーザーに対して新しい証明書が作成されます。

特定のユーザーのみ

このオプションは、1 人以上のユーザーが選択されている場合にのみ表示されます。左側のコンソールペインの目的のグループノードの下でグループのメンバーと証明書をクリックす

ると、グループのメンバーが右側のコンソールペインに表示されます。ユーザーの選択は、Window エクスプローラと同じ方法で行います（SHIFT キーまたは CTRL キーを押しながら、マウスの左ボタンでユーザーを選択します）。

システムが証明書を自動的に生成し、割り当てます。終了をクリックして、ウィザードを閉じます。

注意：ここで生成されたキーファイル(*.p12)とセキュリティオフィサーの証明書の公開部分は、中央設定で指定されたディレクトリに保存され、ユーザーが利用できるようにする必要があります。この設定を行うには、u.trust LAN Crypt 設定で、ポリシーファイルの秘密鍵が存在しない場合に、u.trust LAN Crypt がユーザーの*.p12 ファイルを検索するフォルダを指定します。

セキュリティオフィサーの証明書の公開部分も同様です。u.trust LAN Crypt がユーザーキーファイルを自動的に認識できるように、ファイル名はユーザーのログオン名（logon.p12）と一致している必要があります。

u.trust LAN Crypt は正しいファイルを見つけると、PIN ダイアログを表示します。この PIN をユーザーに伝えるために PIN を送信する必要があります（パスワードログファイルにあります）。ユーザーが PIN を入力すると、証明書と関連するキーが自動的にインポートされます。

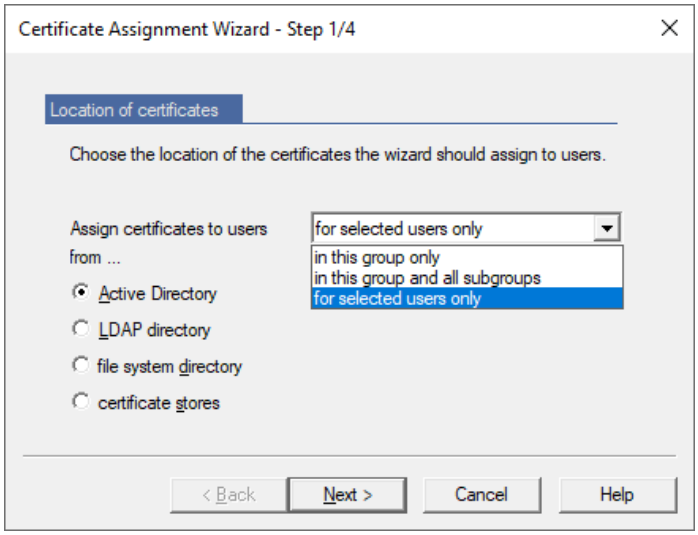
u.trust LAN Crypt は、セキュリティオフィサーの証明書の公開部分を含む*.cer ファイルを見つけると、自動的にインポートします。

または、ユーザー用のキーファイルと管理者証明書のパブリック部分を手動で配布することもできます。この場合、クライアントがその両方をインポートするようにしてください。

3.18.3 証明書の割り当てウィザード

u.trust LAN Crypt には、証明書をユーザーに割り当てる作業のほとんどを実行するウィザードがあります。ウィザードを実行するには、コンテキストメニューのグループのメンバーと証明書から証明書の割り当てウィザードを選択します。

ウィザードの最初のダイアログで、証明書をこのグループのメンバーのみに割り当てるか、このグループとすべてのサブグループに割り当てるか、または選択したユーザーのみに割り当てるかを指定します。



特定のユーザーのみ

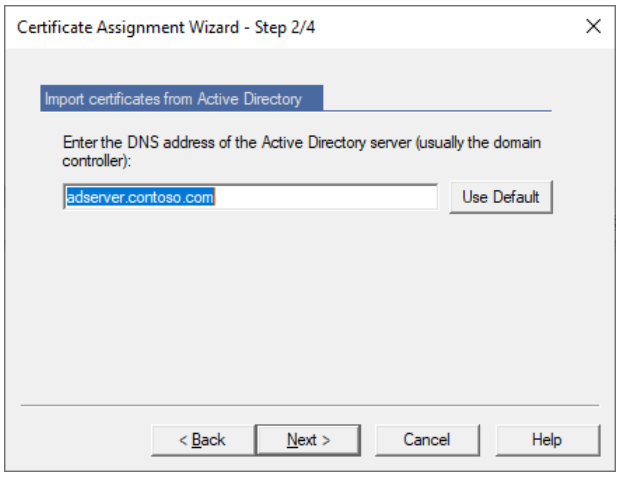
このオプションは、1 人以上のユーザーが選択されている場合にのみ表示されます。左側のコンソールペインの目的のグループノードの下でグループのメンバーと証明書をクリックすると、グループのメンバーが右側のコンソールペインに表示されます。ユーザーの選択は、Windows エクスプローラと同じ方法で行います（SHIFT キーまたは Ctrl キーを押しながら、マウスの左ボタンでユーザーを選択します）。

ウィザードは、以下のソースからの証明書の割り当てをサポートしています。

- Active Directory からユーザーへの証明書の割り当て
- LDAP ディレクトリからユーザーへの証明書の割り当て
- ファイルシステムのディレクトリからユーザーに証明書を割り当て
- 証明書ストアからユーザーへの証明書の割り当て

3.18.3.1 Active Directory からの証明書の割り当て

Active Directory からユーザーに証明書を割り当てるオプションを選択した場合は、手順 2 で Active Directory コントローラの名前を FQDN 形式で入力する必要があります（例：Active Directory からユーザーに証明書を割り当てる）。



デフォルトを使用をクリックすると、現在ログオンしているドメインコントローラのアドレスが適用されます。

ウィザードを開始するには、次へをクリックします。システムが証明書を自動的にインポートして割り当てます。証明書が正常に割り当てられたことを確認するメッセージが表示 されます。終了をクリックして、ウィザードを閉じます。

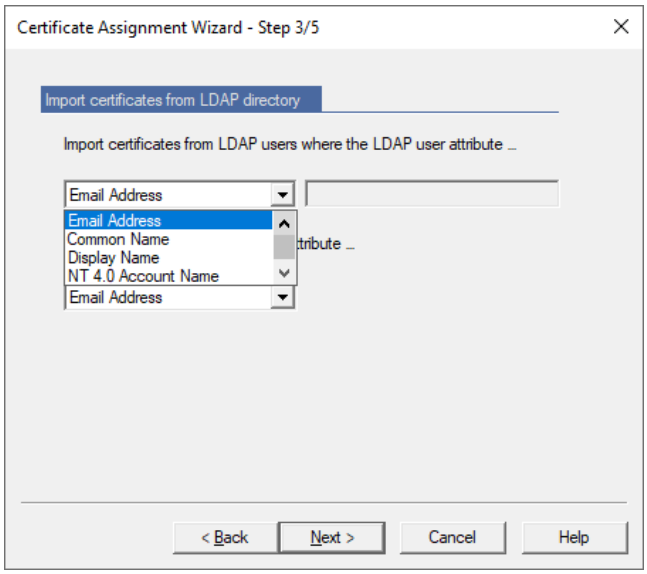
3.18.3.2 LDAP ディレクトリからの証明書の割り当て

LDAP ディレクトリのユーザーに証明書を割り当てオプションを選択した場合は、手順 2 で証明書をインポートする LDAP ディレクトリのアドレスを入力する必要があります。

注意：
Microsoft AD
入力フィールドが空白のままであってはなりません。ここには少なくともドメインと国を入力する必要があります。
例 1：DC=mydomain,DC=COM
例 2：OU=marketing,DC=mydomain,DC=COM

[デフォルトを使用]をクリックすると、現在ログオンしているドメインコントローラのアドレスが適用されます。

証明書を割り当てるには、LDAP ユーザーのプロパティを u.trust LAN Crypt ユーザーと照合します。



以下の LDAP ユーザープロパティが使用できます。

- メールアドレス
- コモンネーム(CN)
- 表示名
- NT4.0 アカウント名
- ユーザープリンシパル名 (UPN)
- サーネーム
- <other>, ユーザー定義属性

これらのプロパティが以下の u.trust LAN Crypt ユーザーのプロパティと一致するように指定できます：

- メールアドレス
- ユーザー名
- ログオン名
- コメント

各 u.trust LAN Crypt ユーザープロパティに対応させたい LDAP ユーザープロパティを選択します。

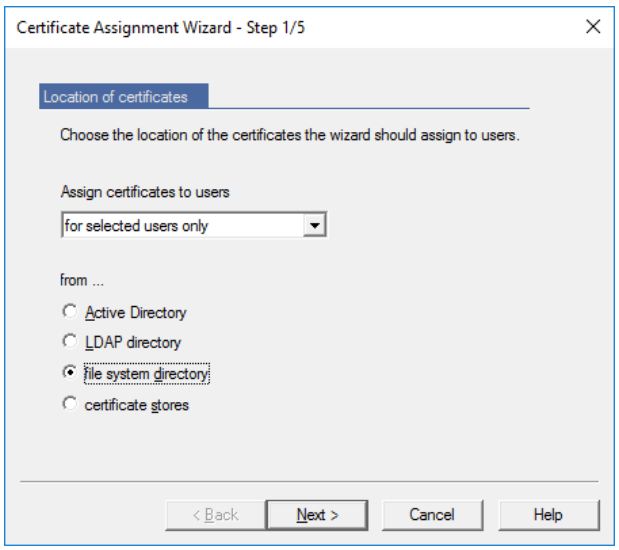
これらのプロパティが一致する場合、システムは LDAP ユーザーの証明書をインポートし、適切な u.trust LAN Crypt ユーザーに自動的に割り当てます。

注意：矛盾を防ぐため、常に一意であるメールアドレスを割り当て基準として使用することをお勧めします。

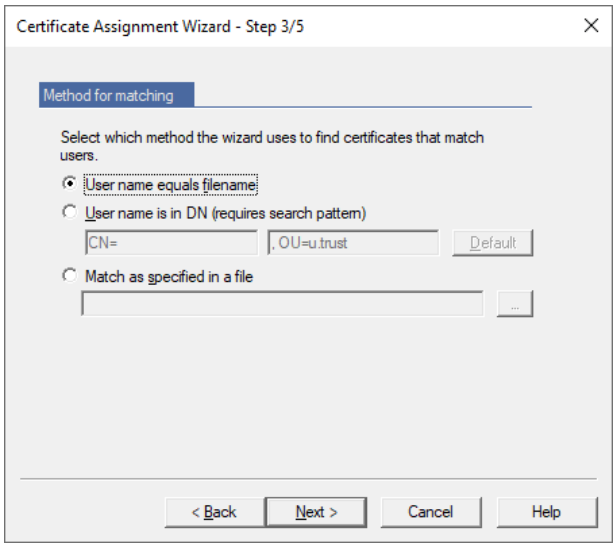
ウィザードを開始するには、次へをクリックします。システムが証明書を自動的にインポートして割り当てます。証明書が正常に割り当てられたことを確認するメッセージが表示されます。終了をクリックして、ウィザードを閉じます。

3.18.3.3 ディレクトリからの証明書の割り当て

LDAP ディレクトリのユーザーに証明書を割り当てオプションを選択した場合は、手順 2 で、証明書をインポートするディレクトリのアドレスを入力する必要があります。



ディレクトリを指定した後、u.trust LAN Crypt がユーザーに証明書を割り当てる方法を定義するダイアログが表示されます。



- ユーザー名=ファイル名

  証明書ファイルのファイル名がユーザー名と同じ場合は、このオプションを選択します。

  ファイル名に対応するすべてのユーザーは、適切な証明書に割り当てられます。

- ユーザー名が DN にある（検索パターンが必要です）。

  u.trust LAN Crypt は、証明書の識別名にユーザー名が含まれている場合、そのユーザー名を検索し、適切なユーザーに証明書を割り当てることができます。u.trust LAN Crypt は、検索パターンを使用して DN 内のユーザー名を特定します。

  この検索パターンは、[ユーザー名が DN にある]オプションの入力フィールドで指定できます。システムは、DN 内で指定された 2 つの文字列の間に表示されるユーザー名を検索します。

  例

  証明書では、ユーザー名は常に CN=の下に存在します。

  (例：CN=DSmith,OU=u.trust)

  最初の入力フィールドに CN=を入力し、2 番目の入力フィールドに OU=u.trust を入力すると、LAN Crypt はこの 2 文字の文字列の間にあるユーザー名（この例では DSmith）を検索します。証明書は自動的にユーザーに割り当てられます。

- ファイルで指定された一致

  必要な課題をファイルから取り出すこともできます。

  たとえば、Utimaco Smartcard Administration で生成された証明書のパブリック部分は、あらかじめ定義されたディレクトリのファイルに保存されます。Utimaco Smartcard Administration はこれらのファイルを使用して、各ユーザーにどの証明書が割り当てられているかを記録するファイルを生成します。他の PKI でもこの種のリストを生成できます。もちろん、このリストは自分で生成することもできます。

  以下の書式を使用してください。

  ユーザー名;ファイル名

  例

  ゲスト

  DSmith;DSmith.cer

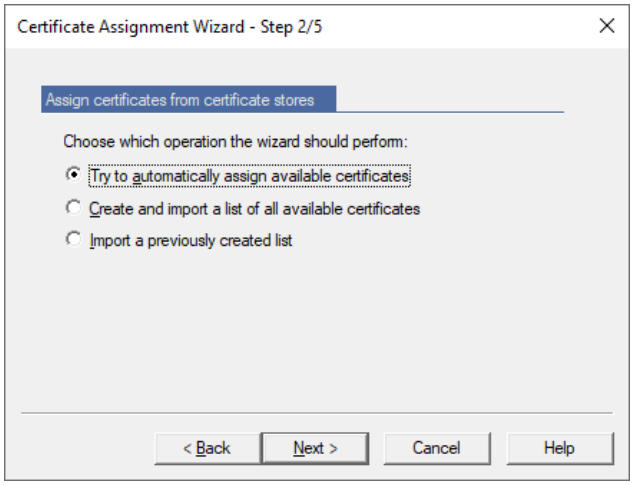
  ....

システムは、このファイルの割り当てに従って証明書を割り当てます。

次へをクリックしてウィザードを開始し、証明書を自動的に割り当てます。

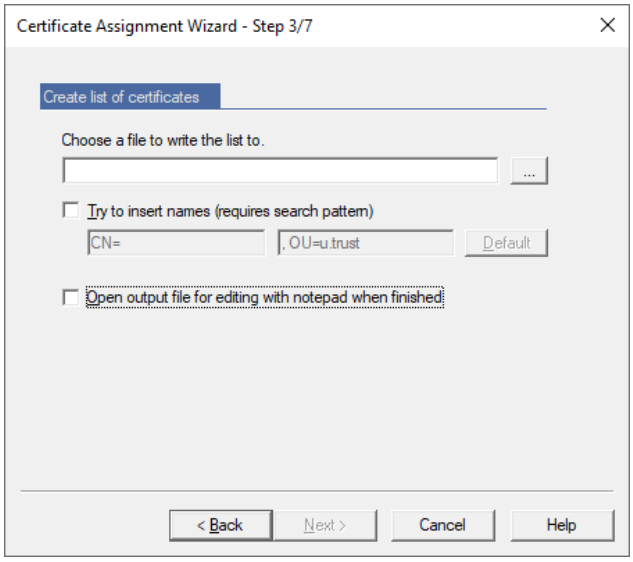
3.18.3.4 証明書ストアからの証明書の割り当て

証明書ストアからユーザーに証明書を割り当てるオプションを選択した場合、ウィザードの第 2 ステップでは、利用可能なすべての証明書のリストを生成してインポートするか、既存のリストをインポートするかを指定するよう求められます。u.trust LAN Crypt はこのリストを使用して証明書を割り当てます。



例えば、割り当てが既に一度、開始されたが、リストが生成された後にプロセスが中断された場合、以前に作成されたリストをインポートオプションを使用することができます。システムはここで作成されたファイルを再利用できます。

[利用可能なすべての証明書のリストを作成し、インポート]オプションを選択すると、このダイアログが表示されます。



リストを書き込むファイルを選択します。

u.trust LAN Crypt は、証明書ストアで利用可能なすべての証明書のリストを作成します。このリスト には、証明書を割り当てるユーザー名のプレースホルダが含まれています。

例

*****; My; OU=u.trust LAN Crypt Certificate, CN=LAN Crypt Admin; 0010-ae671e47...

*****ルート; CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com; 0010-4cad...

プレースホルダー（*****）はユーザー名で置き換えることができます。

証明書にユーザー名が含まれている場合は、以下のオプションを使用できます：

- 名前の挿入

  u.trust LAN Crypt はユーザーを認識しようとします。証明書の識別名(DN)にユーザーの名前が含まれていれば、u.trust LAN Crypt はそれを見つけ、適切なユーザーに証明書を割り当てることができます。u.trust LAN Crypt は検索パターンを使って DN に含まれるユーザーの名前を特定します。

  ユーザー名が DN にあるオプションの入力フィールドで検索パターンを指定します。システムは、DN 内の指定された 2 つの文字列の間にあるユーザー名を検索します。

  例

  証明書では、ユーザー名は常に"CN="になります。

  (例：CN=DSmith,OU=u.trust)

  最初の入力フィールドに CN=と入力し、2 番目の入力フィールドに OU=u.trust と入力すると、u.trust LAN Crypt はこの 2 文字の文字列の間にあるユーザー名（この例では DSmith）を検索します。システムはプレースホルダをユーザー名に置き換え、証明書を自動的にユーザーに割り当てます。

- 終了後、メモ帳で編集するために出力ファイルを開きます。

  このオプションを選択すると、生成後に証明書のリストが開きます。 このリストを編集できます。関連する証明書のプレースホルダをユーザー名で置き換えることができます。リストを保存すると、システムは編集したバージョンを使用して証明書を割り当てます。

次へをクリックしてウィザードを開始し、証明書を自動的に割り当てます。

3.19 暗号化ルールの提供 - ポリシーファイルの生成

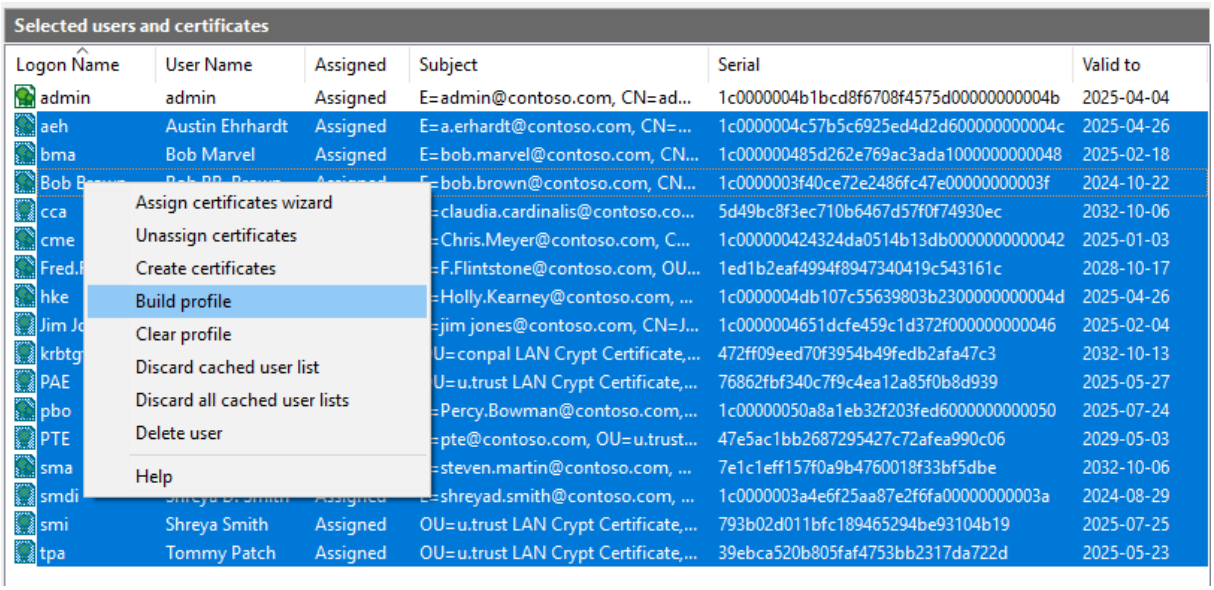
u.trust LAN Crypt は、生成（または変更）されたすべてのプロファイルを 管理データベースに保存します。ここではまだ個々のユーザーには影響しません。

個々のプロファイルを解決してポリシーファイルを作成するには、u.trust LAN Crypt セキュリティオフィサー が u.trust LAN Crypt プロファイルリゾルバーを実行する必要があります。これにより、管理コンソールでの設定に従って、各ユーザーのポリシーファイルが生成されます。次にユーザーがログオンすると、システムは新しい暗号化プロファイルをロードします。

注意：u.trust LAN Crypt 管理コンソールコンソールで設定を変更（新しいキーの追加、新しいルールの追加、TrustBuilder MFA...）した後は、必ず新しいポリシーファイルを生成する必要があります。この変更は、ユーザーが新しいポリシーファイルを自分のマシンにロードした後に有効になります。

3.19.1 グループ全体または選択したユーザーのポリシーファイルの作成

ポリシーファイルは、プロファイルの作成ウィザードで作成されます。複数のユーザーを選択し、ツールバーまたはユーザーのコンテキストメニューからプロファイルの作成を開始すると、ウィザードが起動します。



単一のユーザーで、コンテキストメニューからプロファイルの作成/クリアを選択した場合、プロファイルは即座に作成されます。メッセージボックスがセキュリティオフィサーに結果を通知します。

注意：コンテキストメニューでプロファイルのクリアオプションを選択すると、そのユーザーには空のプロファイルが作成されます。u.trust LAN Crypt クライアントを使用してプロファイルを更新すると、このユーザーは暗号化ルールと暗号キーを使用できなくなります。暗号化されたデータへのアクセスはできなくなります。このユーザーには、いつでもプロファイルを再度提供することができます。u.trust LAN Crypt クライアント経由でプロファイルが再度更新された場合のみ、このユーザーは暗号化ルールとキーが定義された暗号化プロファイルを受け取り、再び暗号化されたデータを扱うことができるようになります。

ウィザードを起動するビューによって、ウィザードのエントリーポイントは異なります：

- スコープの選択（デフォルト）
- ユーザーの収集と証明書の検証

  スコープの選択ができない、または許可されていない場合、たとえば、選択されたユーザーと証明書ノードで選択されたユーザーに対してプロファイル作成が開始されている場合など。
- プロフィールの作成

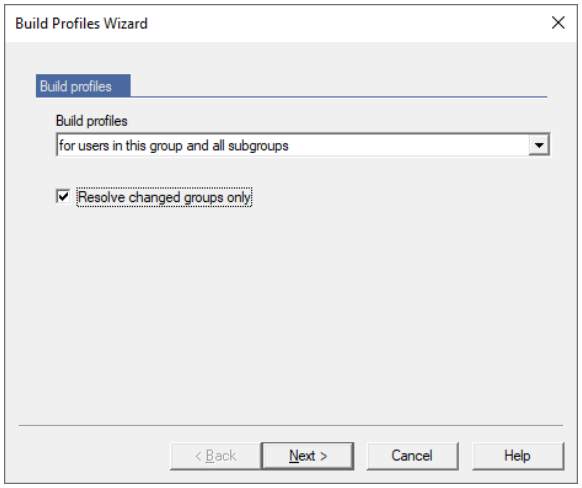
  複数のユーザーに対してプロファイルのクリアを開始した場合。グループ全体に対してこのアクションを開始することはできません。証明書のチェックは必要ありません。

ウィザードの最初のページで、プロファイル作成の範囲を選択できます。

プロファイルの作成

- このグループのユーザーのみ
- このグループとすべてのサブグループのユーザー
- 選択されたユーザーのみ

  変更されたグループのみを解決するオプションを有効にすると、変更によって新しいポリシーファイルが必要になったユーザーにポリシーファイルの作成が制限されます。これにより、大規模な組織におけるポリシーファイルの生成を高速化できます。



ウィザードの 2 ページ目では、すべてのユーザーデータが収集され、ユーザーの証明書が検証される間、進行状況が表示されます。すべてのユーザーの処理が完了すると、次のページが表示されます。

ウィザードの 3 ページ目には、証明書に関する警告が表示されます。ユーザーに有効な 証明書が割り当てられていない場合、またはユーザーの証明書の有効期限が間もなく切れる場合、そのユーザーはこのページに表示されます。

以下の証明書の警告とエラーが表示されます。

- ユーザーの証明書はまもなく期限切れになります（警告）
- ユーザーの割り当てられた証明書はすべて期限切れです（エラー）
- ユーザーに証明書が割り当てられていません（エラー）
- このユーザーには証明書が割り当てられていないため、スキップするようマークされています（警告）

エラーの場合、プロファイル作成を続行する前に、このページのオプションの少なくとも 1 つを選択する必要があります。

- リストに表示されたユーザーに対して再度警告をしないでください。

  証明書の有効期限が切れているか、証明書が割り当てられていないすべてのユーザーをスキップします。これらのユーザーは、新しい証明書が割り当てられるまで、プロファイル作成時にスキップされます。

- 有効な証明書が割り当てられていないユーザーを常にスキップ

有効な証明書がないすべてのユーザーを無視します。これはグローバル設定であり、中央設定でも構成できます。

Back ボタンをクリックして、ウィザードのスコープ選択ページに戻ります。

ウィザードの 4 ページ目には、すべてのプロファイルが作成されている間、プログレスバーが表示されます。ウィザードはキャンセルできますが、これはプロファイルの作成を停止します。すでに作成されたポリシーファイルは削除されず、元に戻されません。

ウィザードの最後の 5 ページ目には、作成されたプロファイルの数が表示されます。 プロファイル作成を強制的に停止するエラーが発生した場合は、エラーメッセージが表示されます。

注意：[中央設定]の[アンチウイルス]タブ、[ルールの解決]タブ、または[その他の設定]タブで変更を行うと、すべてのユーザーのポリシーファイルが常に変更されます。このタイプの変更後、すべてのユーザーの新しいポリシーファイルを作成する必要があります。

3.19.2 証明書スナップインによる選択されたプロビジョニング

証明書スナップインを使用して、ポリシーファイルを提供することもできます。このスナップインには、[グループのメンバーと証明書]ノードおよび各グループ ノードでアクセスできます。

証明書スナップインを使用してポリシーファイルを生成する場合は、 の追加機能も使用できます。

- 証明書を割り当てるユーザーを選択します。すべてのユーザーに対して新しいポリシーファイル を生成する必要はありません。

  Windows エクスプローラのように、複数のユーザーを同時に選択することができます（マウスクリック+SHIFT または Ctrl）。
- セキュリティオフィサーは、グループにどのユーザーが存在するかを即座に確認できます。
- システムは、ユーザー名の横に証明書アイコンを表示し、証明書のステータスを示します。
  - 赤色の意味

    証明書の有効期限が切れています。
  - 黄色の意味

    証明書が設定された有効期限警告期間内に実行されていること。
  - 緑色の意味

    何も問題ありません
  - 灰色の意味

    そのユーザーに証明書が割り当てられていないか、システムが証明書を割り当てる際にそのユーザーを見逃しています。

ポリシーファイルを提供するには、必要なユーザーを選択し、ツールバーの青い歯車アイコン、または選択したユーザーのコンテキストメニューのプロファイルのビルドをクリックします。

3.19.3 プロファイルのクリア

証明書スナップインを使用すると、1 人ないし複数のユーザーのプロファイルをクリアできます。プロファイルのクリアは、空のプロファイルを生成することを意味します。ユーザーは、空のポリシーファイルに 1 回ログオンして、マシンにキャッシュされている現在のポリシーファイルの設定を上書きする必要があります。その後、暗号化されたデータにアクセスできなくなります。

プロファイルをクリアするには、証明書スナップインでユーザーを選択し、[選択されたユーザーのプロファイルのクリア]アイコンをクリックするか、コンテキストメニューの[プロファイルのクリア]をクリックします。

（SHIFT キーを押しながらマウスの左ボタンでユーザーを選択）、アイコンをクリックして、複数のユーザーを選択すると、プロファイルをクリアできます。

注意：u.trust LAN Crypt 中央設定の設定は、プロファイルのクリア方法を定義します。プロファイルをクリアするプロセスは、プロファイルを構築するプロセスと似ています。

3.20 データベースのロギング

u.trust LAN Crypt は、u.trust LAN Crypt 管理コンソールコンソールで発生したイベントを u.trust LAN Crypt データベースに記録します。u.trust LAN Crypt のログ機能では、ログに記録するイベントを指定したり、イベントをアーカイブしたり、ログエントリーを確認したりすることができます。

グローバルパーミッション ロギングエントリーを読むとロギングの管理は、セキュリティオフィサーがロギングモジュールにアクセスする方法を制御します。これらの権限は、マスターセキュリティオフィサーがセキュリティオフィサーに与えることができます。

ロギングエントリーの読み込み	セキュリティオフィサーは、ログの設定とログされたイベントを見ることができます。
ログの管理	セキュリティオフィサーはログの設定を変更できます。彼らは、エントリーをアーカイブ、削除、チェックすることができます。

ロギングの基本設定は、u.trust LAN Crypt 管理コンソールコンソールの中央設定にあるロギングノードで行うことができます。このノードは、少なくともロギングエントリーの読み取り権限を持つセキュリティオフィサーのみが閲覧できます。

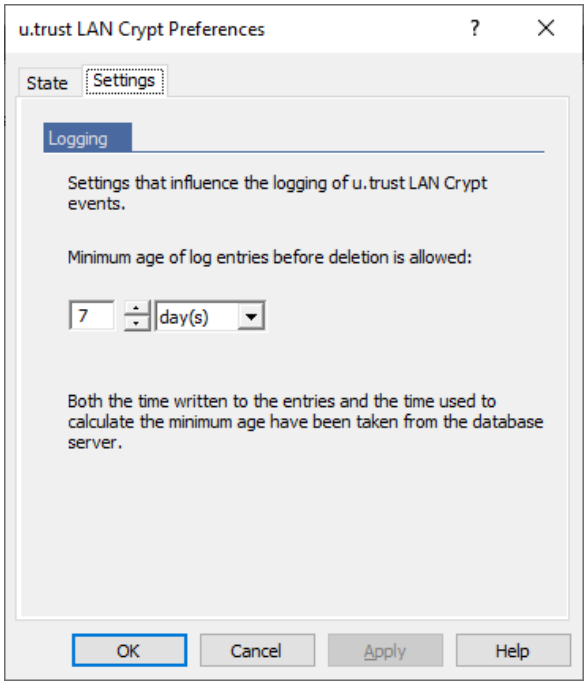
基本設定はマスターセキュリティオフィサーのみが行うことができます。2 つ目のレベルの権限を追加することで、 セキュリティを追加することができます（シナリオはログの管理であり、グローバル権限ログのエントリーの読み取りおよびログの管理が必要です。）。

基本設定では、どのイベントをログに記録するかも指定します。マスターセキュリティオフィサーだけが これを指定できます。

注意：セキュリティオフィサーがログオンする前に発生したイベントは、データベースに直接記録することはできません。これらはキャッシュされ、次のログオン成功後にデータベースに書き込まれます。

3.20.1 設定

ロギングノードのコンテキストメニューからプロパティをクリックすると、基本設定を行うダイアログが表示されます。



設定タブ

このページでは、ログエントリーを削除できる期間を指定します。

分散データベースを使用する場合、この設定により、各サイトでエントリーが削除される前に、本部にエントリーがコピーされることが保証されます。

ステートタブ

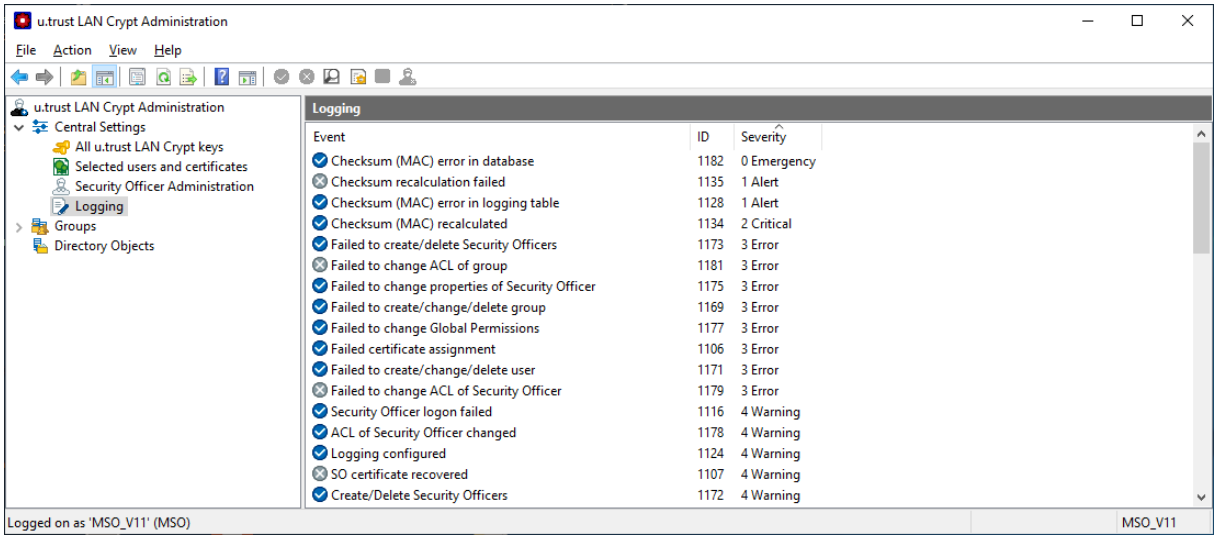
ステータスタブには、ログに記録されたエントリー数に関する情報が表示されます。複数の場所がある場合、表示は場所ごとに拡大されます。さらに、いくつのエントリーがすでにアーカイブされているか、削除できるかどうかも表示されます。

3.20.2 ログに記録されたイベント

ロギングノードを選択すると、ログに記録できるすべてのイベントが右側のコンソールペインに表示されます。ここで、どのイベントをログに記録するかを選択できます。

注意：マスターセキュリティオフィサーのみが、ログに記録するイベントを選択できます。

[重大度]列のヘッダーをクリックして、カテゴリ(緊急、アラート、エラー、警告、通知、情報)に従ってイベントを並べ替えます。



ログに記録するイベントを選択するには、イベントをダブルクリックするか、イベントを選択して ツールバーの該当するシンボルをクリックします。

- 選択されたイベントのロギングを有効にします。
- 選択されたイベントのロギングを無効にします。

複数のイベントを同時に選択できます（マウスクリック＋Shift または Ctrl）。

イベントを選択したら、ツールバーのディスケットアイコンをクリックして設定を保存します。ただし、保存せずにこのビューを離れると、その都度、設定を保存するかどうかを尋ねられます。

3.20.3 エントリーの表示とエクスポート

注意：エントリーを表示およびエクスポートするには、セキュリティオフィサーにグローバル権限ログエントリーの読み取りが必要です。

ログエントリーの読み取りグローバル権限を持っているセキュリティオフィサーは、エントリーを表示し、ファイルにエクスポートすることができます。

エントリーを表示するには、ロギングノードのコンテキストメニューで 表示とエントリーのエクスポート をクリックするか、ツールバーのアイコンをクリックします。

ログに記録されたエントリーを表示したり、エクスポートしたりするためのダイアログが開きます。

このダイアログは、ロギング用に選択されたすべてのイベントを表示します。

列のヘッダーをクリックして、エントリーを並べ替えます。

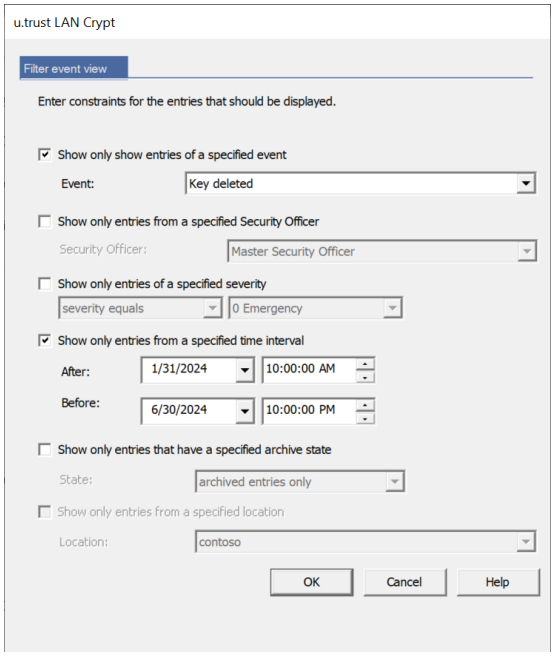
エントリーをダブルクリックすると、そのエントリーの詳細が表示されます。

u.trust LAN Crypt には、表示される エントリーに条件を指定できるフィルタもあります。

3.20.4 イベントのフィルタリング

ロギングの設定は、ロギングノードで定義できます。ロギングされたイベントを表示およびエクスポートするために、フィルタ機能を使用できます。ロギングノードが選択されている場合、コンテキストメニュー（マウスの右ボタン）またはアクションメニューの表示とエクスポートエントリーで定義できます。

ロギングのエントリーの表示とエクスポートノードをクリックすると、表示されるイベントのフィルタを指定するダイアログが開きます。



これらの制約を使用してイベントをフィルタリングできます：

- 指定したイベントのエントリーのみ表示

  このオプションを選択すると、ドロップダウンリストから選択したイベントのエントリーのみが 表示されます。リストには、ログに記録できるすべてのイベントが含まれます（キーの削除、ルールの変更など）。

- 指定したセキュリティオフィサーからのエントリーのみ表示

  このオプションを選択すると、ドロップダウンリストからセキュリティオフィサーを選択できます。すると、指定したセキュリティオフィサーがログオンしていたときに記録された、 これらのイベントのみが表示されます。ドロップダウンリストには、エントリーが存在するセキュリティオフィサーのみが含まれます。

- 指定した重要度のエントリーのみ表示

  このオプションを選択すると、どのエントリーを表示するかについて、特定の重大度レベルまたは重大度範囲を選択できます。重大度が以下および重大度が以上は、重大度レベルの前の数値を指します。

- 指定した時間間隔のエントリーのみを表示

  このオプションを選択すると、エントリーが記録された期間を定義できます。

- アーカイブ状態を指定したエントリーのみを表示

このオプションを選択すると、アーカイブされたエントリーのみを表示するか、まだアーカイブされていないエントリーのみを表示するかを指定できます(すでにアーカイブされたエントリーは、削除されるまでデータベースに残ります)。このオプションを選択しないと、両方のタイプのエントリーが表示されます。

- 指定した場所からのエントリーのみ表示

  このオプションを選択して、エントリーを表示する場所を指定します。分散データベースを使用している場合は、複数の場所が関係する可能性があります。データベースの複製方法によって、表示できる場所が決まります。

注意：エントリーの表示とエクスポート機能を実行した後でも、イベントの表示ダイアログのフィルターボタンをクリックすることでフィルタを定義することができます。また、この機能は表示メニューからフィルターを選択しても利用できます。

3.20.5 エントリーのアーカイブ、削除、チェック

注意：セキュリティオフィサーは、エントリーをアーカイブ、削除、およびチェックする前に、グローバル権限ログの管理が必要です。

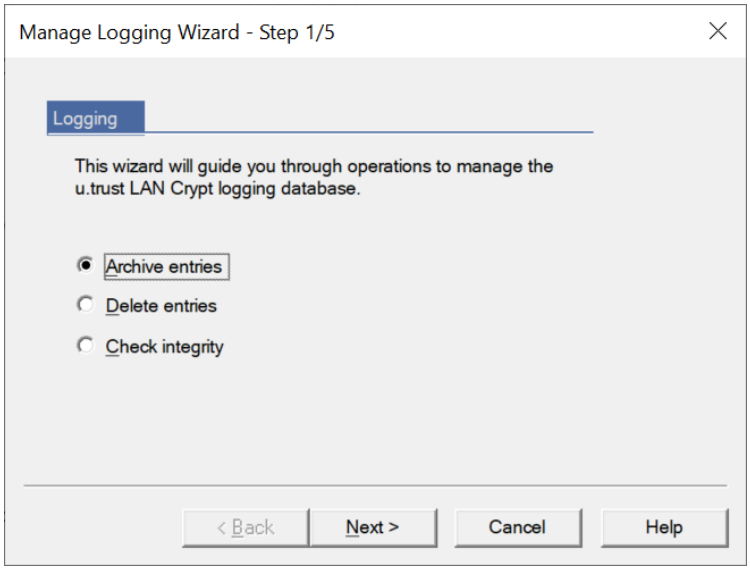
グローバル権限（ロギングの管理）を持つセキュリティオフィサーは、ログに記録されたエントリーをアーカイブ、削除、およびチェックできます。

アーカイブをクリックするか、ロギングノードのコンテキストメニューのエントリーを削除およびチェックするか、タスクバーのシンボルをクリックして、これらのタスクを実行するためのウィザードを起動します。

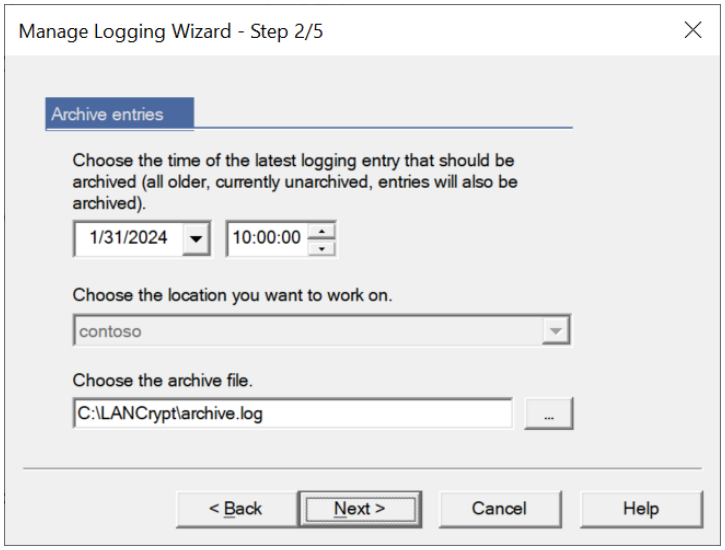
 記録されたエントリーをアーカイブ、削除、確認するためのウィザードを起動します。

エントリーのアーカイブ

エントリーをアーカイブするには、 [エントリーのアーカイブ]を選択し、[次へ]をクリックします。



- アーカイブされる最後のエントリーの日時。その時点から現在までのすべてのエントリーがアーカイブされます。さらに、この時点で、場所ごとにアーカイブすることもできます（利用可能な場合）。



注意：異なる場所を選択できるのは、分散データベースを使用している場合のみです。この時点でどの場所を選択できるかは、データベースの複製方法によって異なります。上の図では 1 つの場所のみが表示されています。場所は常に u.trust LAN Crypt のインストール時に定義したエントリーです。このエントリーは後から変更できません。

- エントリーを書き込むファイル名

次へをクリックします。次のダイアログで、選択されたエントリーの数を確認できます。次へをクリックします。すべてのエントリーがアーカイブされると、ウィザードの最後のダイアログが表示されます。終了をクリックしてウィザードを閉じます。

すでにアーカイブされたエントリーはデータベースに残り、削除することができます。その状態は、アーカイブ済みに設定されています。

アーカイブされたエントリーの削除

アーカイブされたエントリーを削除するには、[アーカイブされたエントリーの削除]を選択し、[次へ をクリックします。

次のダイアログで指定します。

- 削除される最後のエントリーの日付と時刻。その時点から現在までのすべてのエントリーが削除されます。

注意：可能な最後の時間は、ログノードの設定タブで定義できるログエントリーの指定された最小年齢に依存します。

- エントリーを削除する場所(もしある場合)。

次へをクリックします。次のダイアログで、選択されたエントリーの数を確認できます。Next をクリックします。すべてのエントリーが削除されると、ウィザードの最後のダイアログが表示されます。完了をクリックして、ウィザードを終了します。

アーカイブの完全性のチェック

ログに記録されたイベントの整合性をチェックするには、［アーカイブの整合性のチェック］を選択し、［次へ］をクリックします。

次のダイアログで、チェックするデータを選択します。データベース　またはアーカイブされたエントリーの中から、チェックするエントリーを選択できます。

分散データベースのエントリーをチェックするには、どの場所のエントリーをチェックするかを選択します。

アーカイブを確認する場合は、参照...ボタンをクリックしてファイルを選択します。

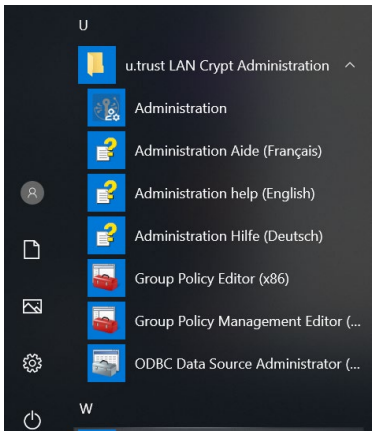
次へをクリックします。次のダイアログで、選択されたエントリーの数を確認できます。

Next をクリックします。すべてのエントリーのチェックが完了すると、ウィザードの最後のダイアログが表示されます。整合性チェックの結果が表示されます。データが操作されている場合は、適切な警告が表示されます。

終了をクリックしてウィザードを閉じます。

4 u.trust LAN 暗号化設定

注意：構成設定は、32 ビットのグループポリシー管理エディタ（GPME.msc）または 32 ビットのローカルグループポリシーエディタ（GPEdit.msc）で定義する必要があります。どちらのエディタも Windows のスタートメニューの u.trust LAN Crypt 管理コンソールフォルダにリンクされています。



これにより、正しいバージョンが開始されるようになります。

注意：Windows 10 マシンからドメインコントローラーの u.trust LAN Crypt グループポリシーを設定する場合は、グループポリシー管理コンソールを使用するために、まず Microsoft の Remote System Admin Toolkit（RSAT）をインストールする必要があります。また、RSAT は最近の Windows 10 バージョンでは 32 ビットのグループポリシー管理コンソールをサポートしなくなり、64 ビットバージョンのみをインストールすることに注意してください。この場合、u.trust LAN Crypt の管理テンプレートファイルをインストールする必要があります（このページの注意事項を参照してください）。

以下の設定は、マシン固有またはユーザー固有の設定です。これらの設定を編集するには、ドメインまたは Active Directory の管理者権限が必要です。これらの設定は、システム管理者のみが行ってください。

LAN CRYPT 設定ノードで構成設定を選択します。このノードは、管理コンソールの各コンピュータおよびユーザーノードでシステムポリシーを操作するときに表示されます。Active Directory 環境では、LAN Crypt 構成ノードは GPO コンピュータ構成またはユーザー構成（Windows 設定/u.trust LAN Crypt）に表示されます。

注意： 解凍したインストールパッケージの Config フォルダにある管理テンプレート(*.admx と *.adml) を使用することもできます。ADMX ファイルは、"C:/WindowsPolicyDefinitions "フォルダ、または利用可能な場合は中央ストアにコピーする必要があります。一方、各言語ファイル（*.ADML）は、対応する言語サブフォルダ（例："en-US"）にコピーする必要があります。

通常、設定はマシンを対象としています。しかし、選択したユーザーに特定の権限を割り当てるために、ユーザー固有の設定を行うことができます。ユーザー固有の設定を行うと、マシン固有の設定より優先されます。

ユーザー固有の設定を取り消し、マシン固有の設定を適用する場合は、その設定のステータスを設定されていませんに設定する必要があります。これを行うには、設定を選択し、DEL キーを押します。管理コンソールの[設定済み]列に[いいえ]と表示されます。

4.1 クライアント設定

クライアント設定ノードを選択すると、設定可能な項目が右側のコンソールペインに表示されます。エントリーをダブルクリックしてダイアログを開き、必要な設定を行います。

4.1.1 暗号化/復号化の許可

u.trust LAN Crypt のユーザーであれば誰でも、ファイルのコンテキストメニューからメニュー項目を選択することで、ファイルを暗号化または復号化することができます。つまり、ルールが定義されていないファイルを暗号化することもできます。

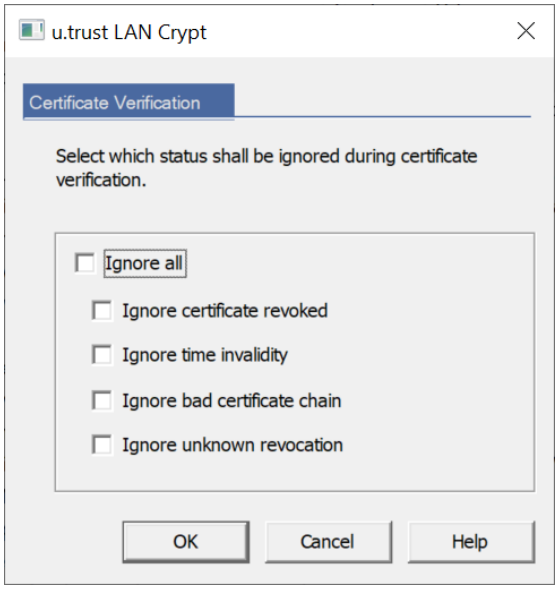
これを防ぎたい場合は、これらのファイルのコンテキストメニューにこのオプションを表示しないように、ここで指定することができます。

暗号化/復号化の許可

暗号化ルールが定義されていないファイルを、コンテキストメニューから暗号化または復号化できないようにします。

4.1.2 証明書検証中の無視

u.trust LAN Crypt では、ユーザー証明書をチェックする際に見つかったエラーを無視するかどうかを指定できます。



この手順は、証明書の有効期間が終了し、新しい証明書がまだない場合に便利です。ユーザーが暗号化プロファイルに引き続きアクセスできるように、新しい証明書が発行されるまで有効期間のチェックを無視できます。

その結果、実際には有効期限が切れている同じ証明書を引き続き使用することができます。新しい証明書が利用可能になれば、再度、時間無効を無視することができます。

注意：証明書チェック中に発生したエラーを無視することは、常にセキュリティの低下を意味します。

- 証明書の失効を無視

  証明書が、ログオン時に評価される証明書失効リストに掲載されている場合、その証明書は実際にはログオンに使用されない可能性があります。ただし、このオプションが選択されていても、ユーザーは暗号化プロファイルにアクセスし続けることができます。

- 時間無効を無視

  証明書の有効期限が切れていても、このオプションを選択すると、ユーザーは暗号化プロファイルに引き続きアクセスできます。

- 不正な証明書チェーンを無視

  発行者の証明書のパブリックパートがクライアントマシンで利用できなかったり、間違った証明書ストアに保存されていたりしても、ユーザーは暗号化プロファイルにアクセスし続けることができます。

- 不明な失効を無視

  一部のベンダーの PKI が証明書の失効理由を CRL に書き込む場合、一般的な標準に準拠していません。失効理由が不明な場合、通常は証明書を使用できません。ただし、このオプションを選択すると、ユーザーは暗号化プロファイルに引き続きアクセスできます。

注意：ユーザー証明書をチェックする際に見つかったエラーを無視することは、通常、会社のセキュリティポリシーを損なうことになりますのでご注意ください。u.trust LAN Crypt

クライアントは、RFC5280 に従って、不明な失効ステータスを認識しません。そのため、証明書を失効させる際には別の理由を付けてください。

これらの設定は、[サーバー設定]で定義することもできます。証明書は、セキュリティオフィサーが u.trust LAN Crypt 管理コンソールコンソールにログオンした時と、追加認証が行われた時の両方で検証されます。

4.1.3 すべての環境変数の解決

u.trust LAN Crypt はパスの環境変数 %USERNAME% を解決します。

ここでは、他の環境変数をパスで解決するかどうかを指定できます。

しかし、パスに他の環境変数を使用すると、ユーザーがそれを変更できる場合に問題が発生する可能性があります。その結果、暗号化プロファイルでパスデータが正しく機能しなくなる可能性があります。さらに、環境変数は Windows のバージョンによって異なるパスに影響する可能性があります。

4.1.4 有効なメニュー項目

ここでは、u.trust LAN Crypt のユーザーメニューで表示されるメニューオプションをクライアントコンピュータで指定できます。デフォルトでは、すべてのメニューオプションが表示されます。ここでメニューオプションを抑止すると、そのメニューオプションはクライアントコンピュータに表示されません。つまり、この機能はこのクライアントでも使用できません。これにより、たとえば、クライアントコンピュータで復号化をオフにする （解除する）ことを防ぐことができます。

4.1.5 デフォルトの無視ルール

u.trust LAN Crypt ドライバーはワークステーションの起動時に常にロードされるため、ユーザー固有の暗号化プロファイルがまだロードされていなくても、すべてのファイルが暗号化されているかどうか、適切なアクセス権を持っているかどうかが既にチェックされています。このため、この段階ではパフォーマンスが低下する可能性があります。

ただし、u.trust LAN Crypt の設定でマシン固有の設定を行えば、ユーザーの暗号化プロファイルが読み込まれるまで、u.trust LAN Crypt ドライバーが特定のドライブやフォルダを無視するように設定することができます。

クライアント設定]の[既定の無視ルール]をダブルクリックすると、u.trust LAN Crypt のドライバーが無視するディレクトリを指定するダイアログが開きます（例：c:„.*;d:„.*）。

複数のパスを入力する場合は、セミコロンで区切ってください。

ただし、このルールを使用する場合は、ユーザーの暗号化プロファイルがロードされるまで、u.trust LAN Crypt の特定のアクセスチェックが実行されないことを考慮する必要があります。

例

デフォルト無視ルールに"c:„.*;d:„.*"と入力すると、ユーザーの暗号化プロファイルがロードされるまで、ドライバーは C ドライブと D ドライブ上のすべてのフォルダを無視します。

ターミナルサーバーで u.trust LAN Crypt を使用している場合でも、デフォルトの無視ルール設定を使用することでパフォーマンスを高速化できます。例えば、複数のユーザーが同じターミナルサーバーで作業しているが、そのうちの一人だけが u.trust LAN Crypt を使用している場合、他のユーザーのセッションをすべて無視するようにドライバーに指示することができます。これらのユーザーには暗号化プロファイルがロードされていないため、デフォルトの無視ルールのみが適用されます。

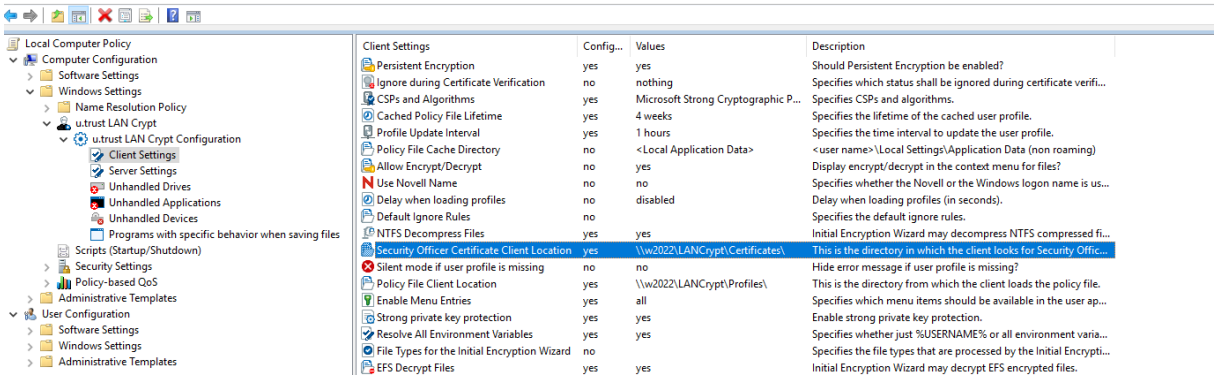
注意：ここで定義した項目には、すべてのサブフォルダも含まれることに注意：してください。

注意：u.trust LAN Crypt の新規インストール（アップデートではない）では、デフォルトの無視ルールが "*"で定義されています。その結果、ユーザーのプロファイルがロードされるまで、u.trust LAN Crypt の特定のアクセス保護はすべてのパスとファイルに対して無効となります。ユーザーは、この期間中またはプロファイルをアンロードしたときに、暗号化されたファイルを削除することができます。これは、保存されているファイルのキーを持っていない場合でも同様です。

デフォルト無視ルール（例："C:¸Program Files*.*"）にパスを定義すれば、これを変更することができます。

4.1.6 セキュリティ責任者証明書依頼者の所在地

保存場所を指定するには、クライアント設定を選択し、右側のコンソールペインでセキュリティオフィサー証明書クライアントの場所をダブルクリックします。



パスを指定すると、u.trust LAN Crypt は、関連するユーザーポリシーファイルの証明書が存在しない場合、自動的にこのディレクトリからセキュリティオフィサーの証明書をインポートしようとします。その結果、指定したディレクトリからすべての*.cer ファイルをインポートします。

4.1.7 キーファイルクライアントの場所

保存場所を指定するには、[クライアント設定]を選択し、右側のコンソールペインで [キーファイルクライアントの場所]をダブルクリックします。

パスを指定すると、u.trust LAN Crypt は、ポリシーファイルの秘密鍵が存在しない場合、自動的にそのユーザーの*.p12 キーファイルのインポートを試みます。このファイルは logonname.p12 という名前でなければなりません。

つまり、システム管理者がパスを指定するまで、セキュリティオフィサー証明書のパブリック部分またはユーザー証明書は自動的にロードされません。

u.trust LAN Crypt 管理コンソールは、ユーザー用の*.p12 ファイルとセキュリティオフィサー証明書のパブリック部分の両方を同じフォルダに保存します。しかし、クライアントから見ると、これらのパスは別々に設定できるので、必要に応じてこれらの機能のどちらかを無効にすることができます。にもかかわらず、これらのパスは通常同じです。セキュリティオフィサー証明書とユーザー証明書を異なるフォルダから自動的に読み込む場合は、該当するフォルダに手動でコピーする必要があります。

4.1.8 ポリシーファイルクライアントの場所

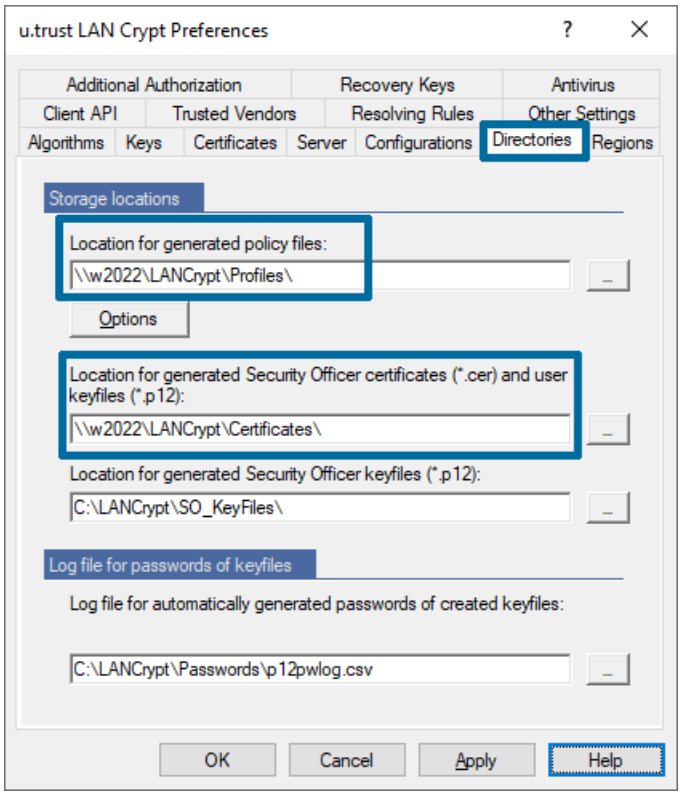
保存場所を指定するには、[クライアント設定]を選択し、右側のコンソールペインで[ポリシーファイルクライアントの場所]をダブルクリックします。

ユーザー固有のポリシーファイルの場所のパスを入力します。クライアントが自分のポリシー ファイル(たとえば、共有ネットワークドライブ)にアクセスできるようにするには、クライアントの視点からパスを入力する必要があります。

これは通常、u.trust LAN Crypt 管理コンソールコンソールを介してセキュリティオフィサーによって生成されたフォルダです。この時点ではこれらのファイルにディスクドライブは関連付けられていないため、UNC (Universal Naming Convention) の大文字と小文字の規則に従う必要があります。

この設定では、%LOGONSERVER%環境変数を使用することができます（負荷分散などのため）。

セキュリティオフィサーの証明書、キーファイル、およびポリシーファイルのグループポリシーに入力されたパスは、u.trust LAN Crypt 管理コンソールの[中央設定]ノード、[ディレクトリ]タブで定義されたパスと一致する必要があります。



4.1.9 ポリシーファイルキャッシュディレクトリ

キャッシュの保存場所を指定するには、[クライアント設定]を選択し、右側のコンソールペインで［ポリシーファイルキャッシュディレクトリ]をダブルクリックします。

ポリシーファイルのローカルコピーは、このディレクトリに保存されます。このコピーは通常、ネットワーク　ディレクトリから読み込まれます。ユーザーは、このローカルディレクトリにデータを書き込む権限を持っている必要があります。これにより、ネットワークに接続されていない場合でも、ユーザーの暗号化プロファイルが利用できることが保証されます。

リストに表示されている保存場所のいずれかを使用するか、<other>を選択して入力フィールドに別の保存場所を入力します。

保存場所を手動で指定する場合は、このフォルダがクライアントコンピュータにも存在することを確認する必要があります。

注意：u.trust　LAN　Crypt 環境からユーザーを削除する場合、ローカルコピーはコンピュータに保存されたままであることを考慮する必要があります。この場合、ユーザーはその中に含まれる権限でデータにアクセスすることができます。

これを防ぐには、このユーザー用に空のポリシーファイルを作成する必要があります。これを行うには、ポリシーファイルをクリアし、すべてのグループからユーザーを削除します(プロフィールのクリアを参照してください)。

4.1.10 プロファイル読み込み時の遅延

ここでは、ユーザープロファイルが読み込まれるまでの時間（秒）を指定できます。この遅延は、例えばトークン上の証明書を使用する場合に重要です。プロファイルのロードに遅延があるため、証明書が必要なときにトークンにアクセスできます。一般的な値は 20 秒です。

4.1.11 初回暗号化ウィザードのファイルタイプ

ここで特定のファイル　タイプを定義すると、指定したタイプのファイルのみが初回暗号化ウィザードで処理されます。ユーザーは、初回暗号化ウィザードでこの設定を変更できません。

この設定は、暗号化ルールが存在するファイルにのみ影響します。

フォルダの中に、ここで指定したファイルタイプの他のファイルが含まれている場合、それらは最初の暗号化には含まれません。暗号化されるのは、ユーザーがそれらを再度開いて保存するときだけです。

初回暗号化ウィザードでユーザー自身にこの設定を定義させる場合は、この設定を[未構成]のままにしてください。

ここでファイルの種類を指定し、後でユーザーに選択させるつもりであれば、設定をもう一度未設定に戻してください。

注意：この設定は、初回暗号化ウィザードにのみ適用されます。エクスプローラの拡張機能プロファイルに従って暗号化を使用して暗号化を開始した場合、この設定は何の効果も持ちません。

ファイルタイプをセミコロンで区切ったリストで指定します。

例：docx;xlsx;pdf;txt

4.1.12 キャッシュされたポリシーファイルの寿命

u.trust LAN Crypt の標準動作

ユーザーが Windows にログオンすると、まずキャッシュされたプロファイルが読み込まれます。次に u.trust LAN Crypt は、指定されたポリシーファイルの場所（ネットワークドライブ）への接続を確立することで、新しいポリシーファイルがユーザーに利用可能かどうかを確認します。新しいポリシーファイルが見つかった場合、キャッシュされたユーザープロファイルが更新されます。

この方法は、u.trust LAN Crypt がポリシーファイルの新しいバージョンが存在するかどうかをチェックしている間、ユーザーが暗号化されたファイルの操作を開始できるという利点があります。

ネットワークドライブにアクセスできない場合、ユーザーは更新できるまでキャッシュされたユーザープロファイルで作業します。

このオプションを[設定しない]に設定すると、u.trust LAN Crypt の動作は前述のようになります。

この設定を使用すると、標準の動作を変更できます。

注意：オプションを選択し、コンテキストメニュー（右クリック）で削除をクリックすると、設定なしに設定できます。設定済み列には、該当するオプションの他に［いいえ］が表示されます。

ここでは、キャッシュされたポリシーがクライアントコンピュータで有効な期間を指定できます。

ここで定義された期間内であれば、ポリシーファイルはクライアント上で有効であり、ポリシー共有上のファイルの場所への接続がない場合でも、ユーザーは暗号化されたデータにアクセスすることができます。

ポリシー ファイルがキャッシュされ、有効である期間は、日または週単位で定義できます。

指定した時間が経過すると、u.trust LAN Crypt はポリシーファイルをネットワークドライブからロードして再度更新しようとします。これが不可能な場合、ポリシーファイルはアンロードされます。ユーザーは暗号化されたデータにアクセスできなくなります。ポリシーファイルは、有効なポリシー ファイルが利用可能な場合にのみ更新され、再度ロードされます （たとえば、ポリシー ファイルのクライアントロケーションへの接続による次のログオン時など)。ユーザーは再び暗号化されたデータにアクセスできます。キャッシュ保存期間のカウンタはリセットされます。

キャッシュの保存期間を指定することで、クライアント コンピュータに定期的に最新のポリシー ファイルを提供し、ユーザーが常に最新のポリシーを使用できるようにすることができます。一方、このオプションを[設定しない]に設定すると、ユーザーはポリシーファイルのキャッシュバージョンを無制限に使用し続けることができるため、ユーザーが同じポリシーファイルを無制限に使用することを防ぐことができます。

以下の場合、キャッシュの保存許可期間のカウンタはリセットされます。

- ポリシーファイルの保存場所にアクセス可能で、有効なポリシーファイルがクライアントに転送された（ユーザーのログオン時または指定された更新間隔によってトリガーされたなど）が、ポリシーファイルは既存のものと比較して新しいものではありません。
- 新しいポリシーファイルが利用可能で、正常に読み込まれました。

以下の場合、キャッシュの保存許可期間のカウンタはリセットされません。

- クライアントコンピュータが新しいポリシーファイルを受信しようとします。しかし、ポリシーファイルの保存場所にアクセスできません。
- 新しいポリシーファイルが転送されました。しかし、エラーにより読み込めませんでした。
- 新しいポリシーファイルが利用可能です。しかし、それには新しい証明書が必要です。ユーザーはこの証明書を持っていないか、読み込むことができません。

ポリシーファイルの更新に失敗した場合、キャッシュされたポリシーファイルの有効期限がクライアントコンピュータのバルーンツールチップに表示されます。ユーザーは、u.trust LAN Crypt トレイアイコンから手動更新を開始できます。ユーザープロファイルの更新間隔設定に従って、自動更新も実行されます。

ポリシーファイルはキャッシュされません

このオプションを"0"に設定すると、ポリシー ファイルはキャッシュされません。これは、ポリシーファイルのファイルの場所にアクセス可能な場合、ログオン時にユーザーがユーザープロファイルを受け取ることを意味します。アクセスできない場合、またはプロファイルの読み込み時にエラーが発生した場合、ユーザーは暗号化されたファイルにアクセスできません。

4.1.13 NTFS 解凍ファイル

この設定により、初回暗号化ウィザードで NTFS 圧縮ファイルを処理できるようになります。NTFS 解凍ファイルオプションを［はい］に設定すると、ウィザードは NTFS 圧縮ファイルを解凍し、該当する場合は暗号化します。

NTFS ファイル解凍をオプションをいいえに設定すると、初回暗号化ウィザードは NTFS 圧縮ファイルを無視します。これらのファイルは、暗号化ルールが指定されていても暗号化されません。

このオプションを設定した後、ユーザーは初回暗号化ウィザードでこのオプションを変更することはできません。初回暗号化ウィザードでこのオプションを自分で設定できるのは、ここで未設定に設定されている場合だけです。

注意：u.trust LAN Crypt で暗号化されたファイルを NTFS で圧縮すると、そのファイルは u.trust LAN Crypt で復号化できなくなります。このようなファイルを復号化しようとするとエラーメッセージが表示されます。NTFS で圧縮するファイルは、u.trust LAN Crypt で暗号化されていない必要があります。

4.1.14 EFS ファイルの復号化

この設定により、初回暗号化ウィザードで EFS 暗号化ファイルを処理できるようになります。EFS 復号ファイルオプションを［はい］に設定すると、ウィザードは EFS 暗号化ファイルを復号化し、u.trust LAN Crypt 暗号化ルールが適用される場合に再度暗号化します。

EFS DeCrypt Files オプションをいいえに設定すると、初回暗号化ウィザードは EFS 暗号化ファイルを無視します。これらのファイルは、暗号化ルールが指定されていても、u.trust LAN Crypt によって再暗号化されません。

このオプションを設定した後、ユーザーは初回暗号化ウィザードでこのオプションを変更することはできません。初回暗号化ウィザードでこのオプションを自分で設定できるのは、ここで未設定に設定されている場合だけです。

注意：オプションを選択し、そのコンテキストメニュー（右クリック）で［削除］をクリックすると、オプションを［構成なし］に設定できます。設定済み列には、該当するオプションの他に［いいえ］が表示されます。

4.1.15 プロファイル更新間隔

この設定は、u.trust LAN Crypt が新しいポリシーファイルをチェックし、必要に応じて更新する頻度を定義します。

u.trust LAN Crypt は、ポリシーファイルが保存されているネットワークドライブにアクセスする必要があります。u.trust LAN Crypt は、ネットワークドライブに新しいバージョンのポリシーファイルが存在するかどうかを確認し、必要に応じてクライアントコンピュータのポリシーファイルを更新します。

u.trust LAN Crypt は、ユーザープロファイルを正常に読み込むために必要なすべての手順（必要に応じて、新しい証明書の検索、新しい証明書の検証など）を自動的に実行します。古いプロファイルは新しいプロファイルに置き換えられ、新しいプロファイルはプロセス中にエラーが発生しなかった場合にのみロードされます。その後、キャッシュ保存期間のカウンタがリセットされます。ポリシーファイルが同じ場合、カウンタもリセットされます。

更新間隔は、分、時間、日、週で指定できます。

注意：u.trust LAN Crypt では、15 分未満の更新間隔は許可されません。このオプションが設定されていない場合、ポリシーファイルは自動的に更新されません。

4.1.16 ユーザープロファイルがない場合のサイレントモード

u.trustLAN Crypt は、デフォルト設定の場合、ユーザープロファイルが見つからないとエラーメッセージを表示します。

ここでは、ユーザープロファイルが見つからない場合にこのエラーメッセージを表示しないように指定できます。

エラーメッセージを隠すを[はい]に設定すると、エラーメッセージは表示されません。

注意：この設定は、すべてのユーザーが u.trust LAN Crypt を使用する必要がないターミナルサーバー環境で特に役立ちます。

4.1.17 永続的暗号化

ファイルは通常、暗号化ルールが適用されている間だけ暗号化されたままになります。たとえば、暗号化されたファイルを暗号化ルールが定義されていないフォルダにコピーした場合、そのファイルはコピー先のフォルダで復号化されます。永続的な暗号化を[はい]に設定すると、ファイルを移動またはコピーしても暗号化された状態を維持できます。

この機能を無効にするには、[永続的暗号化]をダブルクリックし、[永続的暗号化の有効化]のリストフィールドで[いいえ]を選択します。

4.1.18 強力な秘密鍵保護

ここでは、u.trust LAN Crypt で秘密鍵が使用されるたびに、ユーザーに認証のプロンプトが表示されるように指定できます。この設定を有効にすると、セキュリティオフィサーにも適用されます（LAN Crypt 管理コンソール設定の強力な秘密鍵保護を有効にするを参照）。

注意：このポリシーは、以前にインポートした証明書や手動でインポートした証明書には適用されません。この設定を有効にすると、u.trust LAN Crypt 経由でインポートされた証明書にのみ適用されます。

4.1.19 CSP とアルゴリズム

ここでは、CSP とハッシュアルゴリズムを指定できます。

秘密鍵をインポートする CSP を選択する必要があります。

注意：この設定の変更は、u.trust LAN Crypt クライアントと u.trust LAN Crypt 管理コンソールコンソールの両方に影響します。例えば、CSP の設定が Microsoft Base Smart Card Crypto Provider の場合、両方のケースでスマートカードによるログインが必要になります。

4.1.20 平文ファイルの防止

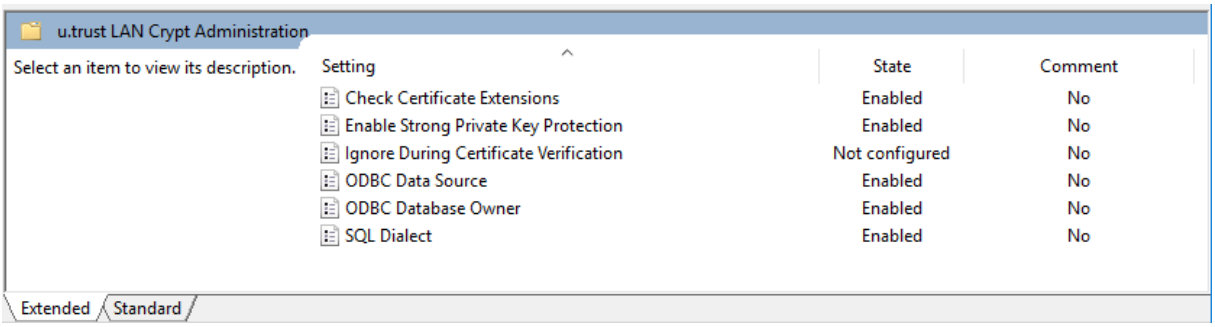
この設定により、u.trust LAN Crypt ユーザープロファイルがまだロードされていない場合、またはユーザーがプロファイルを持っていない場合に、定義されたネットワークパス、マップされたドライブ、またはローカルドライブに平文ファイルが作成されないようにすることができます。ネットワークパスまたはドライブ文字をターゲットとして指定できます。

例

¥¥Server1
¥¥Server2
X:
Y:
Z:

4.2 LAN Crypt の管理設定

注意：これらの設定はサーバーに対して行う必要があります。これらの設定は、1 つの例外（強力な秘密鍵保護を有効にする）を除いて、クライアントコンピュータには影響しません。



ただし、標準設定を使用しない場合は、管理機能を初めて起動する前に、これらのサーバー設定を行うことが重要です。

4.2.1 強力な秘密鍵保護の有効化

ここでは、u.trust LAN Crypt で秘密鍵が使用されるたびに、(マスター)セキュリティオフィサーに認証のプロンプトが表示されるように指定できます。この設定を有効にすると、クライアントにも適用されます（クライアント設定の強力な秘密鍵保護ページ 166).

注意： u.trust LAN Crypt ScriptingAPI を使用するコンピュータでは、グループ ポリシーでこの設定を無効にする必要があります。そうしないと、ス Crypt を実行するときにパスワード照会で常にユーザーの操作が必要になります。

4.2.2 SQL 方言

ここでは、ODBC データソースとの通信に使用する SQL 方言を指定します。これはシステム構成に使用されます。

- MS SQL サーバー
- Oracle
- スタンダード SQL

4.2.3 ODBC データベース所有者

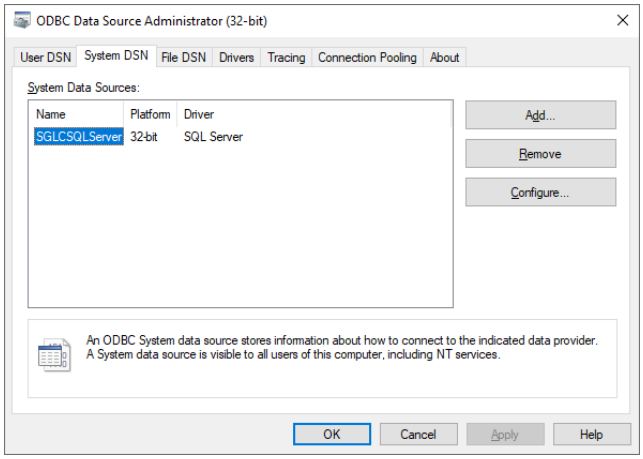
ここでは、使用しているデータベースが正しくアドレス指定できるように、データベース所有者を入力します。

MS SQL Server の場合、ジェネレータのデフォルト値「dbo」は変更しないでください。これは、Oracle データベースを使用している場合にのみ変更する必要があります。

注意：Oracle データベースを使用している場合は、ここにデータベース所有者を大文字で入力する必要があります。これは、データベーステーブルの作成時に使用された名前と同じでなければなりません。

4.2.4 ODBC データソース

ここでは、ODBC データソースへのアクセスに使用する名前を入力します。



u.trust LAN Crypt は、ODBC データソースのデフォルト名として SGLCSQL Server を使用します。別の名前を使用したい場合は、u.trust LAN Crypt 管理コンソールを初めて実行する前にここに入力してください。

注意： ODBC データソースの名前は大文字と小文字を区別します。ここに入力する名前は、ODBC データソースの作成時に入力した名前と同じでなければなりません。u.trust LAN Crypt のバージョン 4.0.3 までは、32 ビットの ODBC データソースしか使用できません。

4.2.5 証明書検証中の無視

ここでは、セキュリティオフィサーがログオンしたとき、または管理コンソールで証明書が割り当てられたときに、どの証明書ステータスを無視するかを指定できます。

4.2.6 ハッシュアルゴリズム

使用するハッシュアルゴリズムは、この時点でのみ表示されます。クライアント設定で設定する必要があります。

4.2.7 証明書拡張子のチェック

デフォルトでは、u.trust LAN Crypt が証明書ストアから証明書を割り当てる際、キー使用プロパティにキー暗号化やデータ暗号化の値が設定されている証明書のみを使用します。

しかし、証明書の拡張をチェックでは、このチェックを行わないように指定することができ、u.trust LAN Crypt は他のプロパティを持つ証明書を使用することができます。

証明書拡張子のチェック：他のプロパティを持つ証明書の使用を許可しません。

注意：ただし、これらのタイプの証明書が u.trust LAN Crypt で使用できるかどうかは、使用している CSP によって異なります。このチェックをオフにする場合は、使用したいタイプの証明書が u.trust LAN Crypt で実際に使用できることを確認してください。

4.3 処理しないドライブ、アプリケーション、デバイス

u.trust LAN Crypt では、ドライブ、アプリケーション、デバイス（ネットワークファイルシステム）を u.trust LAN Crypt のフィルタドライバーで無視し、透過暗号化/復号化から除外するように指定できます。

バックアッププログラムは、処理しない可能性のあるアプリケーションの一例です。バックアップデータを暗号化したままにしたい場合は、このアプリケーションを暗号化/復号化プロセスから除外することができます。その場合、バックアップ時にデータは暗号化されたままになります。

ディスクドライブ全体を除外することで、パフォーマンスを大幅に向上させることができます。例えば、"E:"ドライブ上で暗号化を実行しない場合、単に "無視ドライブ" として定義することができます。あるいは、"暗号化ルールの無視"オプションを使用して、このディスクドライブのルールを定義することもできます。

ドライブを「処理しない」としてマークすると、フィルタドライバーはプロファイルを処理しないため、ファイル操作がより迅速に実行されます。

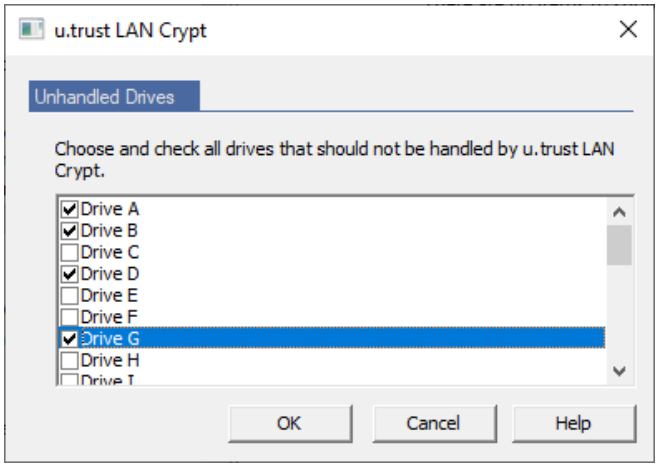
これらの設定は LAN Crypt 設定ノードにあります。

注意：これらはマシン固有の設定であるため、クライアントコンピュータを再起動するまで有効になりません。

4.3.1 処理しないドライブの追加

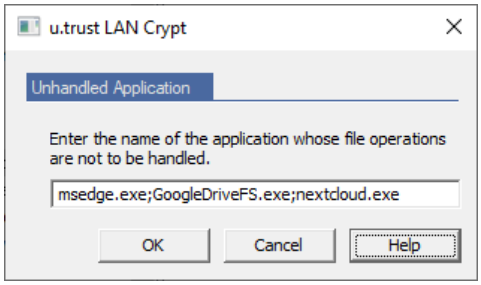
処理しないドライブを選択し、コンテキストメニューの［処理しないドライブの追加］をクリックします。

u.trust LAN Crypt に無視させたいドライブを選択し、[OK]をクリックします。



4.3.2 処理しないアプリケーションの追加

クライアント設定の[処理対象外アプリケーション］ をダブルクリックすると、処理対象 外アプリケーションを指定するダイアログが開きます。



典型的な用途

- バックアッププログラムは、常に暗号化されたデータを読み込んで保存するように、「処理しない」として定義することができます。
- また、暗号化されたファイルがそのようなプログラムで暗号化されていないアーカイブに追加されるべきではない場合、圧縮プログラムは未処理として定義することができます。
- u.trust LAN Crypt と同時に使用するとエラーが発生する可能性があるが、暗号化を必要としないアプリケーションは、通常、暗号化プロセスから除外することができます。

処理しないアプリケーションを指定するには、その実行ファイル名全体を入力する必要があります。

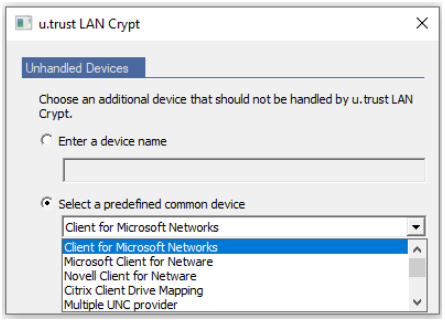
アプリケーションの名前とパス（必要な場合）を入力します。

必要に応じて、[子プロセスを含める] オプションを有効にし、[OK]をクリックします。

注意：u.trust LAN Crypt はデフォルトで特定のアプリケーションを未処理のアプリケーションとして扱います。アプリケーションを「処理しないアプリケーション」として指定する前に、u.trust LAN Crypt クライアントのユーザーメニューの"クライアントステータス"（処理しないタブの処理しないアプリケーションセクション）で、そのアプリケーションがデフォルトで定義されているかどうかを確認してください。

4.3.3 処理しないデバイスの追加

クライアント設定の［処理しないデバイス］をダブルクリックして、[処理しないデバイス]を指定するダイアログを開きます。



処理しないデバイスダイアログには、u.trust LAN Crypt の暗号化処理から除外できるネットワークファイルシステムや特定の種類のドライブが表示されます。技術的な理由により、ここで単一のネットワークドライブを除外することはできません。除外できるのはネットワークファイルシステム全体のみです。ここに表示される定義済みのデバイスは次のとおりです：

- Microsoft ネットワーク用クライアント
- Netware 用 Microsoft クライアント
- Netware 用ノベルクライアント
- Citrix クライアントのドライブマッピング
- 複数の UNC プロバイダー
- ブートボリューム
- リムーバブル
- 光学機器
- ローカルボリューム
- ネットワーク共有

注意：セキュリティオフィサーは、この目的のために暗号化ルールを作成することで、個別の（ネットワーク）ディスクドライブを暗号化プロセスから除外することができます。

これらの標準的なネットワークファイルシステムに加え、デバイス名を入力して特定のデバイスを除外することもできます。これは、サードパーティ製のファイルシステムを使用していて、暗号化処理から除外したい場合に便利です。

デバイス名を入力し、[OK]をクリックします。

管理者は、OSR のデバイスツリーなどのツールを使って、システム上で現在使用されているファイルシステムの名前を表示することができます。

5 付録

5.1 ロギング

....セキュリティオフィサー_Utimaco-NI のパーミッションが追加されました。許可されました：0x86000000 - Denied: 0x0)...

Allowed:と Denied:の後の値は、どの権限が実際に変更されたかを示しています。

以下の表を参考に値を解釈してください。

許可：0x86000000

セキュリティオフィサーの ACL：読み取り	0x80000000
セキュリティオフィサーの ACL 証明書の変更	0x02000000
セキュリティオフィサーの ACL リージョンの変更	0x04000000
許可	0x86000000

セキュリティオフィサーのグローバル権限

アクセス許可	値
セキュリティーオフィサーの作成	0x000001
プロファイルの作成	0x000002
キーの作成	0x000004
キーのコピー	0x000008
キーの削除	0x000010
キーの読み取り	0x000020
証明書の作成	0x000040
証明書の割り当て	0x000080
グループの管理	0x000200
データベースへのログイン	0x000400
オペレーションの承認	0x000800
ユーザーの管理	0x001000
ルールの作成	0x002000

アクセス許可	値
グローバル権限の変更	0x004000
ACL の変更	0x008000
特定のキーの使用	0x010000
設定の変更	0x020000
ロギングエントリーの読み取り	0x040000
ログの管理	0x080000
ディレクトリオブジェクトのインポート	0x100000

グループの ACL

キーの作成	0x00000001
キーのコピー	0x00000002
キーの削除	0x00000004
ルールの作成	0x00000008
証明書の割り当て	0x00000010
ユーザーの追加	0x00000020
ユーザーの削除	0x00000040
グループの追加	0x00000080
サブグループの削除	0x00000100
グループの移動	0x00000200
プロパティの変更	0x00000400
グループの削除	0x00000800
プロファイルの作成	0x00001000
ACL の変更	0x00002000
読み取り	0x00004000
可視	0x00008000

セキュリティオフィサーの ACL

アクセス許可	値
名前の変更	0x01000000
証明書の変更	0x02000000
リージョンの変更	0x04000000
設定の割り当て	0x08000000
セキュリティオフィサーの削除	0x10000000
グローバル権限の変更	0x20000000
ACL の変更	0x40000000
読み取り	0x80000000

5.2 権限

5.2.1 グローバル権限

アクセス許可	説明
セキュリティオフィサーの作成	セキュリティオフィサーは、さらにセキュリティオフィサーを作成するグローバル権限を持っています。
プロファイルの作成	セキュリティオフィサーは、プロファイル リゾルバを実行し、個々のユーザーのポリシーファイルを生成するグローバル権限を持っています。このグローバル権限は、セキュリティオフィサー に特定のグループのプロファイルを作成する権限を設定するための前提条件です。プロファイルの作成]により、セキュリティオフィサーは、セキュリティオフィサーがユーザーの親グループに対して[プロファイルの作成]権限を持っているユーザーのプロファイルを作成できます。 この権限は、キーに値を割り当てるための必須条件です。キーの作成権限を持つセキュリティオフィサーは、値のないキーのみを生成できます。
プロファイルの作成 全員	この権限には、プロフィールの作成権限が設定されている必要があります。このグローバルパーミッションは、特定のグループに［プロファイルを作成］パーミッションを設定するための前提条件です。すべてのメンバーのプロファイルの作成では、セキュリティオフィサーがユーザーの親グループで［プロファイルの作成］権限、またはユーザーが所属するグループの 1 つで［すべてのメンバーのプロファイルの作成］権限を持っている場合、セキュリティオフィサーはすべてのユーザーのプロファイルを作成できます。 注意： グローバル権限プロフィールの作成は、すべてのメンバーのプロフィールの作成の前提条件であるため、以下が適用されます。プロファイルの作成権限を非アクティブにすると、[すべてのメンバーのプロファイルの作成］権限も自動的に非アクティブになります。すべてのメンバーにプロファイルを作成権限をアクティブにすると、[プロファイルを作成]権限も自動的にアクティブになります。
キー作成	セキュリティオフィサーは、個々のグループでキーを生成できます。キーの作成権限を持つセキュリティオフィサーは、値のないキーのみを生成できます。管理コンソールでは、値のないキーをグループとユーザーに割り当てることができます。値自体は、ポリシーファイルが生成されるときに生成されます。値のあるキーを手動で生成するには、セキュリティ管理者にプロファイルの作成権限が必要です。

アクセス許可	説明
キーのコピー	セキュリティオフィサーはキーのコピーを許可されています。
キーの削除	セキュリティオフィサーは、個々のグループからキーを削除することができます。
キーの読み取り	セキュリティオフィサーは、グループの個別キーのデータを見ることができます。
証明書の作成	セキュリティオフィサーは、ユーザーの証明書を生成できます。
証明書の割り当て	セキュリティ管理者は、ユーザーに証明書を割り当てることができます。セキュリティオフィサーは、証明書を割り当てるためのウィザードを実行できます。このグローバル権限は、セキュリティオフィサーに特定のグループに証明書を割り当てる権限を設定するための前提条件です。証明書の割り当て］を使用すると、セキュリティオフィサーは、セキュリティオフィサーがユーザーの親グループに対して［証明書の割り当て］権限を持っているユーザーに証明書を割り当てることができます。
証明書の割り当て 全員	この権限には、［証明書の割り当て］権限が設定されている必要があります。このグローバル権限は、特定のグループに対して［すべてのメンバーに証明書を割り当てる］権限を設定するための前提条件です。すべてのメンバーに証明書を割り当てる］を使用すると、セキュリティオフィサーは、ユーザーの親グループで ［証明書を割り当てる］権限を持つすべてのユーザー、またはユーザーが所属するグループの 1 つで［すべてのメンバーに証明書を割り当てる］権限を持つすべてのユーザーに証明書を割り当てることができます。 注意：グローバル権限証明書の割り当ては、すべてのメンバーに証明書を割り当てる前提条件であるため、以下が適用されます：証明書の割り当て］権限を非アクティブにすると、［すべてのメンバーに証明書を割り当てる］ 権限も自動的に非アクティブになります。すべてのメンバーに証明書を割り当てる］ 権限をアクティブにすると、［証明書を割り当てる］権限も自動的にアクティブになります。
グループの管理	セキュリティオフィサーは、グループに変更を加えることができます。サブグループの追加、グループの移動、グループの同期、グループの削除。

アクセス許可	説明
データベースへのログイン	セキュリティオフィサーは u.trust LAN Crypt データベースにログオンできます。この権限のデフォルト設定はアクティブです。 この権限があれば、セキュリティオフィサーは、（例えば、スタッフが退社した場合など）あまり労力をかけずに、簡単にデータベー スを変更することができます。この権限は、他の誰かが自分の行動を承認した場合にのみ行動を許可される人々には付与されません。このため、これらの人は確認が必要なアクションしか許可できず、u.trust LAN Crypt に変更を加えることはできません。
オペレーションの承認	セキュリティオフィサーは、確認が必要な行動に参加することができます。
ユーザーの管理	セキュリティオフィサーは、ユーザーをグループに追加したり、グループから削除したり、グループを同期したりすることができます。
ユーザーのコピー	セキュリティオフィサーは、グループにユーザーを追加（コピー）することができます。このグローバル権限は、セキュリティオフィサーが特定のグループにユーザーをコピーパーミッションを設定するための前提条件です。ユーザーをグループに追加するには、セキュリティオフィサーはユーザーの親グループにユーザーをコピー権限を持っている必要があります。
ルールの作成	セキュリティオフィサーは、ユーザーの暗号化ルールを生成することができます。
グローバル権限の変更	セキュリティオフィサーは、別のセキュリティオフィサーに付与されたグローバル権限を変更できます。
ACL の変更	セキュリティオフィサーはグループの ACL を変更することができます。
特定のキーの使用	セキュリティオフィサーは、暗号化ルールで特定のキーを使用したり、すべての u.trust LAN Crypt キーで特定のキーを表示することができます。
設定の変更	セキュリティオフィサーは設定（パス）を変更できます。このパーミッションは、ノードの中央設定に構成タブを表示するため、およびセキュリティオフィサーがデータベースにログオンしている場合にディレクトリタブで変更できるようにするために必要です。
ロギングエントリーの読み取り	セキュリティオフィサーは、ログに使用される設定とログに記録されたイベントを表示できます。
ログの管理	セキュリティオフィサーはログの設定を変更することができます。セキュリティオフィサーは、エントリーのア

	ーカイブ、削除、およびチェックを行うことができます。

アクセス許可	説明
ディレクトリオブジェクトのインポート	セキュリティオフィサーは、ディレクトリサービスからOU、グループ、ユーザーをインポートし、u.trust LAN Cryptデータベースに追加することができます。ディレクトリオブジェクトをインポートする前に、セキュリティオフィサーはグループの管理権限とユーザーの管理権限も必要です。これらはディレクトリオブジェクトのインポート権限を選択すると自動的に設定されます。 セキュリティオフィサーがこの権限を持っていない場合、（OU、グループ、ユーザーのインポートに使用される）［ディレクトリオブジェクト］ノードは管理コンソールに表示されません。

5.2.2 セキュリティオフィサーの設定変更権限

アクセス許可	説明
名前の変更	権限の所有者が割り当てられたセキュリティオフィサーの名前の変更を許可します。
証明書の変更	権限の所有者が割り当てられたセキュリティオフィサーの証明書の変更を許可します。
リージョンの変更	権限の所有者が割り当てられているセキュリティオフィサーのリージョンプレフィックスの変更を許可します。
設定の割り当て	権限の所有者が割り当てられているセキュリティオフィサーの設定の変更を許可します。
セキュリティオフィサーの削除	権限の所有者が割り当てられているセキュリティオフィサーを削除できるようにします。
グローバル権限の変更	権限の所有者が割り当てられているセキュリティオフィサーのグローバル権限の変更を許可します。
ACL の変更	権限の所有者が割り当てられているセキュリティオフィサーの ACL を変更できます。
読み取り	中央設定ノードで権限の所有者が割り当てられているセキュリティオフィサーを表示します。このセキュリティ

	オフィサーの処理を許可するすべての権限の前提条件です。このタイプの権限が選択されている場合、自動的に設定されます。

5.2.3 セキュリティオフィサーによるグループ処理権限

アクセス許可	説明
キーの作成	セキュリティオフィサーは、グループ内でキーを生成することができます。
キーのコピー	セキュリティオフィサーはキーのコピーを許可されています。
キーの削除	セキュリティオフィサーはキーの削除を許可されています。
ルールの作成	セキュリティオフィサーは、ユーザーのルールを作成することができます。
証明書の割り当て	セキュリティオフィサーは、ユーザーに証明書を割り当てることができます。 セキュリティオフィサーは、証明書の割り当てに使用するウィザードを実行できます。証明書の割り当てにより、セキュリティオフィサーは、グループが親グループでもあるグループ内のユーザーに証明書を割り当てることができます。
全メンバーに証明書を割り当て	この権限には、[証明書を割り当てる] 権限が設定されている必要があります。すべてのメンバーに証明書を割り当てる] を使用すると、セキュリティオフィサーはグループ内のすべてのユーザー(グループが親グループであるユーザー、およびグループのメンバーで別の親グループを持つユーザー)に証明書を割り当てることができます。 注意：すべてのメンバーへの証明書の割り当てを許可に設定すると、自動的に証明書の割り当てが許可に設定されます。証明書の割り当て]を[拒否]に設定すると、[すべてのメンバーへの証明書の割り当て]が自動的 [拒否]に設定されます。

ユーザーの追加	セキュリティオフィサーは、ユーザーを手動でグループに追加することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
ユーザーのコピー	セキュリティオフィサーは、このグループのユーザーを別のグループに追加する権限を持っています。これは、このグループが親オブジェクトでもあるメンバーにのみ許可されます。

アクセス許可	説明
ユーザーの削除	セキュリティオフィサーは、[グループのメンバーと証明書]スナップインを使用してユーザーを削除できます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
グループの追加	セキュリティオフィサーは、グループのコンテキストメニューを使用して新しいグループを追加することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
サブグループの削除	セキュリティオフィサーは、このグループのサブグループを削除することができます。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
グループの移動	セキュリティオフィサーは、管理部で手動で作成したグループを移動することができます（ドラッグ＆ドロップで）。インポートしたグループは移動できません。 この権限は、グループとユーザーをインポート/同期するための前提条件です。
プロパティの変更	セキュリティオフィサーはグループのプロパティを変更することができます。
グループの削除	セキュリティオフィサーはグループの削除が許可されています。これは、セキュリティオフィサーが上記のグループのサブグループの削除権限を削除していることを前提としています。

	この権限は、グループとユーザーをインポート/同期するための前提条件です。
プロファイルの作成	セキュリティオフィサーには、プロファイルリゾルバを実行し、選択したユーザーのポリシー ファイルを生成する権限があります。プロファイルの作成］ は、グループが親グループでもあるグループ内のユーザーのプロファイルを作成する権限です。

アクセス許可	説明
全メンバーのプロフィールの作成	この権限には、プロファイルの作成権限が設定されている必要があります。すべてのメンバーのプロファイルを作成］ を使用すると、セキュリティオフィサーはグループ内のすべてのユーザー（グループが親グループであるユーザーと、グループのメンバーで別の親グループを持つユーザー）のプロファイルを作成できます。 注意：すべてのメンバーのプロファイルの作成を許可に設定すると、自動的にプロファイルの作成が許可に設定されます。プロファイルの作成］を［拒否］に設定すると、自動的に［すべてのメンバーのプロファイルの作成］が［拒否］に設定されます。
ACL の変更	セキュリティオフィサーは、グループの ACL を変更することができます（別のセキュリティオフィサーを追加するなど）。
読み取り	セキュリティオフィサーにはこのグループの読み取り権限があり、スナップインの内容を確認できます。編集権限が付与されている場合は、自動的に設定されます。
可視	セキュリティオフィサーはグループを見ることができます。ベースノードに設定され、下位に継承されます。セキュリティオフィサーに対して拒否された場合、グループは非表示になります（Read 権限も拒否する必要があります）。

6 法的通知

Copyright © 2024 Utimaco IS GmbH, 2018 - 2023 conpal GmbH, 1996 - 2018 Sophos Limited and Sophos Group.無断複写転載を禁じます。

その他記載されている製品名および会社名は、各社の商標または登録商標です。

本書のいかなる部分の複製、検索システムへの保存、または送信も、電子的、機械的、複写、記録、またはその他の手段を問わず、ライセンス条項に従って文書を複製することができる有効なライセンスを取得しているか、または著作権所有者の書面による事前の許可を得ている場合を除き、禁止されています。

サードパーティサプライヤの著作権情報は、製品ディレクトリのサードパーティソフトウェアドキュメントに記載されています。

テクニカルサポート

u.trust LAN Crypt 製品のテクニカルサポートは、以下の方法で見つけることができます：

- https://support.utimaco.com、有効な保守契約を結んでいる登録顧客は、ダウンロード、ドキュメント、ナレッジアイテムにアクセスできます。

Windows 用のクライアント製品のドキュメントは、以下からダウンロードできます。

- https://help.lanCrypt.com/docs/windows/11_0_0/de/　ドイツ語
- https://help.lanCrypt.com/docs/windows/11_0_0/en/　英語
- https://help.lanCrypt.com/docs/windows/11_0_0/fr/　フランス語

macOS 用クライアント製品のドキュメントは以下からダウンロードできます。

- https://help.lanCrypt.com/docs/macOS/de/　ドイツ語
- https://help.lanCrypt.com/docs/macOS/en/　英語

iOS / iPadOS 用の製品ドキュメントは以下からダウンロードできます。

- https://help.lanCrypt.com/docs/ios/de/　ドイツ語
- https://help.lanCrypt.com/docs/ios/en/　英語

Android 用の製品ドキュメントは以下からダウンロードできます。

- https://help.lanCrypt.com/docs/android/de/　ドイツ語
- https://help.lanCrypt.com/docs/android/en/　英語

u.trust LAN Crypt 2Go の製品ドキュメントは、以下からダウンロードできます。

- https://help.lanCrypt.com/docs/2Go/de/　ドイツ語
- https://help.lanCrypt.com/docs/2Go/en/　英語

管理者用製品ドキュメントは以下からダウンロードできます。

- https://help.lanCrypt.com/docs/admin/11_0_0/de/　ドイツ語
- https://help.lanCrypt.com/docs/admin/11_0_0/en/　英語
- https://help.lanCrypt.com/docs/admin/11_0_0/fr/　フランス語

メンテナンスにご登録いただいているお客様は、下記までメールをお送りください。

support@utimaco.com

u.trust LAN Crypt ソフトウェアのバージョン番号、オペレーティングシステム、パッチレベル、エラーメッセージのテキストを含みます。