StorageTek™ Crypto Key Management System (KMS)

管理マニュアル

Part No: 316030101
Revision: A
Version: 2.0

Crypto Key Management System (KMS)

管理ガイド

Version 2.0

Sun Microsystems, Inc.
www.sun.com

Part No. 316030101
2008 年 4 月, Revision A

皆様からのフィードバックを歓迎いたします。次の Sun Learning Services Feedback System にご連絡ください。

SLSFS@Sun.com

または

Sun Learning Services
Sun Microsystems, Inc.
One StorageTek Drive
Louisville, CO 80028-3256
USA

可能であれば、マニュアル名、部品番号、版も記入してください。これによって、より早く 回答することができます。

原典: *Crypto Key Management System (KMS) Administration Guide Version 2.0*
Part No: 316195101
Revision A

Please
Recycle

通知

この製品に関する次の適合規制宣言および警告宣言を確認してください。

注意 – 機器損傷の可能性: 周辺機器を接続するケーブルは遮蔽して、接地する必要があります。ケーブルの取扱説明書を参照してください。遮蔽されていないケーブルおよび適切に接地していないケーブルを使用してこの機器を操作すると、ラジオやテレビの受信妨害が生じる可能性があります。

この機器に対して事前に StorageTek により明示的な承認を得ていない変更または改変を行なった場合の動作は保証されません。また、この機器に変更または改変を行うと、有害な妨害が生じる可能性があります。

米国 FCC の適合規制宣言

次の規制適合声明は、米連邦通信委員会 (FCC) 規則 47 CFR 15.105 に関連しています。

注 – This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his or her own expense.

CISPR 22 および EN55022 の警告

この製品は、クラス A 情報技術装置です。この製品を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるように要求されることがあります。

日本の適合規制宣言

次に示す日本語の適合規制宣言は、VCCI EMI 規制に関連するものです。

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

英語訳: This is a Class A product based on the Technical Requirement of the Voluntary Control Council for Interference by Information Technology (VCCI). In a domestic environment, this product may cause radio interference, in which case the user may be required to take corrective actions.

台湾の警告ラベル宣言

次の警告ラベル宣言は、台湾 R.O.C. の BSMI 規制に関連するものです。

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策

英語訳: This is a Class A product.In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate measures.

内部コードライセンス宣言

StorageTek の内部コードライセンス契約は、次のとおりです。

StorageTek の内部コードライセンス契約は、次のとおりです。

通知

内部コードライセンス

この機器を設置および操作する前に、この注意事項を注意深くお読みください。この通知は、エンドユーザーであるお客様 (個人または法人であるかを問わない) と、この機器の製造会社である Storage Technology Corporation (以下、「StorageTek」と表記) との間に締結される法的な契約書です。お客様は、パッケージを開封し、本契約書に記載されている機器のユニットを受け入れ使用することによって、本契約書の条項に拘束されることに同意したものとします。本契約書の条項に同意しない場合は、パッケージを開封せず、この機器を使用しないでください。お客様がお客様の会社にこの条項を順守させる全権限を有していない場合は、パッケージを開封せず、この機器を使用しないでください。ご不明な点は、認可された StorageTek 販売店か、またはこの機器を購入した小売店にお問い合わせください。この機器を StorageTek から直接購入した場合は、StorageTek の販売担当者にお問い合わせください。

1. **定義**: 用語の定義を次に示します。
   a. 「派生物」とは、1 つ以上の既存の作品に基づいた作品 (翻訳や編曲、または作品を改作、変換、または改変してできるその他の形態) のことです。編集による改訂、注釈、詳述、その他の改変によって構成された、全体として 1 つのオリジナルの著作品となる作品は派生物です。
   b. 「内部コード」とは、(i) 機器の不可欠な一部であり、(ii) 機器がそのデータの格納および取得の機能を実行するために必要とし、(iii) この機器のユーザーインタフェースで実行されるマイクロコードのことです。内部コードには、この機器に組み込まれていたり、この機器内部で実行されたり、あるいはこの機器に接続して実行または使用されたりする場合がある、ほかのマイクロコードやソフトウェア (データファイルを含む) は含まれません。このようなコードには保守コードが含まれますがこれに限定されません。
   c. 「保守コード」とは、この機器に組み込まれていたり、この機器内部で実行または使用されたり、あるいはこの機器に接続して実行または使用されたりする場合がある、マイクロコードやその他のソフトウェア (データファイルを含む) のことです。保守コードは、機器の故障を検出、記録、表示、または分析する場合に使用されます。
   d. 「マイクロコード」とは、機器に埋め込まているか、または機器にロードされて、この機器の外部ユーザーインタフェースで実行される命令セット (ソフトウェア) のことです。マイクロコードには内部コードと保守コードの両方があり、磁気媒体やその他の記憶媒体、集積回路、またはその他の媒体上にある場合があります。
2. 購入またはリース契約によりお客様が入手した機器は、StorageTek により、あるいは StorageTek のために他社で製造されたものであり、マイクロコードを含んでいます。この機器を受け入れて操作することにより、お客様は、StorageTek またはそのライセンサがすべてのマイクロコード、および機器の操作や保守サービスで実行または使用される可能性のあるすべてのコピーの所有権を保持していること、またマイクロコードが StorageTek またはそのライセンサの著作物であることを承諾したものとします。
3. StorageTek は、機器のエンドユーザーであるお客様に対して、内部コードの各コピー (あるいは StorageTek または認可された StorageTek 販売業者や小売業者により提供された代替品) を使用するための個人的で譲渡不可 (下記の譲渡条項で許可されている場合を除く) かつ非独占的なライセンスを許諾します。このライセンスにより、エンドユーザーであるお客様は、StorageTek (またはそのライセンサ) の公開された公的な仕様書に従って、データの格納および取得の機能を実行するために、内部コードのコピーが提供されている機器の特定ユニットを使用可能にする目的に限って、内部コードを実行できます。
4. お客様のライセンスは、規定された内部コードの使用に限定されています。そのほかの目的で内部コードを使用することはできません。たとえば、次の行為は禁止されています。
   (i) 内部コードへのアクセス、コピー、表示、印刷、改変、変更、修正、パッチ適用、派生物の作成、(電子的またはその他の方法による) 頒布、あるいはそのほかの方法で内部コードを使用すること。
   (ii) 内部コードを逆アセンブル、デコード、翻訳、逆コンパイル、またはリバースエンジニアリングすること (ただし、適用可能なヨーロッパの法律で逆コンパイルが明示的に許可されており、相互運用を可能にするための情報を取得することのみを目的としていて、情報をほかの方法では容易に取得できない場合を除く)。
   (iii) 内部コードの再ライセンス許諾、割り当て、リース契約を行うこと、または内部コードやそのコピーの使用を第三者に許諾すること。

5. 前述したように規定されたライセンスまたはこの注意事項全体は、いかなる方法でも、お客様に対して保守コードまたは保守コードのコピーを使用するためのライセンス、権限、その他の権利を許諾するものではありません。保守コードおよび StorageTek の保守用ツールおよび取扱説明書は、お客様が保管する場合、お客様に送付される機器のユニットに付属している場合、または内部コードとして同じ媒体に含まれる場合がありますが、それらは StorageTek のお客様サービス担当者か、StorageTek によりライセンス供与された事業体の担当者が使用することを意図したものであり、保守コード、保守用ツール、および取扱説明書に関するすべての権利は、StorageTek またはそのライセンサがこれを留保します。お客様は、保守コードを使用しないこと、または第三者に対して保守コードの使用および利用を許可しないことに同意したものとします。
6. エンドユーザーであるお客様は、本通知で規定するすべての義務を、機器を利用する第三者にも確実に適用するための適切な手順をすべて行うことに同意したものとします。
7. お客様は、使用許諾されている機器を譲渡することによってのみ、第三者に内部コードの所有権を譲渡できます。内部コードを使用するためのお客様のライセンスは、機器の所有者または法的占有者でなくなった時点で失効します。譲渡によりお客様が所有しなくなった機器の内部コードのすべてのコピーは、本通知の全条項のコピーとともに譲受人に付与する必要があります。

   お客様によりこのような譲渡が行われた場合 (両当事者のいずれによる追加行為もない場合)、自動的かつ明示的に、この機器を譲渡された当事者は本通知のすべての条項および条件に拘束されることになります。また、譲受人は、内部コードの最初に使用することでこのライセンスの条項に同意したことになります。本通知で許可されていない権利を機器の譲受人に譲渡することはできません。また、StorageTek は、譲受人またはその継承者による請求に対していかなる責務も負いません。さらに、本通知の条項および条件は、現在お客様が所有または使用している内部コード、あるいは StorageTek または第三者から今後取得する内部コードのすべてのコピーに対して適用されます。
8. 内部コードと保守コードの両方のコピーが出荷前に機器にインストールされているか、お客様に送付された機器やその他の構成部品に付属している場合がありますが、これらはすべて、StorageTek のサービス担当者、または StorageTek によりライセンス供与されたサービスプロバイダの便宜上行われたものです。また、機器に関連する保証期間中 (ある場合)、および StorageTek または StorageTek によりライセンス供与されたサービスプロバイダとの保守契約に基づいた機器保証期間中は、内部コードと保守コードはいずれも、この機器に組み込まれて機器内部で実行されるか、この機器に接続して使用されることがあります。お客様は、このような事実によって保守コードに対するいかなる権利もお客様に譲渡されないことに同意したものとします。

   StorageTek またはライセンス供与されたサービスプロバイダが、保守コード、保守用ツール、および取扱説明書をお客様の施設内で保管する場合がありますが、これは、StorageTek のお客様サービス担当者または StorageTek によりライセンス供与されたサービスプロバイダの担当者のみが使用することを意図したものです。さらに、お客様は、

   (i) このような保証期間または保守契約期間の終了時、または

   (ii) 機器の所有権を第三者に譲渡した時点で、この機器に関連し、StorageTek および認可されたサービスプロバイダが、すべての保守用ツールと取扱説明書を持ち去る権利、すべての保守コードを削除または使用不可にする権利、および (内部コードと保守コードの両方を含む) マイクロコードを内部コードのみで構成されるマイクロコードと置き換える権利を有することに同意したものとします。

改版履歴

EC	日付	改訂	説明
000227	2008 年 2 月	A	Crypto Key Management System 2.0 管理ガイド

目次

図目次

表目次

はじめに

対象読者

このマニュアルでは、Sun Microsystems StorageTek™ Crypto Key Management System (KMS) ソフトウェアの構成情報および管理情報について説明します。このマニュアルは、設置場所で KMS ソフトウェアを構成し維持する、ストレージ管理者、システムプログラマ、およびオペレータを対象にしています。

このマニュアルの構成

このマニュアルは、次の章で構成されています。

- 紹介
- 開始する前に
- KMS Manager の使用法
- 「System」メニューの使用法
- セキュリティー責任者の操作
- コンプライアンス責任者の操作
- オペレータの操作
- バックアップオペレータの操作
- 監査者の操作
- KMS コンソールの使用法

索引および用語集も含まれています。

追加情報

米国 Sun Microsystems, Inc. (以降「Sun」と表記) では、追加情報を入手するためのいくつかの方法を提供しています。

Sun の社外向け Web サイト

Sun の社外向け Web サイトでは、マーケティング、製品、イベント、会社、およびサービスに関する情報を提供しています。社外向け Web サイトには、Web ブラウザとインターネット接続できる方であればどなたでもアクセスできます。

Sun の社外向け Web サイトの URL は、http://www.sun.com です。

Sun StorageTek™ ブランドの固有情報の URL は、
http://www.sun.com/storagetek です。

Customer Resource Center

Sun StorageTek 製品の Customer Resource Center (CRC) は、StorageTek ブランドの製品について、メンバーがコードの修正版や技術的なドキュメントを検索して技術的な問題を解決するための Web サイトです。CRC のメンバーになると、その他のサービス (HIPER サブスクリプション、技術的なヒント、よくある質問に対する回答、製品マニュアルの補足、およびオンライン製品サポートの連絡先情報など) を優先的に受ける権利が得られます。保証期間中のお客様や保守サービス契約を結んでいるお客様は、CRC ホームページの「Request Password」ボタンを選択することで、加入を申し込むことができます。Sun の従業員は、SunWeb PowerPort を介して CRC に入ることができる場合があります。

CRC の URL は、http://www.support.storagetek.com です。

パートナーサイト

StorageTek Partners サイトは、StorageTek パートナー契約によるパートナーのための Web サイトです。このサイトは StorageTek のパートナーを支援するために、製品、サービス、カスタマーサポート、開催予定のイベント、トレーニングプログラム、および販促ツールに関する情報を提供します。このサイトでは、「Partners Login」より先のページへのアクセスが制限されています。「Partners Login」ページでは、アクセス権のない Sun の従業員および現在のパートナーがログイン ID とパスワードを要求することができ、パートナーを希望する会社が StorageTek 販売代理店の申し込みを行うことができます。

Sun パートナー契約によるパートナーのための URL は、
http://www.sun.com/partners/ です。

Sun 以外の Web サイト

このマニュアルで紹介する Sun 以外の Web サイトの利用については、Sun は責任を負いません。このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、広告、製品、またはその他の資料についても、Sun は保証しておらず、法的責任を負いません。また、このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、商品、サービスの使用や、それらへの依存に関連して発生した実際の損害や損失、またはその申し立てについても、Sun は一切の責任を負いません。

印刷版

このマニュアルの印刷版の追加を注文するか、ほかの StorageTek ブランド製品の顧客用文書の印刷版を注文する場合は、ご購入先にお問い合わせください。

カスタマーサポート

カスタマーサポートは、Sun または StorageTek と保守契約されたお客様、および Sun の従業員が 24 時間 365 日利用できます。カスタマーサポートの詳細は、Customer Resource Center (CRC) の Web サイトを参照してください。URL は、
http://www.support.storagetek.com です。

お客様からの保守要求

お客様の要求による保守は、お客様が Sun Microsystems StorageTek サポートに電話をかけることから始まります。認定された Sun のサポート担当者が即座に問題情報を記録して、適切なレベルのサポートを提供します。

Sun Microsystems StorageTek サポートに問題を連絡するには、次の手順を実行します。

1. 次の番号に電話をかけます。

   ☎ 800.872.4786 (1.800.USA.4SUN) (米国内)

   ☎ 800.722.4786 (カナダ)

   世界各地の連絡先の電話番号については、
   http://www.sun.com/service/contacting/solution.html
   を参照してください。

2. 電話対応オペレータに問題を説明します。電話対応オペレータは、いくつか質問して、サポート担当者に電話を転送するか、サポート担当者を派遣します。

   保守呼び出しを行う際に次の情報を用意すると、この手順が容易になります。

アカウント名	
サイトロケーション番号	
連絡担当者名	
電話番号	
装置のモデル番号	
デバイスのアドレス	
デバイスのシリアル番号 (わかっている場合)	
問題の緊急性	
障害症状コード (FSC)	
問題の説明	

Sun の各国のオフィス

Sun の各国のオフィスに問い合わせて、お客様の会社に適したストレージ、サービス、およびサポートに関する完全なソリューションについて相談できます。住所と電話番号については、Sun の社外向け Web サイトを参照してください。URL は、http://www.sun.com/worldwide/ です。

関連マニュアル

次のマニュアルでは、Key Management System (KMS) の使用法に関する具体的な項目の追加情報について説明します。

- 『Key Management System (KMS) 2.0 Installation and Service Manual』
- 『Key Management System (KMS) 2.0 Systems Assurance Guide』

読者の利便性を高めるための記号

製品名

KMS は、Sun StorageTek™ Crypto Key Management System の 2.0 実装を指します。

書体

このマニュアル内の例には、斜体の文字が含まれています。斜体は、変数を示すために使用します。これらの変数は実際の値に置き換える必要があります。

コマンド、制御文、およびパラメータで、大文字と小文字が混在している場合は、小文字を省略して略語にできることを示します。たとえば、POLicy コマンドを実行する場合には、単に POL と入力できます。

注意を喚起するメッセージ

注意を喚起するメッセージは、特に重要な情報や、本文や図に一意に関係する情報に注意を引くためのものです。

警告 – ハードウェアやソフトウェアの損傷を防ぐために必要な情報です。

注意 – データの破壊を防ぐために必要な情報です。

参考 – 作業の時間を短縮し容易にするための情報です。または、単なる注意点である場合もあります。

注 – 特別に関心を引く可能性のある情報です。また、規定や手順の例外を示すために使用される場合もあります。

第1章

紹介

概要

Crypto Key Management System (KMS) は、暗号化鍵を作成、格納、および管理します。KMS は、次のコンポーネントで構成されています。

- Key Management Appliance (KMA) − ポリシーベースのライフサイクル鍵管理、認証、アクセス制御、および鍵プロビジョニングの各サービスを提供する、セキュリティーが強化されたボックスです。ストレージネットワークの信頼できる発行局として、KMA では、すべてのストレージデバイスが登録および認証されること、そしてすべての暗号化鍵が規定のポリシーに従って作成、プロビジョニング、および削除されることが保証されます。
- KMS Manager GUI − ワークステーション上で実行されるグラフィカルユーザーインタフェースで、IP ネットワーク経由で KMA と通信し、KMS を設定および管理します。KMS Manager GUI は、顧客が用意するワークステーションにインストールする必要があります。
- KMS クラスタ − システム内の KMA の完全な集合。これらのすべての KMA は相互に認識し、情報を相互に複製します。
- エージェント − KMS クラスタによって管理される鍵を使用して、暗号化を実行するデバイスまたはソフトウェア。KMS 2.0 の場合、エージェントは StorageTek 暗号化テープドライブです。エージェントは、エージェント API を介して KMA と通信します。エージェント API は、エージェントハードウェアまたはソフトウェアに組み込まれている一連のソフトウェアインタフェースです。

KMS の概念

KMS クラスタ

KMS では、複数の KMA のクラスタ化をサポートしています。これによって、負荷分散とフェイルオーバーが実現されます。KMS クラスタ内のすべての KMA は、アクティブ/アクティブ方式で動作します。すべての KMA が、任意のエージェントにすべての機能を提供できます。ある KMA で実行される処理は、クラスタ内のほかのすべての KMA にただちに複製されます。

エージェント

エージェントは、暗号化処理を実行します。具体的には、書き込み時のデータの暗号化と読み取り時のデータの復号化を実行します。エージェントは、暗号化処理の実行に使用される鍵の作成および取り出しのために、KMS クラスタと通信します。

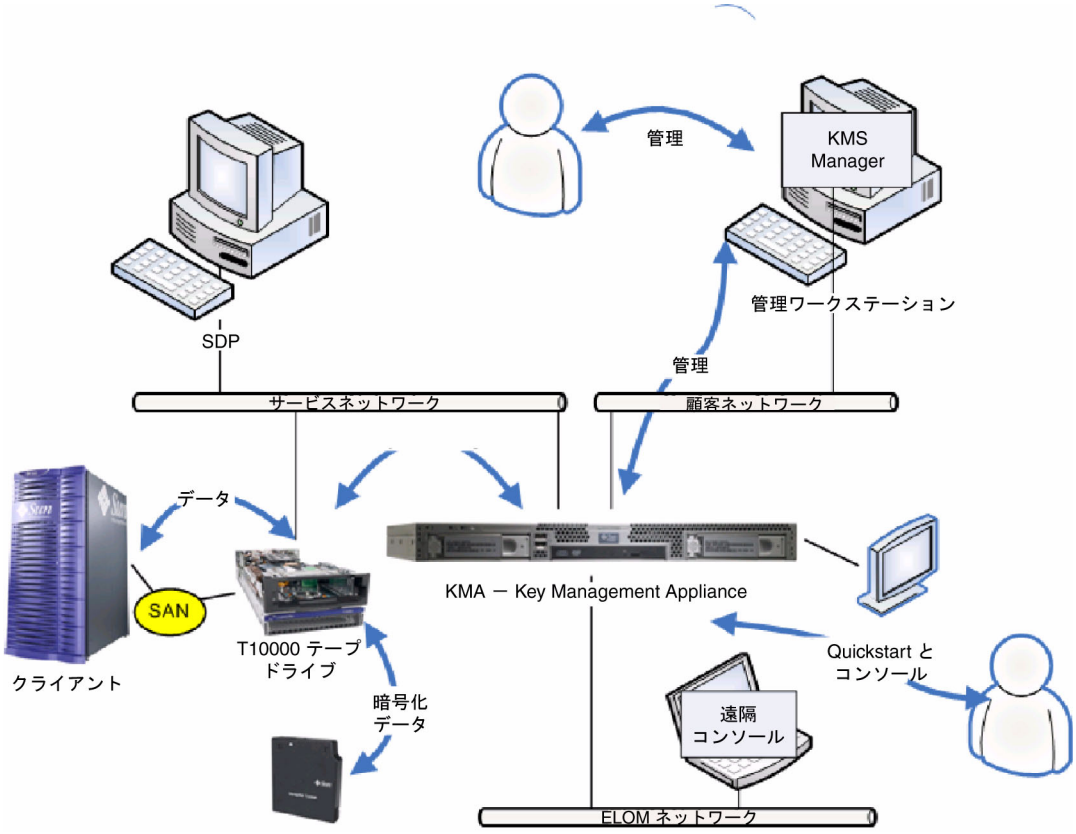
ネットワーク接続

KMS は、TCP/IP ネットワークを使用して、KMA、エージェント、および KMS Manager GUI を実行しているマシン間を接続します。ネットワーク接続を柔軟に行うために、KMA には、ネットワーク接続用の次の 2 つのインタフェースが用意されています。

- 管理接続。顧客ネットワークとの接続に使用します。
- サービス接続。テープドライブとの接続に使用します。

本稼動の KMA インストール環境では、ライブラリ固有のアクセサリキットを利用できます。このアクセサリキットには、ドライブと KMA 間の接続に使用するスイッチおよびケーブルが含まれています。KMA との接続を図 1-1 に示します。

図 1-1 KMA との接続



初期設定 — 直接接続または遠隔コンソール (ELOM)

KMA の初期設定は、コンソール接続経由で実行します。この初期設定は、KMA に直接接続されたモニターとキーボードを使用するか、または Embedded Lights Out Manager (ELOM) の遠隔コンソール機能を使用して実行できます。ELOM が提供するコンソールへの遠隔接続によって、サーバーの機能を実行できます。

ELOM 遠隔コンソール機能には、3 つめのネットワーク接続が必要です。図 1-1 では、「ELOM ネットワーク」と示されています。遠隔コンソール機能を使用するには、このマニュアルで後述する手順に従って、ELOM の IP アドレスを設定する必要があります。

注 – 通常、ELOM ネットワークは、実際には顧客ネットワークと同じネットワークになります。

初期設定 — QuickStart プログラム

出荷時のデフォルト状態の KMA の電源を入れると、初期設定を行うために、QuickStart と呼ばれるウィザード機能がコンソールで実行されます。処理が完了すると、KMS Manager GUI から、その他のほとんどの機能を実行できるようになります。少数の機能に対しては、機能が制限されたコンソールインタフェースが有効なままです。

鍵のライフサイクル

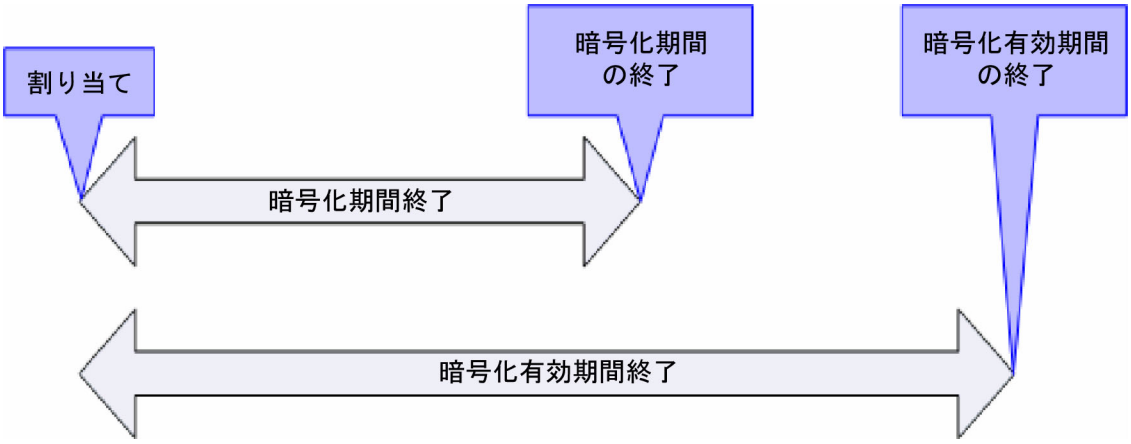
鍵のライフサイクルは、鍵ポリシーに基づいて行われます。KMS によって規定されるライフサイクルは、NIST 800-57 ガイドラインに基づいています。KMS の微妙な違いに対処するために、いくつかの状態が追加されています。

鍵のライフサイクルは、鍵ポリシーで定義されている次の 2 つの期間 (図 1-2 を参照) に基づいています。

- 暗号化期間
- 暗号化有効期間

暗号化期間は、データの暗号化に使用できる鍵が割り当てられてからの期間です。暗号化有効期間は、復号化に使用できる期間です。鍵が割り当てられると、この 2 つの期間は同時に開始されます。

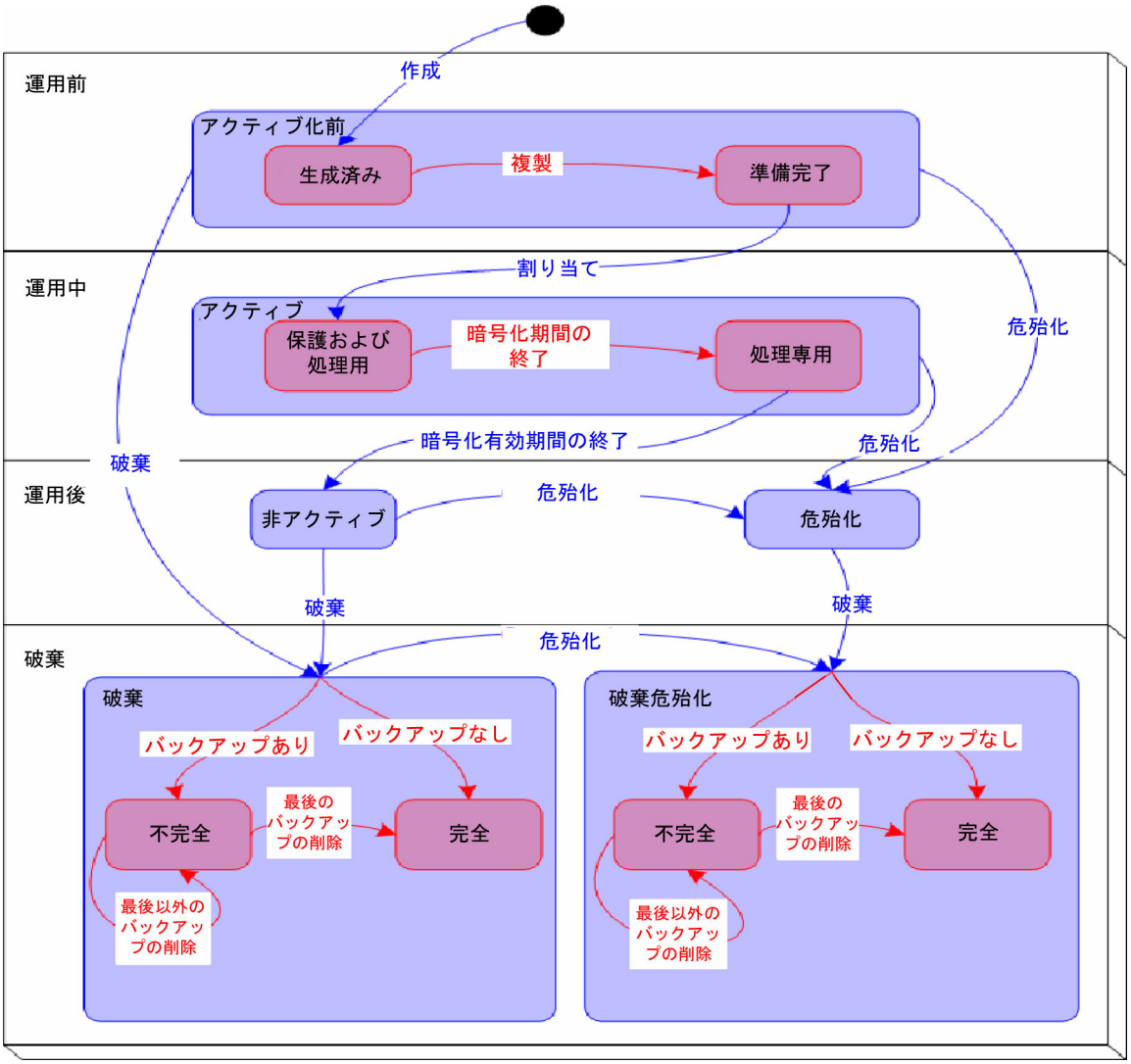
図 1-2　鍵のライフサイクル期間



状態遷移

暗号化期間と暗号化有効期間と、KMS のその他の機能とを組み合わせて、図 1-3 に示すような鍵の状態遷移が定義されます。この図で青色で示されている状態と遷移は、NIST 800-57 で定義されています。

図 1-3　状態遷移図



KMS の状態と遷移

図 1-3 に赤色で示されている状態と遷移は、KMS によって追加されたものです。KMS Manager で鍵を検査しているときには、もっとも内側の状態のみが示されます。KMS の状態を次に示します。

アクティブ化前 (Pre-activation)

鍵は生成済みですが、まだ利用可能にはなっていません。KMS では、アクティブ化前状態に、生成済みと準備完了という 2 つのより詳細な状態が追加されています。

生成済み (Generated)

生成済み状態の鍵とは、KMA クラスタ内の KMA のいずれかで作成された鍵のことです。マルチ KMA クラスタでは、少なくとも 1 つのほかの KMA に複製されるまで、鍵は生成済み状態のままです。KMA が 1 つのみ存在するクラスタでは、鍵が生成済み状態から遷移するには、少なくとも 1 つのバックアップに記録される必要があります。

準備完了 (Ready)

準備完了状態の鍵とは、複製またはバックアップによる損失に対して保護されている鍵のことです。準備完了状態の鍵は、割り当てに使用できます。「複製された状態」の遷移は、鍵が複製されたとき、または単一 KMA クラスタの場合はバックアップされたときに発生します。

アクティブ (Active)

この鍵は、情報を保護する場合 (暗号化) または以前に保護された情報を処理する場合 (復号化) に使用できます。NIST では、アクティブ状態の鍵は保護専用、処理専用、または保護および処理用として指定できることが示されています。さらに、対称データ暗号化鍵の場合は、特定の期間中は情報の保護および処理用として鍵を使用することができ、この期間が過ぎると鍵を引き続き処理専用として使用できることが明確に示されています。

KMS では、アクティブ状態に 2 つの下位の状態が追加されています。これらの状態は NIST に記載されていますが、状態として明確に識別されているわけではありません。

保護および処理 (Protect-and-process)

この状態の鍵は、暗号化と復号化の両方に使用できます。割り当てられた鍵は、この状態になります。暗号化エージェントが新しい鍵の作成を要求すると、割り当てが実行されます。

処理専用 (Process only)

この状態の鍵は、復号化には使用できますが、暗号化には使用できません。エージェントは、たとえば読み取り中または書き込み中の特定のデータユニットに対して使用可能な鍵の中に保護および処理状態の鍵が全くないと判断すると、新しい鍵を作成するはずです。鍵の状態が保護および処理用から処理専用に遷移するのは、その鍵の暗号化期間が終了したときのみです。

非アクティブ (Deactivated)

鍵の暗号化有効期間は過ぎていても、情報の処理 (復号化) を行うためにその鍵がまだ必要となる場合があります。NIST では、この状態の鍵をデータの処理に使用できることが明確に示されています。

厳密に言うと、NIST ガイドラインでは、非アクティブまたは危殆化状態の鍵を含めて、運用後の鍵をアクセス可能な状態のままにしておく必要がある場合は、これらの鍵のアーカイブを推奨することを明確に示しています。これは鍵の復旧処理であり、鍵をアーカイブから再度呼び出して使用可能にすることができます。

KMS では KMA バックアップという形式のアーカイブが用意されていますが、バックアップから 1 つの鍵を再度呼び出すことはできません。このため、KMS では、運用後の段階の鍵を KMS クラスタ内に保持して、エージェントからの要求があればこの鍵を提供します。

危殆化 (Compromised)

承認されていない実体によって解放または検出された鍵は、危殆化されています。危殆化状態の鍵は、情報を保護するために使用してはいけませんが、情報を処理するためには使用できます。

破棄 (Destroyed)

破棄された鍵は存在しなくなりますが、鍵に関する情報は保持できます。KMS 2.0 では、破棄された鍵の鍵データは KMS クラスタから削除されます。破棄された鍵は、エージェントに提供されません。

注 – 鍵を破棄する唯一の方法は、GUI または管理 API を使用することです。

NIST ガイドラインでは、時間に基づいて鍵を破棄する場合の基準は設けられていないようです。

KMS では、破棄状態と破棄危殆化状態に、2 つの下位の状態が定義されています。KMS が作成するバックアップは KMS では制御されないため、これらの状態が作成されています。顧客の管理者は、バックアップが破棄されたら、これを KMS に通知する必要があります。すべてのバックアップが破棄されたあとにのみ、実際に鍵が破棄されたと見なすことができます。これらの下位の状態とは、不完全および完全です。

不完全 (Incomplete)

破棄された鍵が含まれるバックアップがまだ 1 つ以上存在しています。この下位状態では、KMS クラスタ内のどの KMA にも鍵は存在していません。この状態の鍵をエージェントに提供することはできません。

完全 (Complete)

鍵が含まれるすべてのバックアップが破棄されています。鍵はどの KMA にもどのバックアップにも存在しません。厳密には、この鍵が含まれるバックアップがまだ存在している可能性があります。KMS が認識しているのは、バックアップの破棄が KMS に通知されたということのみです。これらのバックアップが実際に破棄されていることを確認するのは、ユーザーの責任です。

破棄状態への遷移は、管理コマンドの実行結果としてのみ発生することに注意してください。また、鍵が非アクティブ状態または危殆化状態という運用後の段階である場合は、引き続き暗号化エージェントに提供することができます。この説明は、運用後の段階に関する NIST の記述と一致しています。NIST ガイドラインでは、運用後段階の鍵が「不要になった」場合には、これを破棄する必要があることが明確に示されています。鍵が「不要になった」かどうかを判定できるのはユーザーのみであり、破棄状態への遷移を開始できるのは外部の実体のみであるとと考えられます。

破棄危殆化 (Destroyed Compromised)

この状態は破棄と同じですが、鍵が破棄前または破棄後に危殆化されています。

ユーザーとロールベースのアクセス制御

KMS には、複数のユーザーをそれぞれユーザー ID とパスフレーズを使用して定義する機能があります。各ユーザーには、1 つ以上の事前定義済みロールが付与されています。これらのロールは、次のとおりです。

- セキュリティー責任者 ― KMS の設定および管理を実行します。
- オペレータ ― エージェントの設定および日常業務を実行します。
- コンプライアンス責任者 ― 鍵グループを定義し、エージェントによる鍵グループへのアクセスを制御します。
- バックアップオペレータ ― バックアップ操作を実行します。
- 監査者 ― システムの監査証跡を参照できます。

QuickStart 処理中に、セキュリティー責任者が定義されます。QuickStart が完了したあとで、KMS Manager GUI を使用してその他のユーザーを定義できます。

各ロールに許可されている操作

14 ページの表 1-1 に、各ロールに許可されている機能のリストを示します。GUI およびコンソールでは、許可されている操作のみが示されます。操作が表示されていても、これを実行しようとすると、失敗する場合があります。この状況は、操作が表示されてからその操作を実行しようとするまでの間に、ユーザーからロールが削除されると発生することがあります。

機能する暗号化システムを構築するには、監査者以外のすべてのロールが必要です。ロールごとに個別のユーザーを作成できます。または、複数のロールを 1 つのユーザーに付与することも可能です。

定足数保護

KMS には、特定の操作に対する定足数保護が用意されています。最大 10 ユーザーの定足数を定義できます。また、1 から定足数ユーザー数までのしきい値が定義されます。この情報は、鍵分割資格と呼ばれます。ユーザー ID とパスフレーズは、システムへのログインに使用されるユーザー ID とパスフレーズとは異なります。定足数による承認が必要な操作を実行しようとすると、各定足数ユーザーがユーザー ID とパスフレーズを入力できる画面が表示されます。操作が許可されるように指定するには、少なくとも指定されたしきい値のユーザー ID とパスフレーズを入力する必要があります。

データユニット、鍵、鍵グループ、および鍵ポリシー

データユニットは、エージェントによって暗号化されたデータを表すために使用されます。テープドライブの場合、データユニットはテープカートリッジであり、データユニットは常に存在しています。これは基本的な要件ではなく、将来的には、データユニットを定義しなくてもエージェントが動作する可能性があります。

鍵は、実際の鍵の値 (鍵データ) とその関連メタデータです。

鍵ポリシーは、鍵を制御するパラメータを定義します。このようなパラメータには、ライフサイクルパラメータ (暗号化期間と暗号化有効期間) や、エクスポートまたはインポートパラメータ (インポート許可とエクスポート許可) などがあります。

鍵グループは、鍵と鍵ポリシーを関連付けます。鍵グループは特定の鍵ポリシーを持ち、エージェントに割り当てられます。各エージェントには、許可された鍵グループのリストがあります。エージェントは、エージェントの許可された鍵グループのいずれかに割り当てられた鍵のみを取り出すことができます。また、エージェントには、デフォルトの鍵グループもあります。エージェントが鍵を作成した場合、具体的には、鍵がデータユニットに割り当てられた場合、その鍵はエージェントのデフォルトの鍵グループに配置されます。エージェントがより高度に鍵グループを制御することができる機能が用意されています。ただし、既存のエージェントはこの機能を活用できません。

システムが機能するには、少なくとも鍵ポリシーが 1 つと鍵グループが 1 つ定義されている必要があります。この鍵グループは、すべてのエージェントのデフォルトの鍵グループとして割り当てられている必要があります。

TCP/IP 接続と KMA

左側に示されている実体と KMA との間にファイアウォールが存在する場合、ファイアウォールでは、各実体が次のポートで KMA と TCP/IP 接続を確立できるように設定されている必要があります。

- KMS Manager から KMA への通信には、ポート 3331、3332、3333、3335 が必要です。
- エージェントから KMA への通信には、ポート 3331、3332、3334、3335 が必要です。
- KMA から KMA への通信には、ポート 3331、3332、3336 が必要です。

ネットワーク内の KMS

図 1-4 に、KMS ソリューションの典型的な配備を示します。

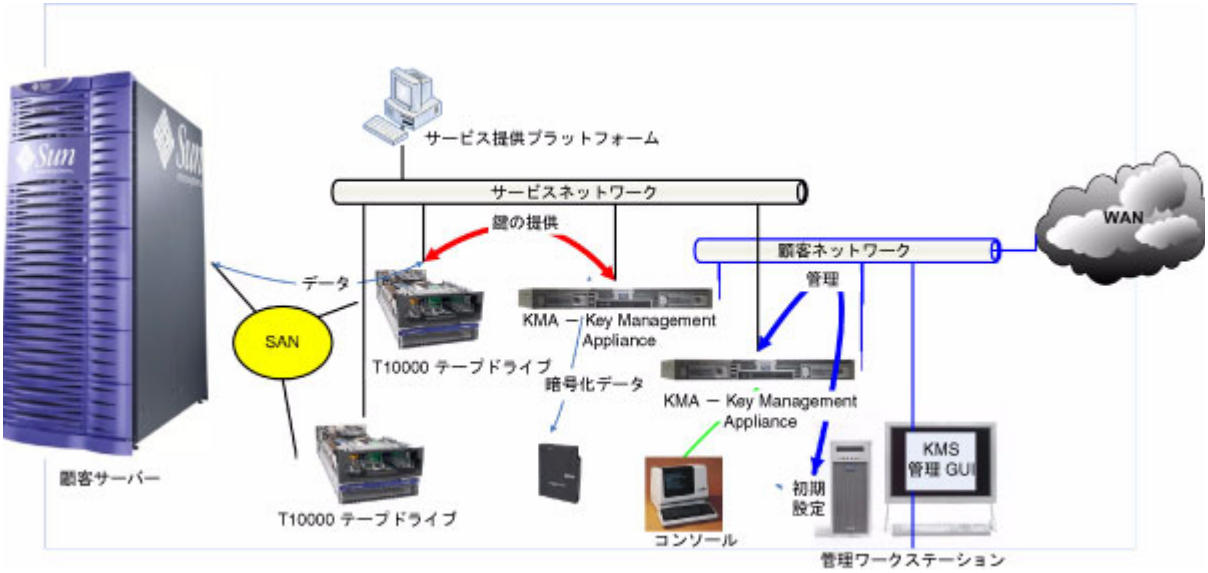


図 1-4　　KMS ソリューションの典型的な配備

KMS Manager のソフトウェア要件

KMS Manager を実行するには、Microsoft® Windows XP、Solaris 10 x86 Update 3、または Solaris 10 x86 Update 4 が動作するワークステーションが必要です。

オンラインヘルプの使用法

KMS Manager には、包括的なオンラインヘルプが用意されています。KMS Manager の任意の画面でヘルプを表示するには、次の手順を実行します。

- パネル上部にある「Help」ボタンをクリックして、全般的なヘルプを表示します。

または

- Tab キーを押すか、パネル内の任意の場所をクリックして、パネルに移動します。次に、F1 キーを押して、コンテキストヘルプを表示します。

ロールベースのアクセス制御

KMS では、次のロールが定義されています。

- **セキュリティー責任者**は、セキュリティー設定値、ユーザー、サイト、および転送パートナーを管理します。
- **コンプライアンス責任者**は、鍵ポリシーと鍵グループを管理し、鍵グループを使用できるエージェントと転送パートナーを決定します。
- **オペレータ**は、エージェント、データユニット、および鍵を管理します。
- **バックアップオペレータ**は、バックアップを実行します。
- **監査者**は、KMS クラスタに関する情報を表示します。

単一 KMA ユーザーアカウントでは、1 つ以上のロールにメンバーシップを割り当てることができます。KMA では、ユーザーのロールに基づいて、要求元のユーザー実体に操作を実行する権限があるかどうかが確認されます。ロールについては、258 ページの「KMA へのログイン」を参照してください。

ロールベースの操作

表 1-1 に、各ユーザーのロールで実行できるシステムの操作を示します。「ロール」列の内容は、次のとおりです。

- **可**。そのロールに対してその操作の実行が許可されていることを示します。
- **定足数**。そのロールに対してその操作の実行が許可されていますが、定足数を満たす必要があることを示します。
- **空欄**。そのロールに対してその操作の実行が許可されていないことを示します。

表 1-1　　システムの操作とユーザーのロール

実体	操作	ロール				
		セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者
コンソール						
	ログイン	可	可	可	可	可
	KMA ロケールの設定	可				
	KMA IP アドレスの設定	可				
	技術サポートの有効化	可				
	技術サポートの無効化	可		可		
	主管理者の有効化	可				
	主管理者の無効化	可		可		
	KMA の再起動			可		
	KMA の停止			可		
	クラスタへの KMS のログイン	定足数				
	ユーザーのパスフレーズの設定	可				
	KMA のリセット	可				
	KMA のゼロ化	可				
	ログアウト	可	可	可	可	可
接続						
	ログイン	可	可	可	可	可
	プロファイルの作成	可	可	可	可	可
	プロファイルの削除	可	可	可	可	可
	構成値の設定	可	可	可	可	可
	切断	可	可	可	可	可
鍵分割資格						
	一覧表示	可				
	変更	定足数				

表 1-1　システムの操作とユーザーのロール

実体	操作	ロール				
		セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者
自律ロック解除						
	一覧表示	可				
	変更	定足数				
KMA のロック/ロック解除						
	状態の一覧表示	可	可	可	可	可
	ロック	可				
	ロック解除	定足数				
サイト						
	作成	可				
	一覧表示	可		可		
	変更	可				
	削除	可				
セキュリティーパラメータ						
	一覧表示	可	可	可	可	可
	変更	可				
KMA						
	作成	可				
	一覧表示	可		可		
	変更	可				
	削除	可				
ユーザー						
	作成	可				
	一覧表示	可				
	変更	可				
	パスフレーズの変更	可				
	削除	可				
ロール						
	一覧表示	可				
鍵ポリシー						
	作成		可			
	一覧表示		可			
	変更		可			
	削除		可			
鍵グループ						
	作成		可			

表 1-1　システムの操作とユーザーのロール

実体	操作	ロール				
		セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者
	一覧表示		可	可		
	データユニットの一覧表示		可	可		
	エージェントの一覧表示		可	可		
	変更		可			
	削除		可			
エージェント						
	作成			可		
	一覧表示		可	可		
	変更			可		
	パスフレーズの変更			可		
	削除			可		
エージェント/鍵グループの割り当て						
	一覧表示		可	可		
	変更		可			
データユニット						
	作成					
	一覧表示		可	可		
	変更			可		
	鍵グループの変更		可			
	削除					
鍵						
	データユニット鍵の一覧表示		可	可		
	破棄			可		
	危殆化		可			
転送パートナー						
	設定	定足数				
	一覧表示	可	可	可		
	変更	定足数				
	削除	可				
鍵転送鍵						
	一覧表示	可				
	更新	可				
転送パートナー鍵グループの割り当て						

表 1-1　システムの操作とユーザーのロール

実体	操作	ロール				
		セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者
	一覧表示		可	可		
	変更		可			
バックアップ						
	作成				可	
	一覧表示	可	可	可	可	
	破棄された鍵を含むバックアップの一覧表示		可	可		
	復元	定足数				
	破棄の確認				可	
コアセキュリティーバックアップ						
	作成	可				
SNMP マネージャー						
	作成	可				
	一覧表示	可		可		
	変更	可				
	削除	可				
イベントの監査						
	表示	可	可	可	可	可
	エージェント履歴の表示		可	可		
	データユニット履歴の表示		可	可		
	データユニット鍵履歴の表示		可	可		
システムダンプ						
	作成	可		可		
システム時刻						
	一覧表示	可	可	可	可	可
	変更	可				
NTP サーバー						
	一覧表示	可	可	可	可	可
	変更	可				
ソフトウェアバージョン						
	一覧表示	可	可	可	可	可
	アップグレード			可		

Key Management Appliance の設定および管理

KMS ソリューションを可能なかぎり迅速かつ簡単に設置および構成する手順については、『KMS 2.0 Installation and Service Manual』を参照してください。

第２章

開始する前に

この章では、次の項目について説明します。

- Embedded Lights Out Manager (ELOM) の起動 － ELOM を使用すると、コンソールへの遠隔接続を行うことができます。
- QuickStart プログラムの実行 － QuickStart は、CSE が新しい KMA の構成に使用するユーティリティーです。

Embedded Light Out Manager (ELOM) の起動

Embedded Lights Out Manager (ELOM) システムには、メインサーバーとは別のプロセッサが搭載されています。プラグを差し込み電源を入れてから、1 ～ 2 分の起動時間のあと、ELOM によってコンソールへの遠隔接続が確立され、QuickStart プログラムなどのサーバーの機能を実行できるようになります。

注 – サーバーの構成に使用するいくつかの基本的な ELOM コマンドについては、『KMA Installation and Service Manual』を参照してください。詳細は、『Embedded Lights Out Manager Administration Guide』を参照してください。

KMA への接続

Embedded Lights Out Manager を介した KMA への接続には、次のいずれかを使用します。

- LAN 1 NET MGT ELOM インタフェースによるネットワーク接続 (推奨)
- KMA に接続されているキーボードとモニター

ポップアップブロッカによって、ここで説明する手順を Windows で開始できなくなります。手順を開始する前に、ポップアップブロッカを無効にしてください。

ウィンドウが表示されても、コンソールウィンドウが表示されない場合は、Web ブラウザまたは Java バージョンと ELOM の互換性がありません。ブラウザと Java を最新版にアップグレードしてください。互換性のあるバージョンの一覧は、表 2-1 を参照してください。

表 2-1 互換性のある Web ブラウザと Java バージョン

クライアント OS	Java Runtime Environment (Java Web Start を含む)	Web ブラウザ
■ Microsoft Windows XP Pro	JRE 1.5 (Java 5.0 Update 7 以降)	■ Internet Explorer 6.0 以降および Mozilla 1.7.5 以降 ■ Mozilla Firefox 1.0
■ Red Hat Linux 3.0 および 4.0		■ Mozilla 1.7.5 以降 ■ Mozilla Firefox 1.0
■ Solaris 9 ■ Solaris 10 ■ SUSE Linux 9.2		■ Mozilla 1.7.5
Java Runtime Environment 1.5 は、http://java.com からダウンロードできます。 ELOM マニュアルの最新バージョンは、http://docs.sun.com/ で参照できます。 Sun Fire X2100 M2 サーバーのマニュアルは、http://docs.sun.com/app/docs/coll/x2100m2 からダウンロードできます。		

ネットワーク接続の使用

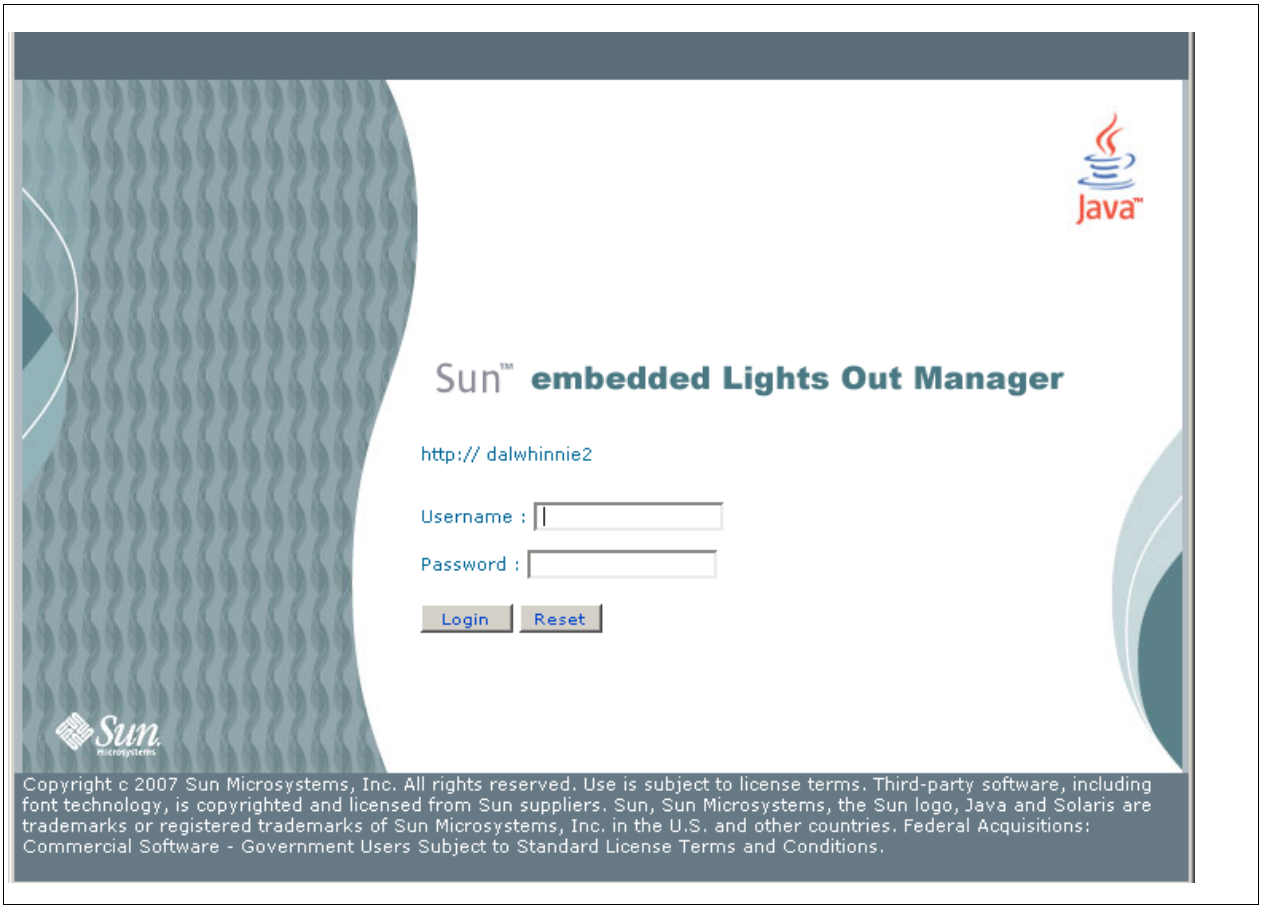
1. ネットワーク上の別のワークステーションを使用して、Web ブラウザを起動します。
2. 構成した LAN 1 (NET MGT) の IP アドレスまたはホスト名を使用して、KMA ELOM に接続します。

注 – ELOM に含まれている証明書が、割り当てられた名前または IP と一致しないため、Web ブラウザに 1 つ以上の警告が表示されます。

---

3. 「OK」または「Yes」をクリックして、警告を無視します。
   警告を無視したあと、ELOM のログインプロンプトが表示されます。

図 2-1　Embedded Lights Out Manager のログイン画面

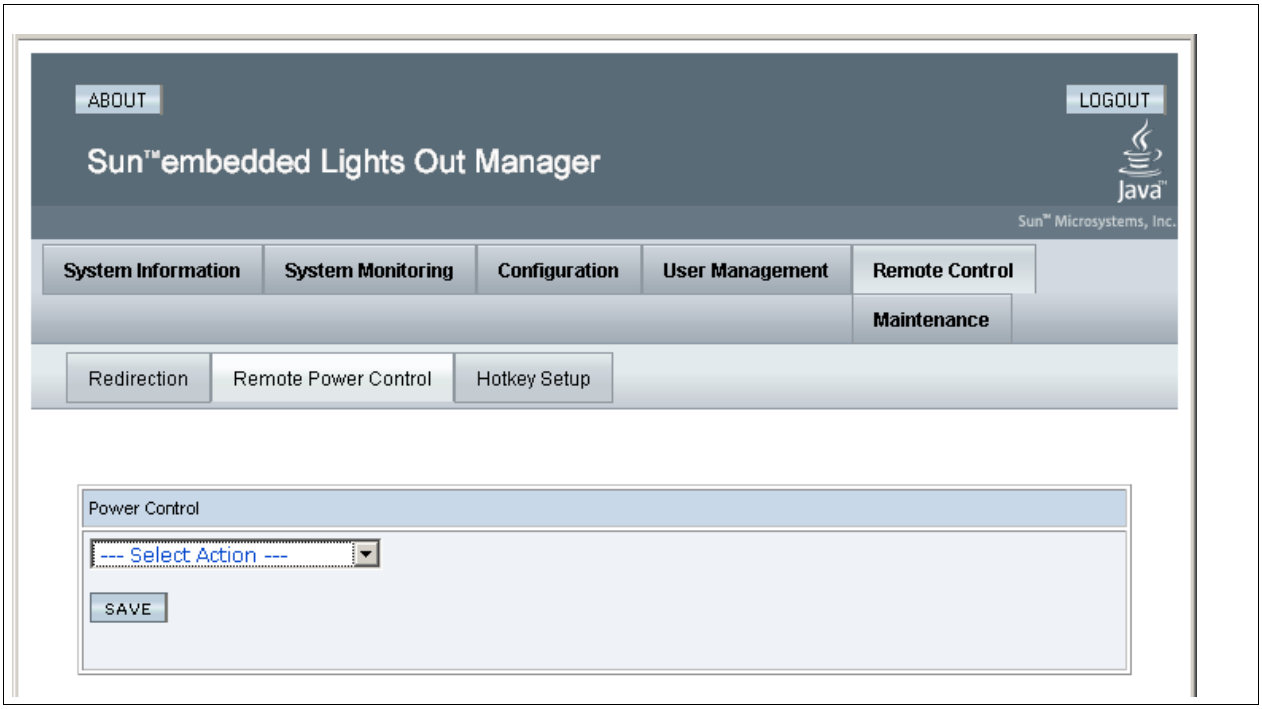


4. ユーザー ID に `root`、パスワードに `changeme` を使用してログインします。
   次に表示される画面は Manager の画面です。サーバーを接続しただけで、まだサーバーの電源が入っていない場合、システムの起動は完了していません。

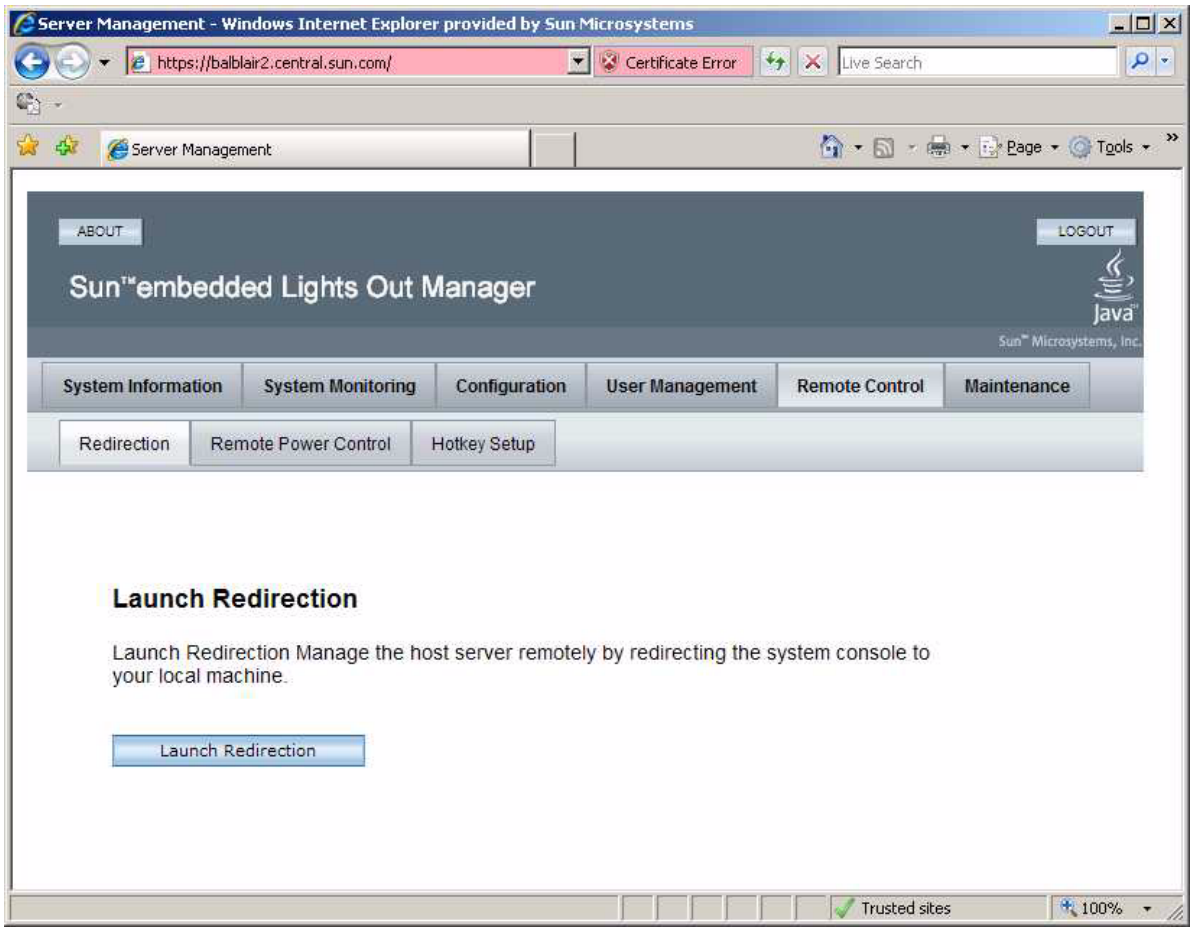
   KMA は、最初の電源投入時に自動的に起動するように構成されており、電源投入から数分で起動して QuickStart プロンプトが表示されるはずです。

5. 「System Monitoring」タブをクリックして、電源の状態を確認します。
   電源の状態が表形式で示されます。
6. 電源の状態が「power off」の場合、
   上側のタブ行の右端にある「Remote Control」タブをクリックします。
7. 下側のタブ行にある「Remote Power Control」タブをクリックします。
8. 「Select Action」ドロップダウンで「Power On」を選択し、「Save」ボタンをクリックします。
   KMA の電源投入が開始されます。この処理には数分かかりますが、KMA の構成を続行することができます。

図 2-2　電源制御

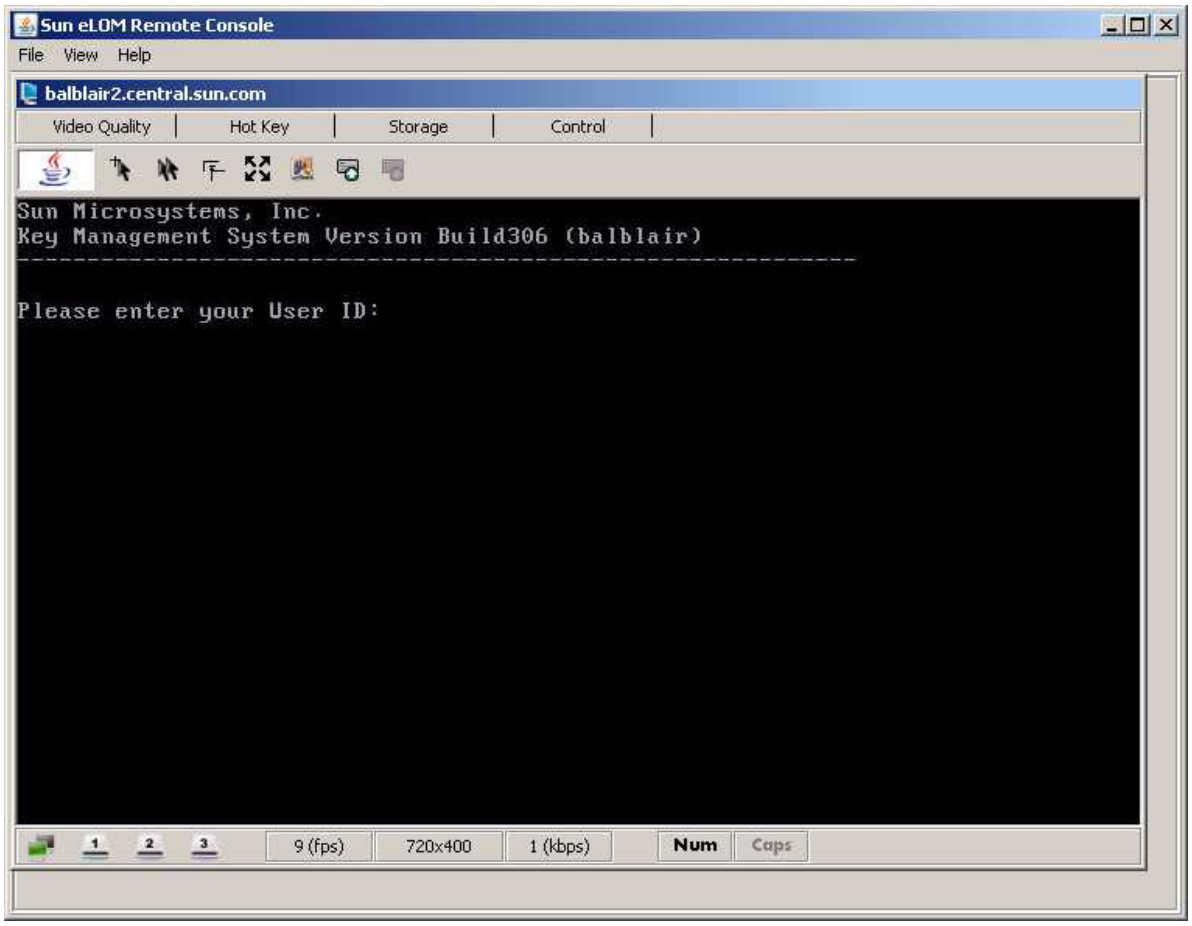


9. 上側のタブ行にある「Remote Control」タブをクリックします。
10. 下側のタブ行にある「Redirection」タブをクリックします。
11. 「Launch Redirection」ボタンをクリックします。



ここで、新しいウィンドウに遠隔コンソール画面が表示されます。

12. 遠隔コンソールウィンドウが表示される前に、Java アプレットがダウンロードされます。javaRKVM.jnlp ファイルが要求された場合は、これを保存してから開き、遠隔コンソールを起動します。表示される可能性がある警告は、すべて無視します。


Sun eLOM Remote Console
File View Help
balblair2.central.sun.com
Video Quality
Hot Key
Storage
Control
Sun Microsystems, Inc.
Key Management System Version Build306 (balblair)
Please enter your User ID:
9 (fps)
720x400
1 (kbps)
Num
Caps

QuickStart プログラムの実行

出荷時のデフォルト状態にある KMA の電源を入れると、QuickStart と呼ばれる特殊なモードの KMA 構成メニューが自動的に実行されます。QuickStart によって、KMA の初期化に必要な最低限の構成情報が収集されます。QuickStart プログラムの実行がいったん正常に完了すると、このプログラムは再度実行できません。QuickStart プログラムにもう一度アクセスする唯一の方法は、KMA を出荷時のデフォルト状態にリセットすることです。

注 – 以降の画面の例で**太字**で示されているエントリは、ユーザーが入力する部分を表します。

QuickStart の起動

QuickStart を実行するには、次の手順を実行します。

KMA の電源を入れます。KMA の電源をはじめて入れると、QuickStart が実行され、「Welcome to QuickStart!」画面が表示されます。

```
Welcome to QuickStart!

The QuickStart program will guide you through
the necessary steps for configuring the KMA.

You may enter Ctrl-c at any time to abort; however,
it is necessary to successfully complete all steps in this
initialization program to enable the KMA.

Press Enter to continue:

Set Keyboard Layout
_____________________________________________________________

Press Ctrl-c to abort.

You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian ( 2) Belarusian ( 3) Belgian
( 4) Bulgarian ( 5) Croatian ( 6) Danish
( 7) Dutch ( 8) Finnish ( 9) French
(10) German (11) Icelandic (12) Italian
(13) Japanese-type6 (14) Japanese (15) Korean
(16) Malta_UK (17) Malta_US (18) Norwegian
(19) Portuguese (20) Russian (21) Serbia-And-Montenegro
(22) Slovenian (23) Slovakian (24) Spanish
(25) Swedish (26) Swiss-French (27) Swiss-German
(28) Taiwanese (29) TurkishQ (30) TurkishF
(31) UK-English (32) US-English

The current layout is US-English.

Please enter the number for the keyboard layout : 32

The keyboard layout has been applied successfully.

Press Enter to continue:
```

注 – Ctrl-c キーを押すと、QuickStart プログラムがリセットされ、「Welcome to QuickStart!」画面が再度表示されます。

IP アドレスの設定

1. 「Press Enter to continue:」プロンプトで、Enter キーを押します。次の情報が表示されます。

```
A static IP Address configuration must be set in order for the KMA
to communicate with other KMAs, Agents, or Users in your system.

Please enter the Management Network Hostname: KMSmgr

Do you want to use DHCP to configure the Management Network
interface? [y/n]: n

Please enter the Management Network IP Address: 129.80.123.32

Please enter the Management Network Subnet Mask: 255.255.254.0

Please enter the Service Network Hostname: SDP

Do you want to use DHCP to configure the Service Network
interface? [y/n]: n

Please enter the Service Network IP Address: 172.18.18.1

Please enter the Service Network Subnet Mask: 255.255.254.0

Please enter the Gateway IP Address (optional but necessary
if this KMA is to communicate with an entity on a
different IP Subnet): 129.80.123.254

Please enter the Primary DNS Server IP Address (optional):
129.80.0.4

Please enter the DNS Domain: my.customer.com

Applying network settings... Done.

The Network Configuration has been updated.

Press Enter to continue:

Press Ctrl-c to abort.
```

2. 「Please enter the Management Network Hostname:」プロンプトで、管理ネットワークのホスト名を入力し、Enter キーを押します。

3. 「Do you want to use DHCP to configure the Management Network interface? [y/n]:」プロンプトで、n または y のいずれかを入力して Enter キーを押します。n を入力した場合は、手順 4 に進みます。y を入力した場合は、手順 6 に進みます。

4. 「Please enter the Management Network IP Address:」プロンプトで、管理ネットワークの IP アドレスを入力して Enter キーを押します。

5. 「Please enter the Management Network Subnet Mask:」プロンプトで、サブネットマスクアドレス (255.255.254.0 など) を入力して Enter キーを押します。

6. 「Please enter the Service Network Hostname:」プロンプトで、サービスネットワークのホスト名を入力して Enter キーを押します。

7. 「Do you want to use DHCP to configure the Service Network interface? [y/n]:」プロンプトで、n または y のいずれかを入力して Enter キーを押します。n を入力した場合は、手順 8 に進みます。y を入力した場合は、手順 10 に進みます。

8. 「Please enter the Service Network IP Address:」プロンプトで、サービスネットワークの IP アドレスを入力して Enter キーを押します。

9. 「Please enter the Service Network Subnet Mask:」プロンプトで、サブネットマスクアドレス (たとえば、255.255.255.0) を入力して Enter キーを押します。

10. 「Please enter the Gateway IP Address (optional but necessary if this KMA is to communicate with an entity on a different IP Subnet:」プロンプトで、ゲートウェイ IP アドレスを入力し、Enter キーを押します。KMA がサブネット外の実体と一切通信しない場合は、このエントリを空白のままにすることができます。

11. 「Please enter the Primary DNS Server IP Address (optional):」プロンプトで、プライマリ DNS サーバーの IP アドレスを入力して Enter キーを押します。このエントリは、空白のままにすることができます。

12. 「Please enter the DNS Domain:」プロンプトで、DNS ドメインを入力して Enter キーを押します。

13. 次の情報が表示され、各ネットワーク設定値が適用されたことが示されます。この処理には 1 ～ 2 分かかることがあります。

KMA の初期化

1. Enter キーを押して続行します。次の情報が表示されます。

```
The KMA Name is a unique identifier for your KMA. This name should
not be the same as the KMA Name for any other KMA in your cluster.
It also should not be the same as any User Names or Agent IDs in
your system.

Please enter the KMA Name: KMA-1

Press Enter to continue:

Set Root Passphrase (Technical Support)
_____________________________________________________________
The 'root' account can only be used by Support personnel to
administer support under extreme circumstances. You must set the
'root' account Passphrase to a secure value.

This Passphrase can be reset at a later date by a Security
Officer User.

Passphrases must be at least 8 characters and at most 64
characters in length.

Passphrases must not contain the User's User Name.
Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter a new Passphrase for the operating system
'root' account: ********

Please re-enter the 'root' Passphrase: ********

Press Enter to continue:
Press Ctrl-c to abort.
```

2. プロンプトで、KMA の一意の識別子を入力します。

注 – QuickStart プログラムを使用して一度設定した KMA 名は、変更することができません。変更する唯一の方法は、KMA を出荷時のデフォルトにリセットして、QuickStart を再度実行することです。

---

3. プロンプトで、前述の規則を満たすように、root のパスフレーズの値を入力します。

4. 「Please re-enter the ‘root’ Passphrase:」プロンプトで、手順 3 で入力したパスフレーズを入力して Enter キーを押します。

クラスタの構成

1. プロンプトで、Enter キーを押します。次の情報が表示され、この KMA を使用して新しいクラスタを作成するか、既存のクラスタに参加するか、またはこの KMA のバックアップからクラスタを復元できることが示されます。

```
You can now use this KMA to create a new Cluster, or you can have
this KMA join an existing Cluster.  You can also restore a backup
to this KMA or change the KMA Version.

Please choose one of the following:
(1) Create New Cluster
(2) Join Existing Cluster
(3) Restore Cluster from Backup

Please enter your choice: 1

Create New Cluster
```

2. プロンプトで、1、2、または 3 を入力して Enter キーを押します。

1 を入力した場合は、31 ページの「鍵分割資格の入力」へ進みます。

2 を入力した場合は、37 ページの「既存のクラスタへの参加」へ進みます。

3 を入力した場合は、40 ページの「クラスタのバックアップからの復元」へ進みます。

鍵分割資格の入力

鍵分割資格のユーザー ID とパスフレーズは、それぞれのユーザー ID とパスフレーズを所有する各個人が入力するようにしてください。この情報を 1 人が収集して入力することは、鍵分割資格を持つことの目的にそぐいません。

鍵分割資格を持つ全メンバーがこの時点で情報を入力することが現実的ではない場合には、ここで資格の単純な設定を入力し、あとで KMS Manager で完全な資格を入力します。

ただし、このようにすると、セキュリティー上のリスクが生じます。単純な鍵分割資格を使用してコアセキュリティーバックアップを作成した場合は、その後バックアップの復元に使用される可能性があります。

1. 「Please enter your choice:」プロンプトで、1 を入力します。次の情報が表示されます。

```
The Key Split credentials are used to wrap splits of the Core
Security Key Material which protects Data Unit Keys.

When Autonomous Unlocking is not enabled, a quorum of Key Splits
must be entered in order to unlock the KMA and allow access to
Data Unit Keys.

A Key Split credential, consisting of a unique User Name and
Passphrase, is required for each Key Split.

The Key Split Size is the total number of splits that will
be generated.

This number must be greater than 0 and can be at most 10.


Please enter the Key Split Size: 1


The Key Split Threshold is the number of Key Splits required to
obtain a quorum.

Please enter the Key Split Threshold: 2

Please enter the Key Split User Name #1: user1

Passphrases must be at least 8 characters and at most 64
characters in length.

Passphrases must not contain the User's User Name.

Passphrases must contain characters from 3 of 4 character classes
(uppercase, lowercase, numeric, other).

Please enter Key Split Passphrase #1: ********

Please re-enter Key Split Passphrase #1: ********

Press Enter to continue:

Press Ctrl-c to abort.
```

注:

- 鍵分割サイズと鍵分割しきい値は、あとで KMS Manager を使用して変更できます。
- セキュリティーを確保するために、承認ユーザーのみがユーザー ID とパスフレーズを入力するようにしてください。これらの項目も、QuickStart プログラムの実行後に変更できます。

2. 「Please enter the Key Split Size:」プロンプトで、生成する鍵分割資格数を入力して Enter キーを押します。

3. 「Please enter the Key Split Threshold:」プロンプトで、定足数を得るために必要な鍵分割数を入力して Enter キーを押します。

4. 「Please enter the Key Split User Name #1:」プロンプトで、最初の鍵分割ユーザーのユーザー名を入力して Enter キーを押します。

5. 「Please enter Key Split Passphrase #1:」プロンプトで、最初の鍵分割ユーザーのパスフレーズを入力して Enter キーを押します。

6. 「Please re-enter Key Split Passphrase #1:」プロンプトで、直前に入力したものと同じパスフレーズを入力して Enter キーを押します。

7. 手順 4 ～手順 6 を繰り返し、選択した鍵分割サイズに対応するユーザー名とパスフレーズをすべて入力します。

注 – 鍵分割のユーザー名とパスフレーズは、KMA の管理を目的として作成されたほかのユーザーアカウントとは独立しています。

初期セキュリティー責任者ユーザー資格の入力

1. 「Press Enter to continue:」プロンプトで、Enter キーを押します。次の情報が表示されます。

```
The Initial Security Officer User is the first User that can
connect to the KMA via the KMS Manager.  This User can subsequently
create additional Users and administer the system.

Please enter a Security Officer User Name: SecOfficer

A Passphrase is used to authenticate to the KMA when a connection
is made via the KMS Manager.
Passphrases must be at least 8 characters and at most 64 characters
in length.
Passphrases must not contain the User's User Name.

Passphrases must contain characters from 3 of 4 character classes
(uppercase, lowercase, numeric, other).

Please enter the Security Officer Passphrase: ********

Please re-enter the Security Officer Passphrase:
********


Press Enter to continue:
Press Ctrl-c to abort.
```

注 – セキュリティー責任者のこの初期ユーザーアカウントは、KMS Manager を使用した KMA へのログインに使用されます。

---

2. プロンプトで、セキュリティー責任者のユーザー名を入力して Enter キーを押します。次の情報が表示されます。
3. プロンプトで、セキュリティー責任者のパスフレーズを入力して Enter キーを押します。
4. 「Please re-enter the Security Officer Passphrase:」プロンプトで、同じパスフレーズを再入力して Enter キーを押します。

重要 – すべての KMA は独自のパスフレーズを持ちます。これは、ユーザーやエージェントに割り当てられたものとは関係ありません。クラスタ内の最初の KMA には、ランダムなパスフレーズが割り当てられます。この KMA の証明書の期限が切れ、クラスタ内の別の KMA からその実体の証明書を取り出す場合は、KMS Manager を使用して、パスフレーズを既知の値に設定する必要があります。手順については、89 ページの「KMA のパスフレーズの設定」を参照してください。

自律ロック解除設定の指定

注意 – 自律ロック解除を使用可能にすると、より便利になり、KMS クラスタの可用性が向上しますが、セキュリティー上のリスクも生じます。自律ロック解除が使用可能である場合は、完全な起動や、格納されている鍵の復号化を行うために必要な情報が、電源が入っていない KMA に保持されている必要があります。

このため、攻撃者は盗難した KMA の電源を入れ、KMA からの鍵の抽出を開始できます。鍵の抽出は簡単ではありませんが、知識が豊富な攻撃者は KMA からすべての鍵をダンプできます。暗号化を使用した攻撃は必要ありません。

自律ロック解除が使用不可である場合、攻撃者は、盗難した KMA から鍵を抽出するために、暗号化を使用した攻撃が必要になります。

自律ロック解除を使用可能にすることを選択する場合は、その前に、考えられる攻撃とセキュリティーに関する考慮事項について慎重に検討するようにしてください。

1. 「Press Enter to continue:」プロンプトで、Enter キーを押します。次の情報が表示されます。

```
When Autonomous Unlocking is DISABLED, it is necessary to
UNLOCK the KMA using a quorum of Key Split Credentials
EACH TIME the KMA starts before normal operation of the
system can continue.  Agents may NOT register Data Units
with or retrieve Data Unit Keys from a locked KMA.

When Autonomous Unlocking is ENABLED, the KMA will
automatically enter the UNLOCKED state each time the
KMA starts, allowing it to immediately service Agent requests.

Do you wish to enable Autonomous Unlocking? [y/n]: y
```

注 – 自律ロック解除機能を使用すると、KMS Manager を使用して定足数のパスフレーズを入力する必要はなく、ハードリセットまたはソフトリセット後の KMA を完全動作状態にすることができます。このオプションは、あとで KMS Manager で変更できます。

2. プロンプトで、y または n を入力して Enter キーを押します。

KMA の時刻の同期

クラスタ内の KMA のクロックは、同期がとれている**必要があります**。初期状態では、すべての KMA で UTC 時刻 (協定世界時) が使用されています。

KMS Manager を使用して、日時の設定を現地時間に変更することもできます。

```
KMAs in a Cluster must keep their clocks synchronized. Specify an
NTP server if one is available in your network. Otherwise, specify
the date and time to which the local clock should be set.

Please enter the NTP Server Hostname or IP Address (optional):
ntp.example.com

Press Enter to continue:
Initializing new cluster...

New KMS cluster has been created.

Press Enter to continue:
Key Management System Version Build xyz
_____________________________________________________________
KMA initialization complete!

You may now connect to the KMA via the KMS Manager in order to
continue with KMS configuration.

Press Enter to exit:

Key Management System Version Build xyz (KMA-1)
_____________________________________________________________

Please enter your User Name:
```

1. 使用しているネットワーク環境で NTP サーバーが使用可能である場合は、「`Please enter the NTP Server Hostname or IP Address (optional):`」プロンプトで、NTP サーバーのホスト名または IP アドレスを入力します。
2. NTP サーバーが使用可能でない場合は、Enter キーを押します。次に、「`Please enter the date and time for this KMA`」プロンプトで、指定されたいずれかの形式で日時を入力するか、または Enter キーを押して表示された日時を使用します。
3. プロンプトで、Enter キーを押します。KMA の初期化が完了します。
4. 終了するには、Enter キーを押します。QuickStart プログラムが終了し、ログインプロンプトが表示されます (258 ページの「KMA へのログイン」を参照)。KMS Manager との通信に必要な最小システム構成が KMS に構築されました。
5. 次の手順として、KMS Manager を使用してクラスタに接続します。手順については、71 ページの「クラスタへの接続」を参照してください。

既存のクラスタへの参加

重要 – この作業を行う前に、セキュリティー責任者は、KMS Manager を使用して KMS クラスタにログインして KMA を作成しておく必要があります。85 ページの「KMA の作成」を参照してください。

KMA の初期化プロセスで指定した KMA 名 (29 ページの「KMA の初期化」を参照) が、KMA の作成時に入力した KMA 名と一致している必要があります。

新しい KMA を既存のクラスタに加えるには、次の手順を実行します。

1. KMA の初期化プロセス (29 ページの「KMA の初期化」を参照) が完了したら、プロンプトで Enter キーを押します。

   次の情報が表示され、この KMA を使用して新しいクラスタを作成するか、既存のクラスタに参加するか、またはこの KMA のバックアップからクラスタを復元できることが示されます。

```
You can now use this KMA to create a new Cluster, or you can have
this KMA join an existing Cluster.  You can also restore a backup
to this KMA or change the KMA Version.

Please choose one of the following:
(1) Create New Cluster
(2) Join Existing Cluster
(3) Restore Cluster from Backup

Please enter your choice: 2

Join Existing Cluster
```

2. 「Please enter your choice:」プロンプトで、2 を入力します。次の情報が表示されます。

```
Join Existing Cluster
-------------------------------------------------------------
Press Ctrl-c to abort.

In order to join a Cluster, the KMA must contact
another KMA which is already in the Cluster.

Please enter the Management Network IP Address or Host Name of an
existing KMA in the cluster: 129.80.60.172

Please enter this KMA's Passphrase:********

Press Enter to continue:

This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #1: user1

Please enter Key Split Passphrase #1: ********

Press Enter to continue:

Joining cluster...

KMA has joined the KMS cluster.

Press Enter to continue:

Key Management System Version xxx
-------------------------------------------------------------

KMA initialization complete!

You may now connect to the KMA via the KMS Manager
in order to continue with KMS configuration.

Press Enter to exit:
```

注 – この新しい KMA がクラスタ内の既存の KMA と通信できるようにするには、KMS Manager を使用して、既存の KMA のデータベースにこの KMA のエントリを作成する必要があります。手順については、85 ページの「KMA の作成」を参照してください。

---

3. プロンプトで、既存のクラスタ内のいずれかの KMA のネットワークアドレスを入力して Enter キーを押します。

4. プロンプトで、その KMA のパスフレーズを入力して Enter キーを押します。

5. 最初の KMA の初期鍵分割ユーザー名を入力します。
6. その鍵分割ユーザーのパスフレーズを入力して Enter を押します。

重要 – 鍵分割ユーザー名およびパスフレーズは、慎重に入力してください。入力ミスがあると、この処理は失敗し、具体的な内容が示されないエラーメッセージが表示されます。攻撃者に対して公開される情報を制限するために、どの鍵分割ユーザー名またはパスフレーズが間違っているかについてのフィードバックは提供されません。

---

7. 手順 5と手順 6を繰り返し、定足数を形成するために十分な数の鍵分割ユーザーの名前とパスワードを入力します。
8. 次の「`Please enter Key Split User Name`」プロンプトで、Enter キーを押します。空白の名前を入力して、終了します。

   初期化が完了します。
9. 終了するには、Enter キーを押します。QuickStart プログラムが終了し、ログインプロンプトが表示されます (258 ページの「KMA へのログイン」を参照)。KMS Manager との通信に必要な最小システム構成が KMS に構築されました。
10. 次の手順として、KMS Manager を使用してクラスタに接続します。手順については、71 ページの「クラスタへの接続」を参照してください。

クラスタのバックアップからの復元

このオプションを使用すると、セキュリティー責任者アカウントを作成できます。このアカウントは、KMS Manager を使用して KMA にバックアップイメージを復元する場合に使用できます。ハードディスクの損傷など、KMA で障害が発生した場合は、バックアップを使用して KMA の構成を復元できます。ただし、出荷時のデフォルト状態に復元した KMA は、既存のクラスタに容易に加えることができ、クラスタピアから複製更新を受信してデータベースを構築することができるため、このような操作は通常は不要です。それでも、KMA のバックアップからの復元は、クラスタ内のすべての KMA に障害が発生した場合に役立ちます。

注 – バックアップを作成しておく必要があります。KMS Manager を使用したバックアップの作成手順については、251 ページの「バックアップの作成」を参照してください。

バックアップイメージを復元するには、次の手順を実行します。

1. KMA の初期化プロセス (29 ページの「KMA の初期化」を参照) が完了したら、プロンプトで Enter キーを押します。

   次の情報が表示され、この KMA を使用して新しいクラスタを作成するか、既存のクラスタに参加するか、またはこの KMA のバックアップからクラスタを復元できることが示されます。

```
You can now use this KMA to create a new Cluster, or you can have
this KMA join an existing Cluster.  You can also restore a backup
to this KMA or change the KMA Version.

Please choose one of the following:
(1) Create New Cluster
(2) Join Existing Cluster
(3) Restore Cluster from Backup

Please enter your choice: 3

Restore Cluster from Backup
```

2. 「Please enter your choice:」プロンプトで、3 を入力します。次の情報が表示されます。

```
Initial Restore Cluster From Backup
Enter Initial Security Officer User Credentials
------------------------------------------------------------
Press Ctrl-c to abort.

The initial Security Officer User is the first User that
can connect to the KMA via the KMS Manager. This User can
subsequently create additional Users and administer
the system.

Please enter a Security Officer User ID: SO1

A Passphrase is used to authenticate to the KMA when
a connection is made via the KMS Manager.

Passphrases must be at least 8 characters and at most 64
characters in length.
```

3. プロンプトで、セキュリティー責任者のユーザー名を入力して Enter キーを押します。
4. プロンプトで、セキュリティー責任者のパスフレーズを入力して Enter キーを押します。

5. 「Please re-enter the Security Officer's Passphrase:」プロンプトで、手順 4 で入力したパスフレーズを再入力して Enter キーを押します。

```
Set Time Information
------------------------------------------------------------

Press Ctrl-c to abort.

KMAs in a Cluster must keep their clocks synchronized.
Specify an NTP server if one is available in your network.
Otherwise, specify the date and time to which the local clock
should be set.

Please enter the NTP Server Hostname or IP Address (optional):

The date and time for this KMA must be specified in ISO 8601 format
including a time zone.  Here are some valid ISO 8601 format
patterns:

    YYYY-MM-DDThh:mm:ssZ
    YYYY-MM-DD hh:mm:ssZ
    YYYY-MM-DDThh:mm:ss-0600
    YYYY-MM-DD hh:mm:ss-0600
    YYYY-MM-DDThh:mm:ss+02:00
    YYYY-MM-DD hh:mm:ss+02:00

Please enter the date and time for this KMA [2007-09-17
22:32:53.698Z]: 2007-09-17 22:33:00-0600

Press Enter to continue:


The KMA is now ready to be restored.

Press Enter to continue:
```

6. 使用しているネットワーク環境で NTP サーバーが使用可能である場合は、「Please enter the NTP Server Hostname or IP Address (optional):」プロンプトで、NTP サーバーのホスト名または IP アドレスを入力します。

7. NTP サーバーが使用可能でない場合は、Enter キーを押します。次に、「Please enter the date and time for this KMA」プロンプトで、指定されたいずれかの形式で日時を入力するか、または Enter キーを押して表示された日時を使用します。

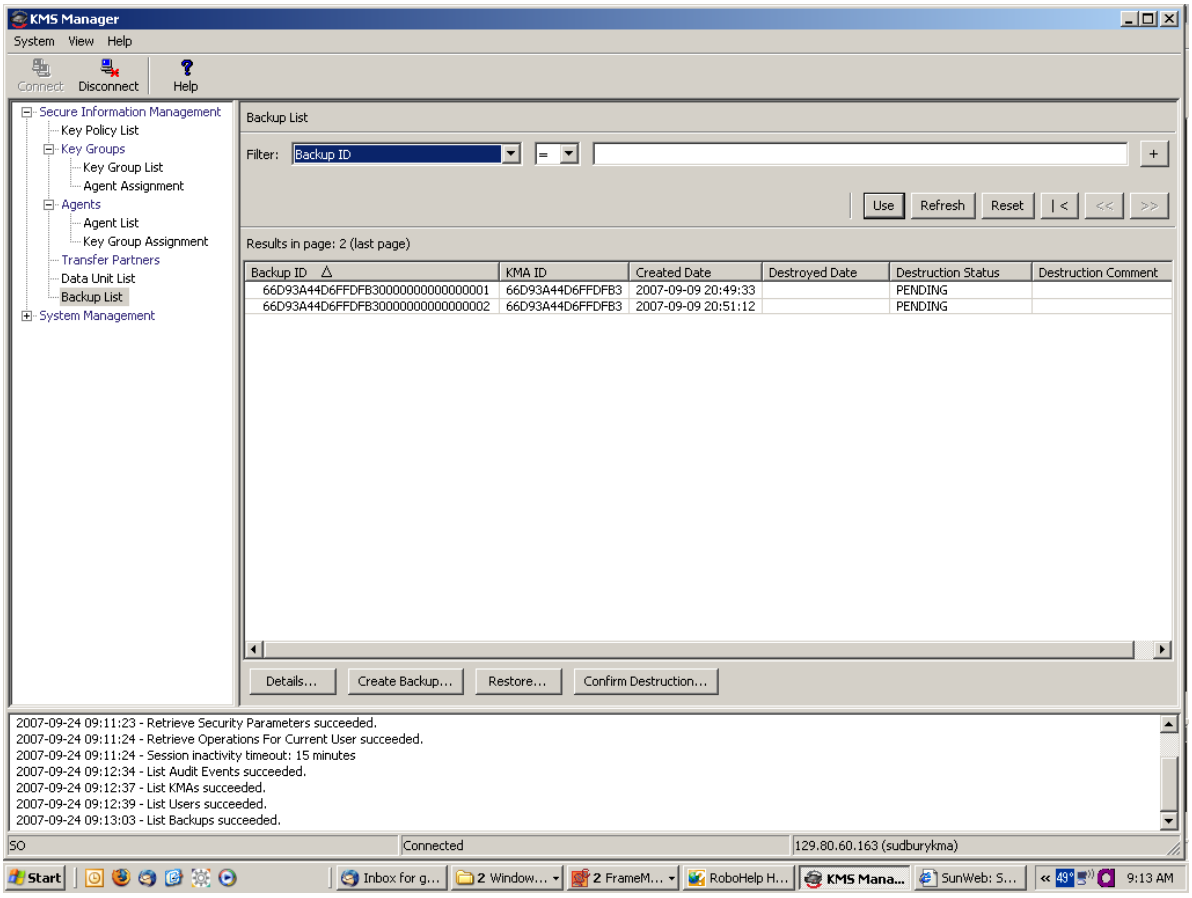
   日時が正確であることを確認します。鍵のライフサイクルは時間間隔に基づいており、鍵の元の作成時刻はバックアップに格納されます。交換用の KMA で時刻が正確に設定されていることは、意図したとおりの鍵ライフサイクルを保持するために必要不可欠です。

8. プロンプトで、Enter キーを押します。次の情報が表示され、初期化が完了したことが示されます。

```
KMA Management System Version xxx
------------------------------------------------------------

KMA initialization complete!

You may now connect to the KMA via the KMS Manager
in order to continue with KMS configuration.

Press Enter to exit:
```

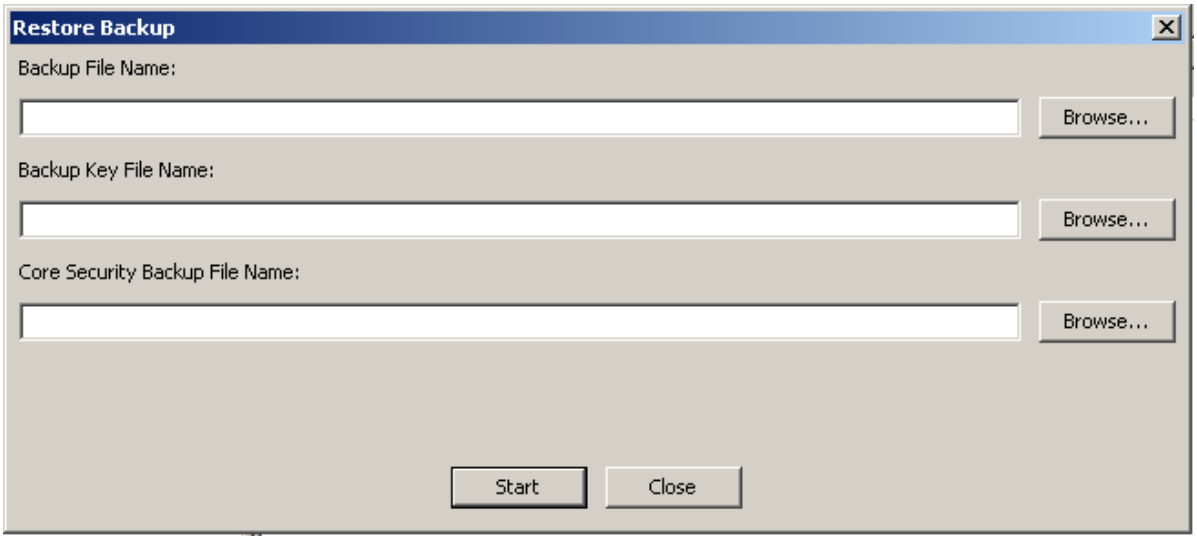
9. 終了するには、Enter キーを押します。QuickStart プログラムが終了し、ログインプロンプトが表示されます。

10. セキュリティー責任者として KMS Manager にログインし、「Backup List」を選択します。「Backup List」画面で、「Restore」ボタンを選択し、バックアップをアップロードして KMA に復元します。

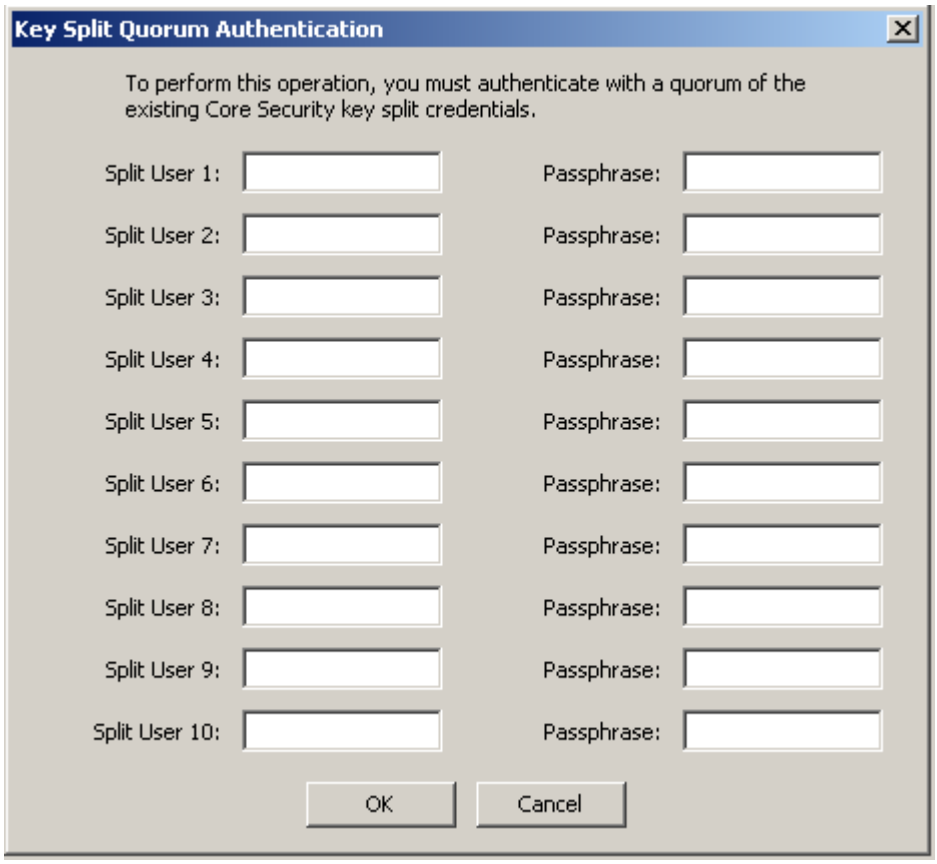


11. 復元処理を完了するために、KMS Manager によって、バックアップ鍵ファイルに対応するバックアップファイル、バックアップ鍵ファイル、およびコアセキュリティーバックアップファイルの入力が要求されます。

    バックアップ鍵ファイルとバックアップファイルは一致している必要がありますが、コアセキュリティーバックアップファイルは任意のものを使用できます。



12. 次に、KMS Manager によって定足数の鍵分割ユーザーの入力が要求されます。このユーザーは、コアセキュリティーバックアップが実行されたときに有効だった鍵分割資格ユーザーである必要があります。



復元が完了すると、バックアップ (コアセキュリティーバックアップではない) の完了時に有効だった鍵分割資格が復元されます。

重要 – 鍵分割ユーザー名およびパスフレーズは、慎重に入力してください。入力ミスがあると、「既存のクラスタへの参加」処理は失敗し、具体的な内容が示されないエラーメッセージが表示されます。攻撃者に対して公開される情報を制限するために、どの鍵分割ユーザー名またはパスフレーズが間違っているかについてのフィードバックは提供されません。

---

13. 復元処理が完了すると、新しいクラスタが作成されます。

第3章

KMS Manager の使用法

この章では、KMS Manager と次の手順について説明します。

- KMS Manager ソフトウェアのインストール
- KMS Manager の起動
- KMS Manager ソフトウェアのアンインストール

ここでは、メニューや区画についても簡単に説明します。

KMS Manager について

KMS Manager は、KMA のクライアントとして機能するアプリケーションです。KMS Manager は、KMA の設定、制御、および監視に使用できます。ユーザーは、割り当てられているロールに応じて、さまざまな操作を実行できます。

KMS Manager ソフトウェアのインストール

KMS Manager ソフトウェアをインストールするには、次の手順を実行します。

1. 次の URL で、Sun StorageTek Customer Resource Center (CRC) Web サイトにアクセスします。

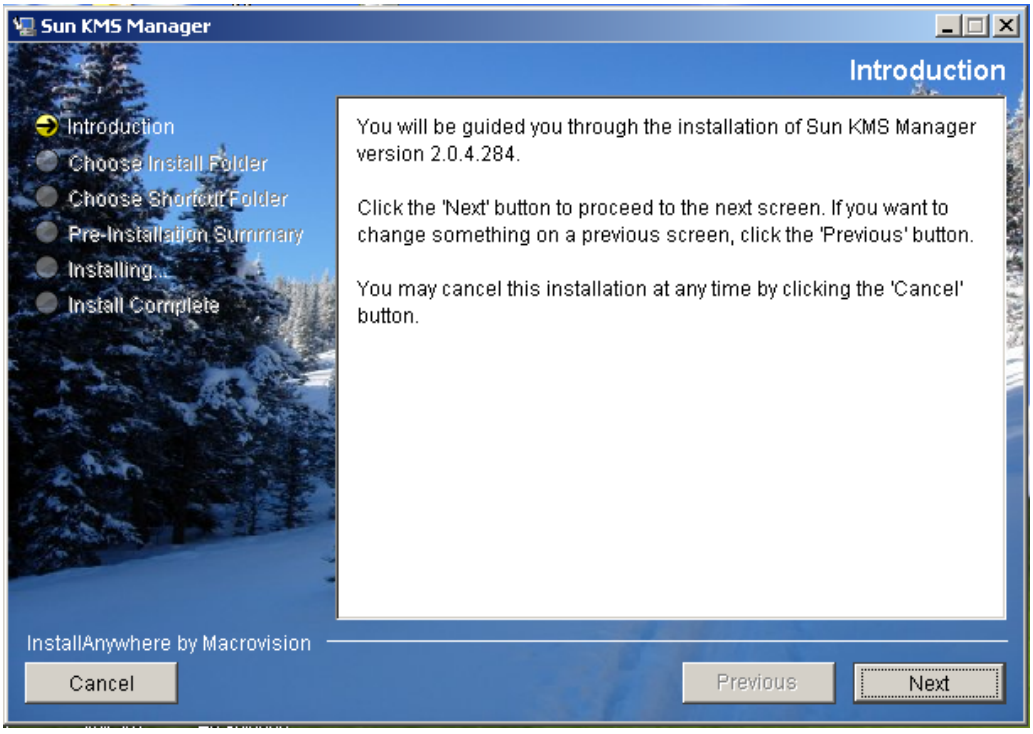
   ```
   http://www.support.storagetek.com/crc_home.html
   ```

2. CRC にログインし、「Code Downloads」領域に移動します。「KMS」リンクをクリックし、コードをダウンロードします。

- Windows の場合は、install.exe をダブルクリックします。
- Solaris の場合は、シェルを開き、cd コマンドを使用して、インストーラのダウンロード先ディレクトリへ移動します。プロンプトで、次のように入力します。

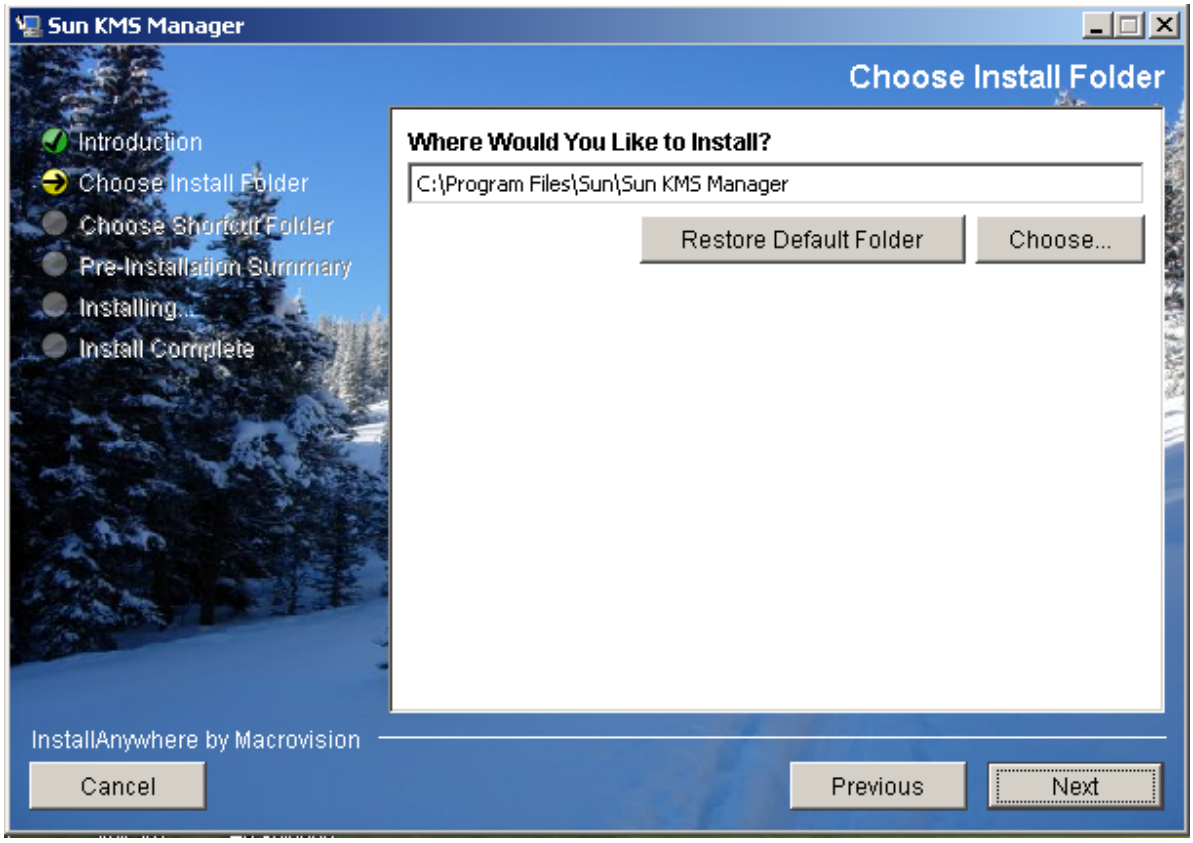
  ```
  sh ./install.bin
  ```

「Introduction」ウィンドウが表示されます。



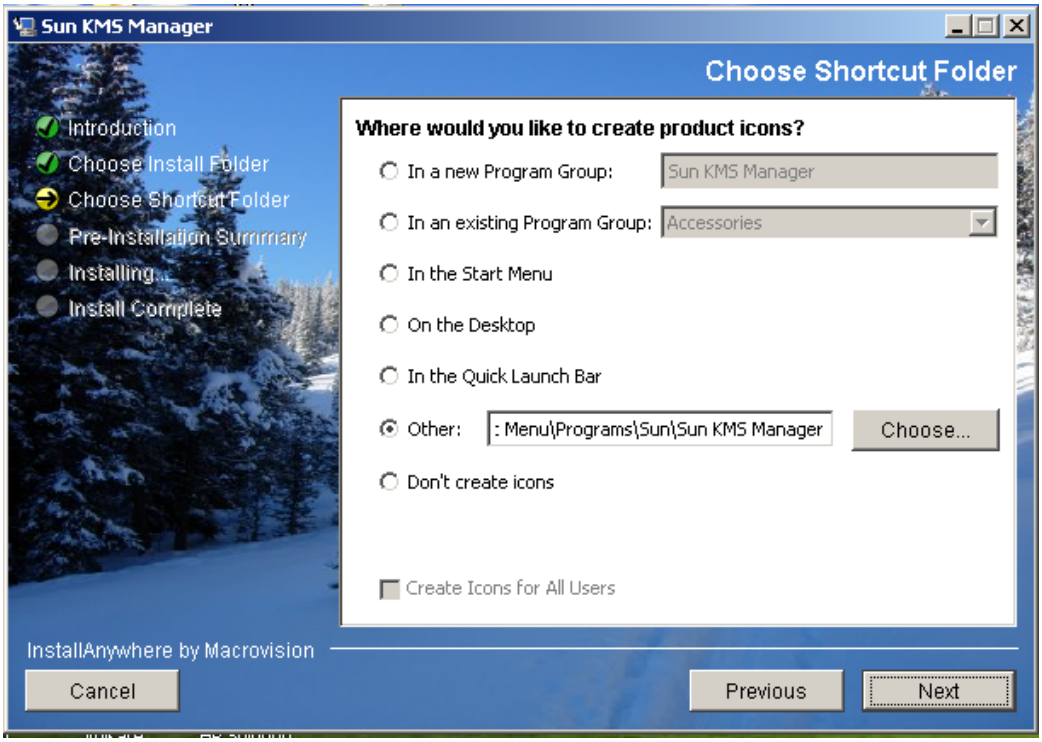
3. 「Next」を選択します。

4. 「Choose Install Folder」ウィンドウが表示されます。



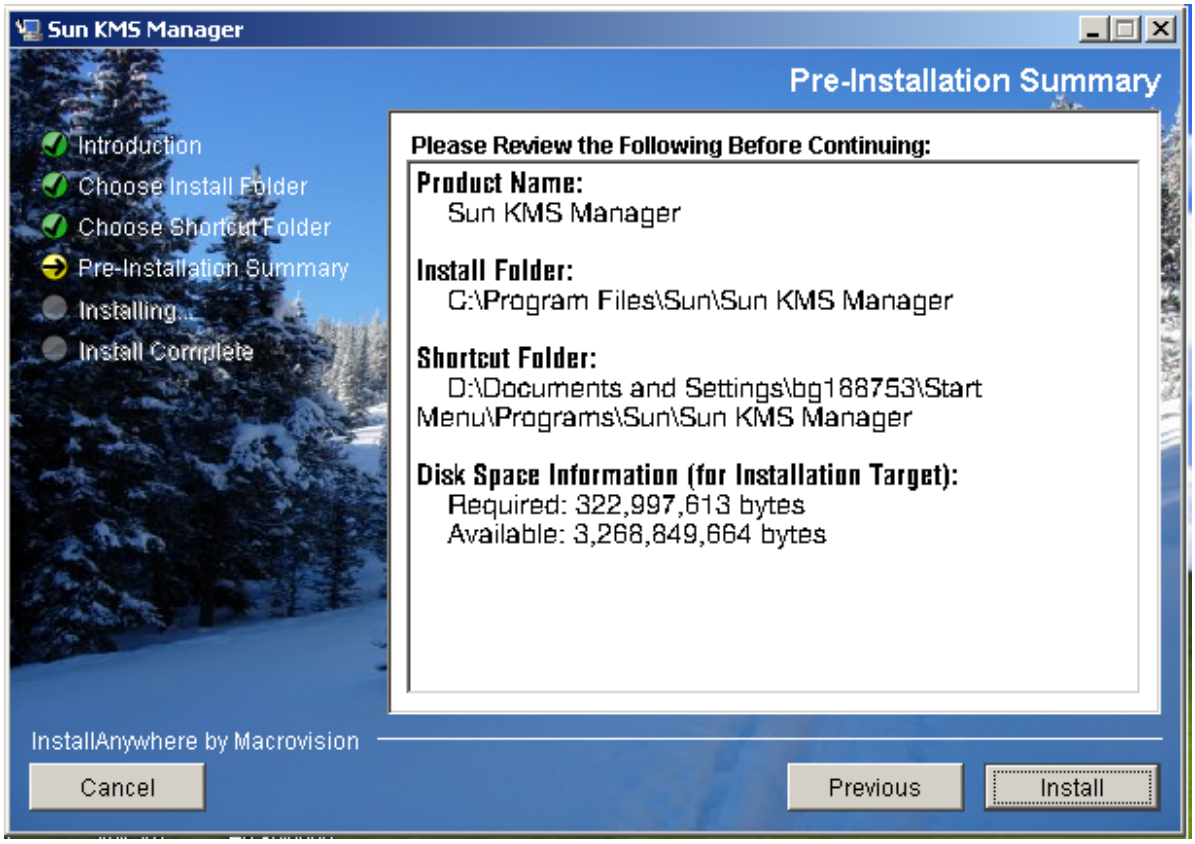
5. そのまま「Next」をクリックしてデフォルトのフォルダを選択するか、または独自のインストールフォルダを指定して「Next」をクリックします。

6. 「Choose Shortcut Folder」ウィンドウが表示されます。ここでは、必要な場所に製品アイコンを作成できます。

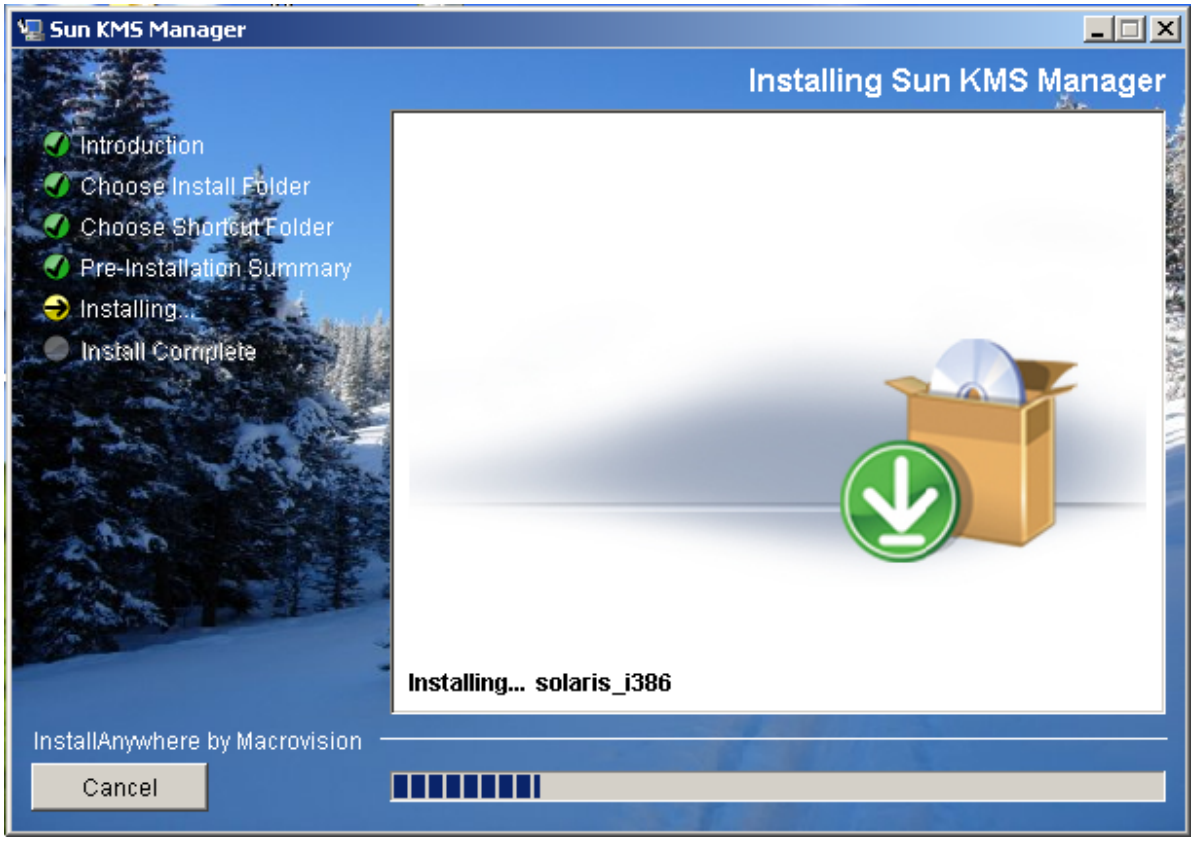


7. 選択してから「Next」をクリックします。

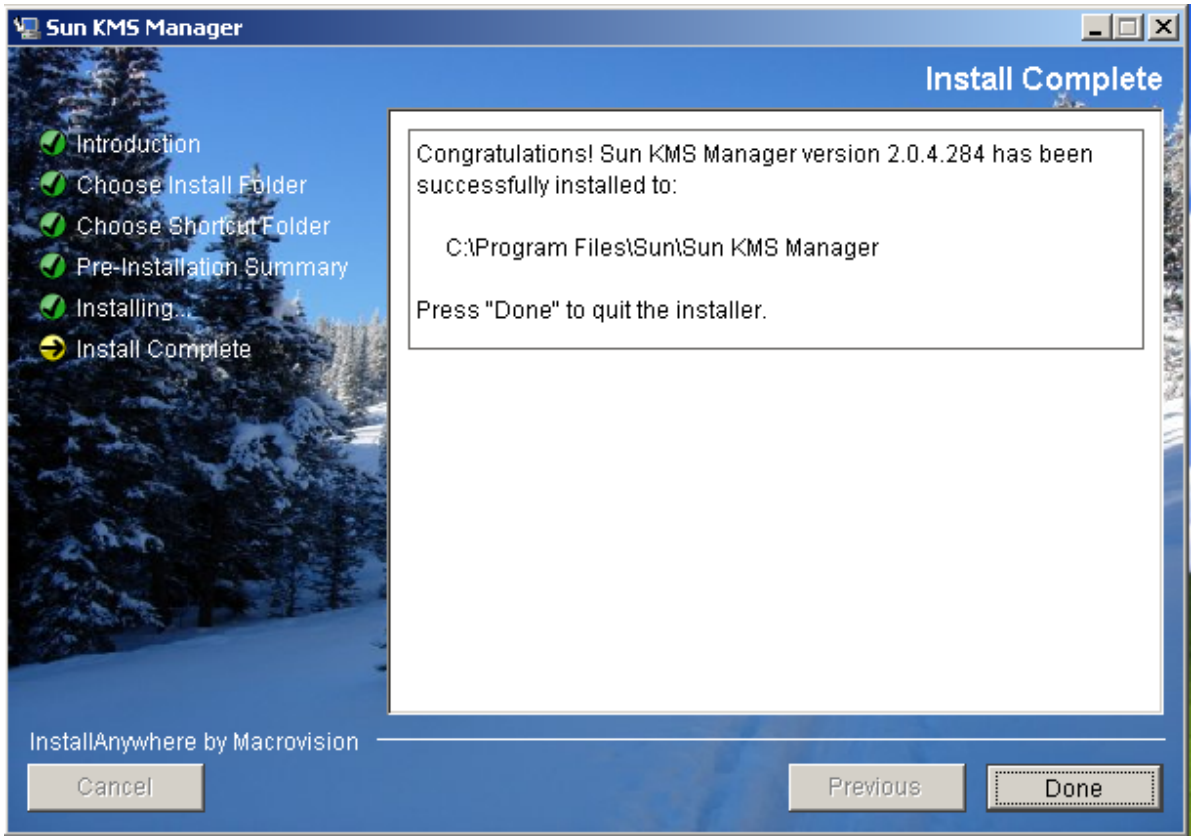
8. 「Pre-Installation summary」画面が表示されます。



9. 「Install」を選択して KMS Manager をインストールするか、または「Previous」を選択して設定を修正します。


Sun KMS Manager
Installing Sun KMS Manager
Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
Installing... solaris_i386
InstallAnywhere by Macrovision
Cancel

10. これで、イントール処理は完了です。「Done」を選択して終了します。



KMS Manager の起動

KMS Manager の起動には、使用している環境に応じて次の 2 つの方法を使用できます。

- Windows での起動
- Solaris での起動

Windows での KMS Manager の起動

インストールプログラムでショートカットを作成するように指定した場合は、そのショートカットをダブルクリックすると、KMS Manager アプリケーションが起動します。

ショートカットを作成しなかった場合は、Windows エクスプローラを起動し、KMS Manager のインストール先へ移動して KMS_Manager.exe を起動します。

Solaris での KMS Manager の起動

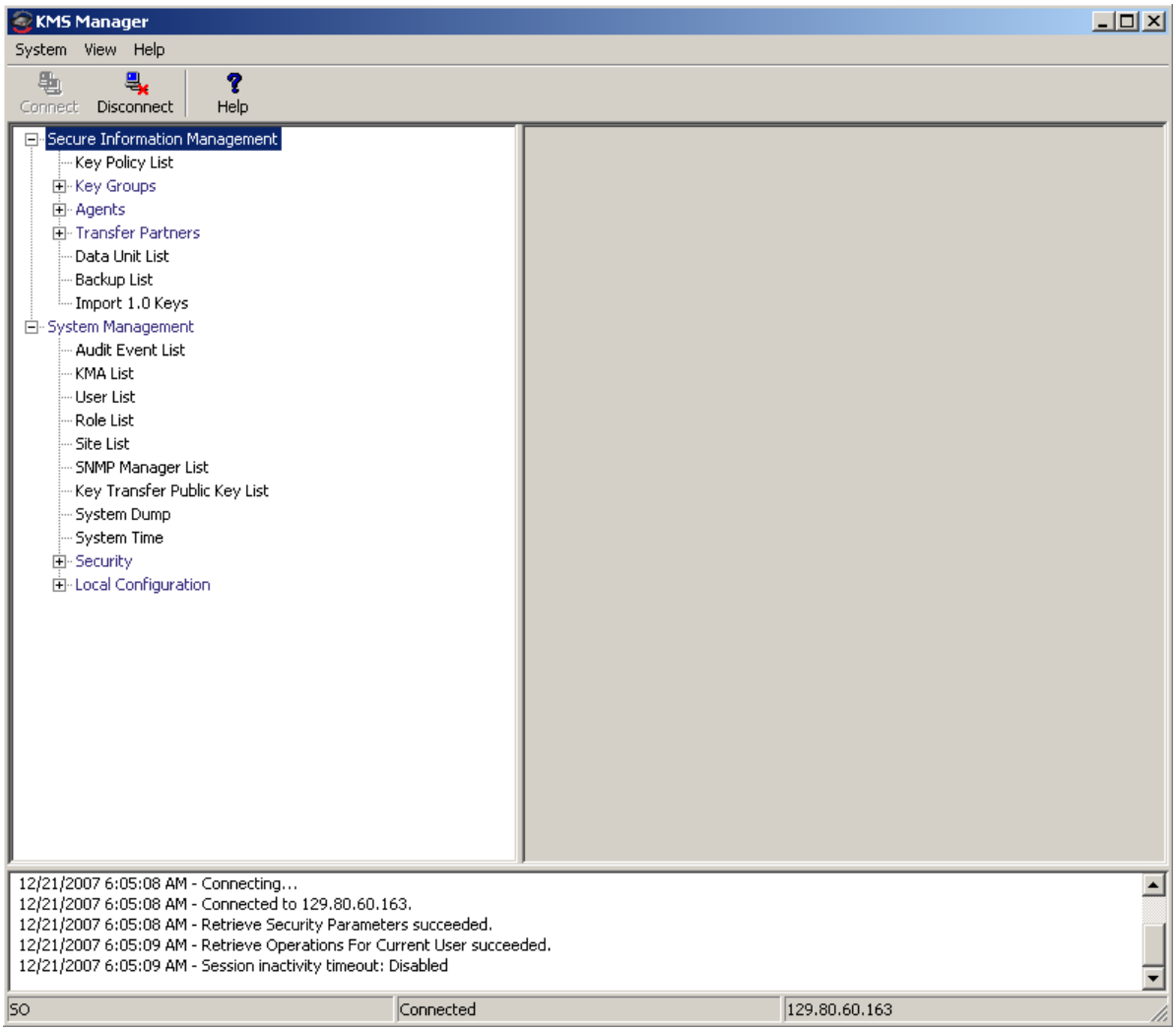
Windows の場合と同様に、インストールプログラムでショートカットを作成するように指定できます。たとえば、ホームディレクトリにショートカットを作成した場合は、シェルプロンプトで次のように入力して起動することができます。

```
~/KMS_Manager
```

または、KMS Manager のインストール先へ移動し、KMS_Manager.exe を起動します。

KMS Manager GUI の概要

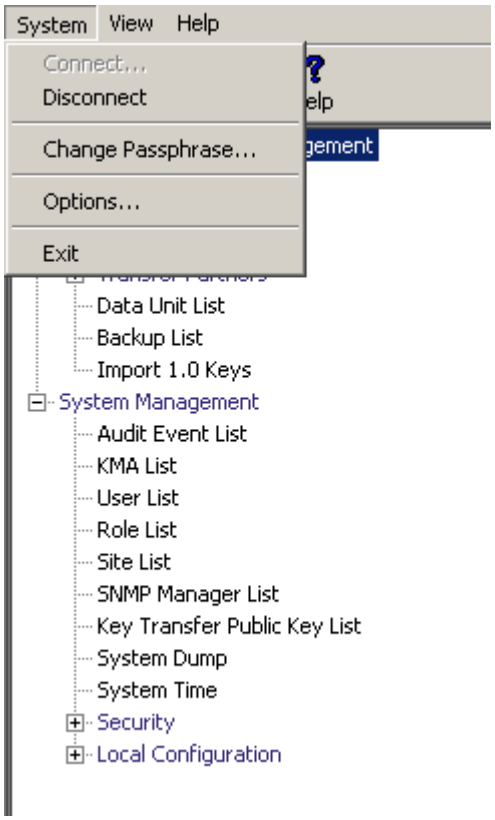
次の図に、KMS Manager GUI とサンプルメニューを示します。



KMS Manager GUI には、「System」、「View」、「Help」の便利な各メニューがあります。該当するアクションバー項目をクリックするとメニューが表示されるので、その中からメニュー項目を選択します。

ツールバーのボタンは、いくつかのメニューオプションへのショートカットを提供します。

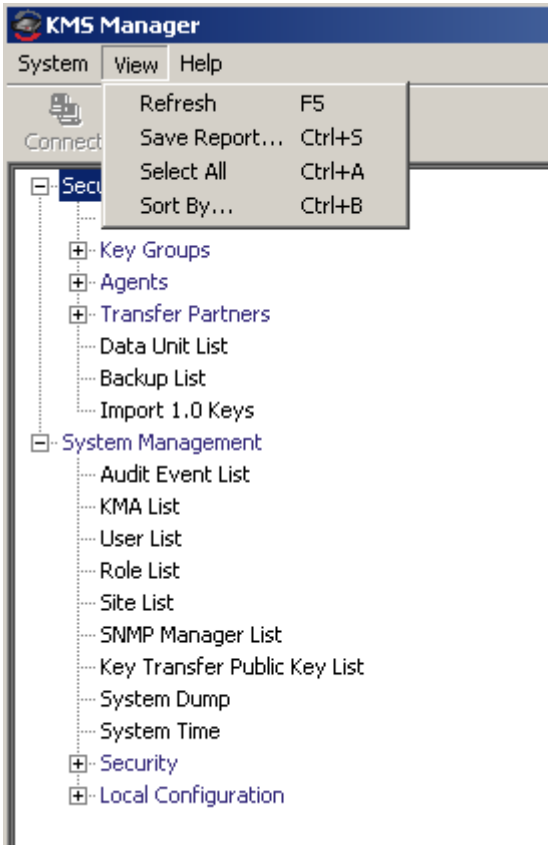
「System」メニュー



「System」メニューのオプション

- Connect...: 「Connect to Cluster」ダイアログボックスを表示します。このダイログボックスでは、事前に用意されているクラスタにプロファイルを使用して接続したり、新しいクラスタプロファイルを作成したりすることができます。
- Disconnect: 「Disconnect from KMA」ダイアログボックスを表示します。このダイアログボックスでは、KMA からの切断を行うことができます。
- Change Passphrase...: 「Change passphrase」ダイアログボックスを表示します。このダイアログボックスでは、パスフレーズを変更できます。
- Options...: 「Options」ダイアログボックスを表示します。このダイアログボックスは、各種構成設定値を指定する場合に使用します。
- Exit: KMS Manager GUI を終了します。

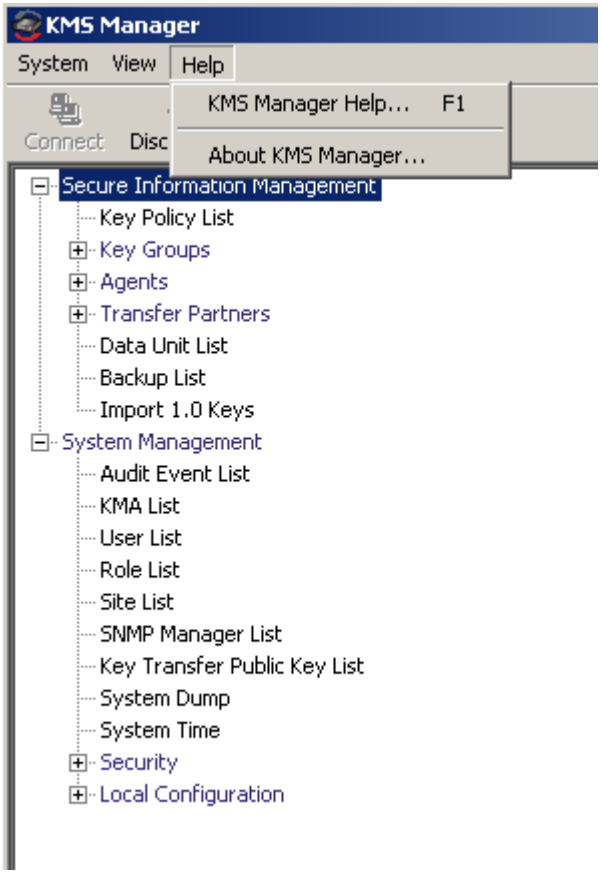
「View」メニュー



「View」メニューのオプション

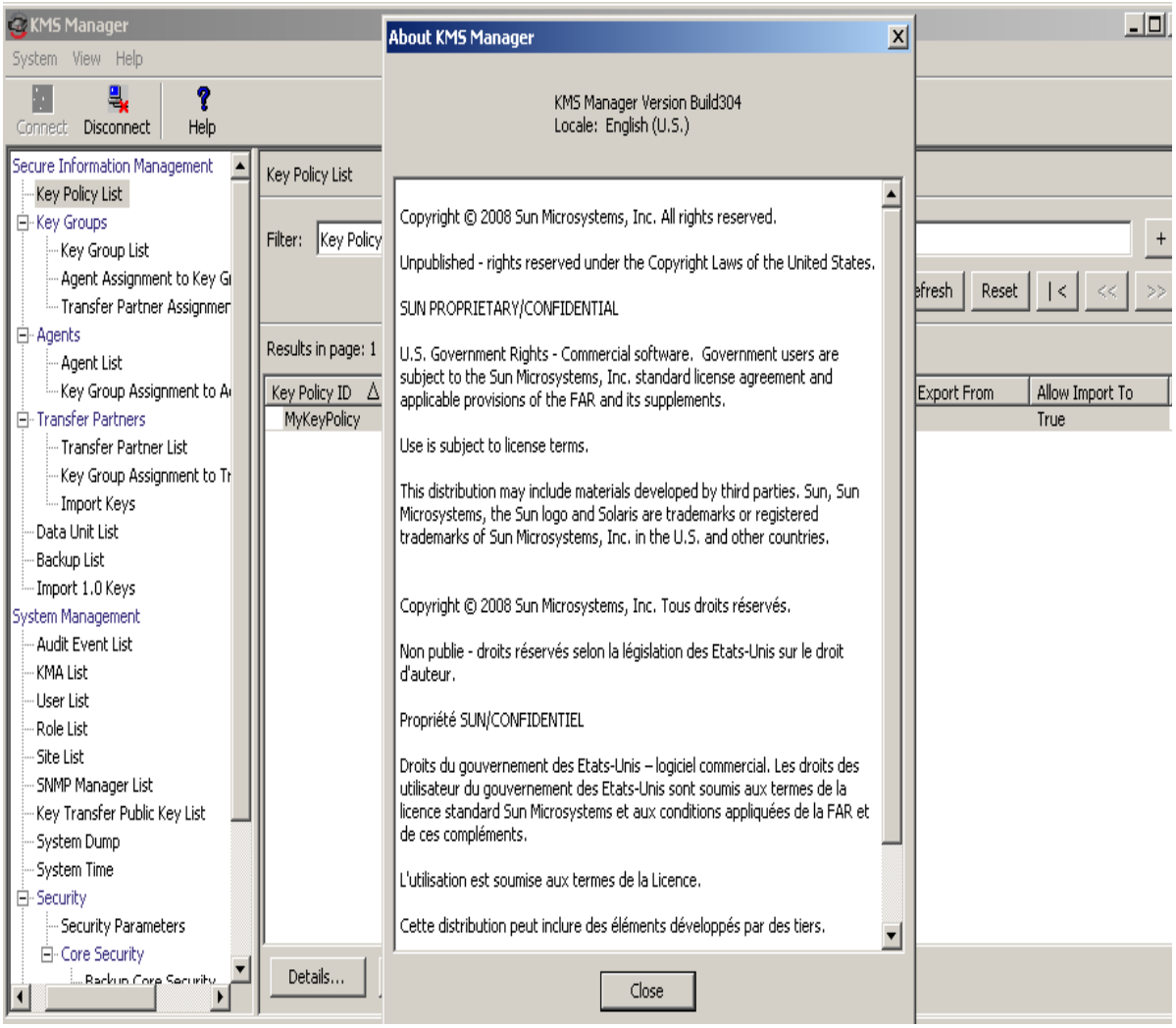
- Refresh: 画面を再表示します。
- Save Report...: 「Save Report」を使用すると、任意の「List」画面の内容を、KMS Manager が実行されているシステムにテキストファイルとしてダウンロードできます。
- Select All: 「Select All」を選択すると、「List」画面上のすべての項目が選択されます。
- Sort By: 「List」画面上の項目のリストをソートします。これは、リストの列見出しをクリックすることと同じです。

「Help」メニュー


KMS Manager
System
View
Help
KMS Manager Help... F1
About KMS Manager...
Connect
Disc
Secure Information Management
Key Policy List
Key Groups
Agents
Transfer Partners
Data Unit List
Backup List
Import 1.0 Keys
System Management
Audit Event List
KMA List
User List
Role List
Site List
SNMP Manager List
Key Transfer Public Key List
System Dump
System Time
Security
Local Configuration

「Help」メニューのオプション

- KMS Manager Help...: KMS Manager のオンラインヘルプの索引と目次を表示します。
- About KMS Manager...: KMS Manager のバージョン情報および著作権情報を表示します。このダイアログボックスを閉じるには、「Close」ボタンを選択します。



ツールバーのボタン

次の表に、KMS のツールバーボタンの説明を示します。

ボタン	説明
	「Connect to KMA」ダイアログボックスを表示します。このダイアログボックスでは、プロファイルを選択して KMA に接続することができます。
	「Disconnect from KMA」ダイアログボックスを表示します。このダイアログボックスでは、KMA からの切断を行うことができます。
	KMS のオンラインヘルプの索引と目次を表示します。

ショートカットキー

ショートカットキーを使用すると、複数のコマンドを 1 回の操作で選択できます。次のショートカットキーが使用されています。

現在の選択の切り取り	Ctrl+X
現在の選択のコピー	Ctrl+C
クリップボードの内容を現在の選択ポイントにコピー	Ctrl+V
レポートをローカルサイトに保存するためのダイアログボックスの表示	Ctrl+S

メニューアクセラレータキー

すべてのメニュー項目について、メニューアクセラレータキーがサポートされています。アクセラレータキーを表示するには、Alt キーを押したままにします。

オンラインヘルプの使用法

オンラインヘルプを使用すると、KMS に関する詳細な情報を確認できます。オンラインヘルプの使用は簡単です。トピックはさまざまな方法で表示できます。次の操作を行うことができます。

- 目次の参照
- キーワードの検索
- 索引の使用
- 前に表示したページへの移動
- トピックの印刷

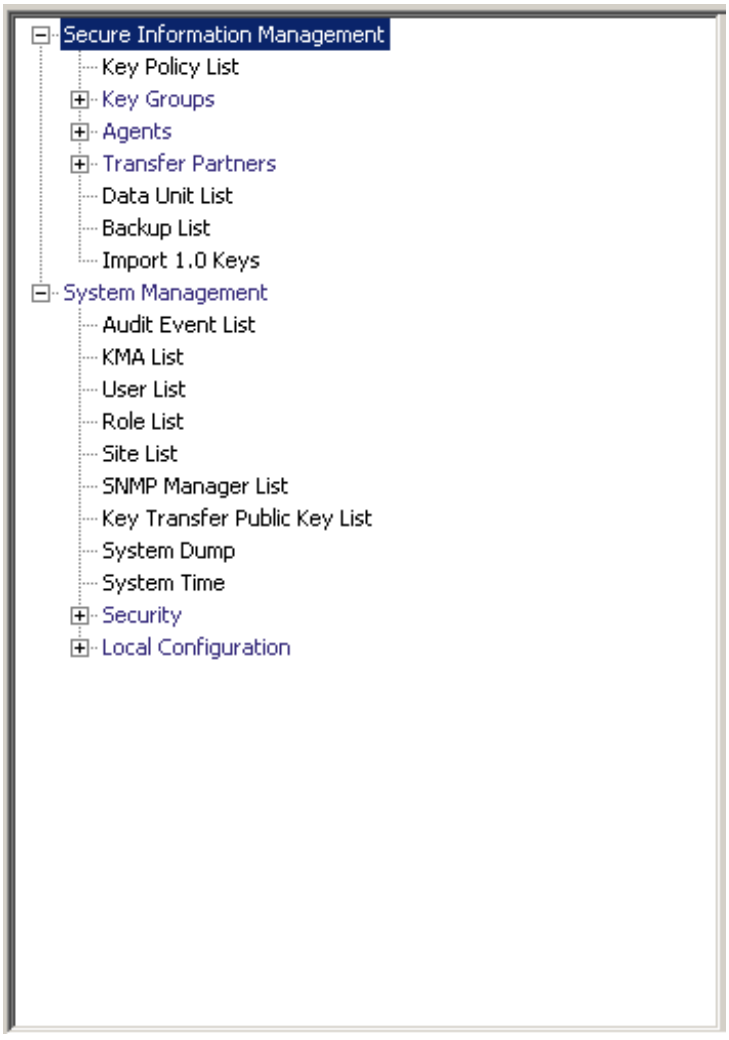
KMS Manager GUI の区画

KMS Manager GUI には、次の 3 つの区画があります。

- KMS 管理操作ツリー
- KMS 管理操作の詳細
- セッション監査ログ

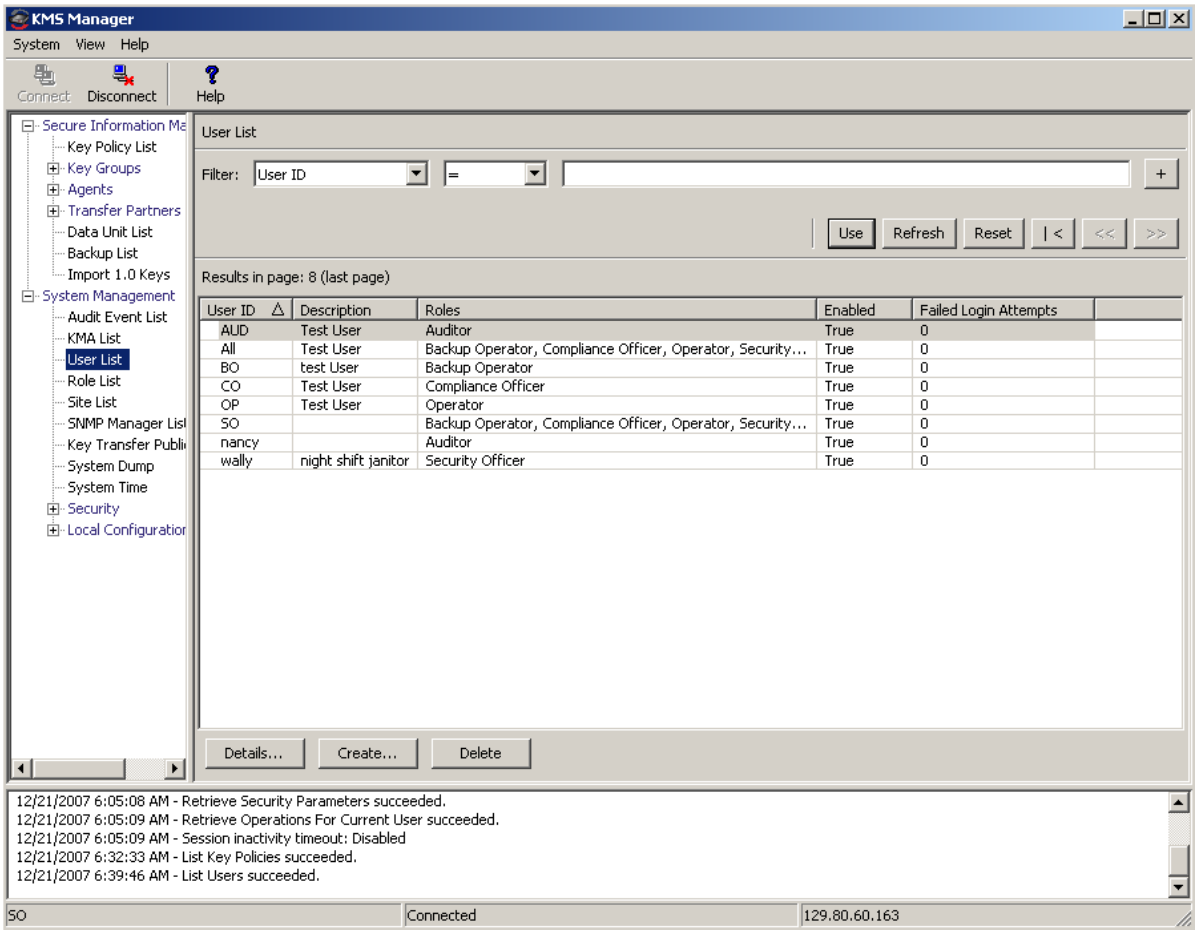
KMS 管理操作ツリー区画

KMS 管理操作ツリー区画は画面の左側にあり、ここには KMS のすべての操作機能が表示されます。このツリー区画に表示されるオプションは、割り当てられているロールに応じて異なります。次の例では、セキュリティー責任者が実行できる操作が表示されています。



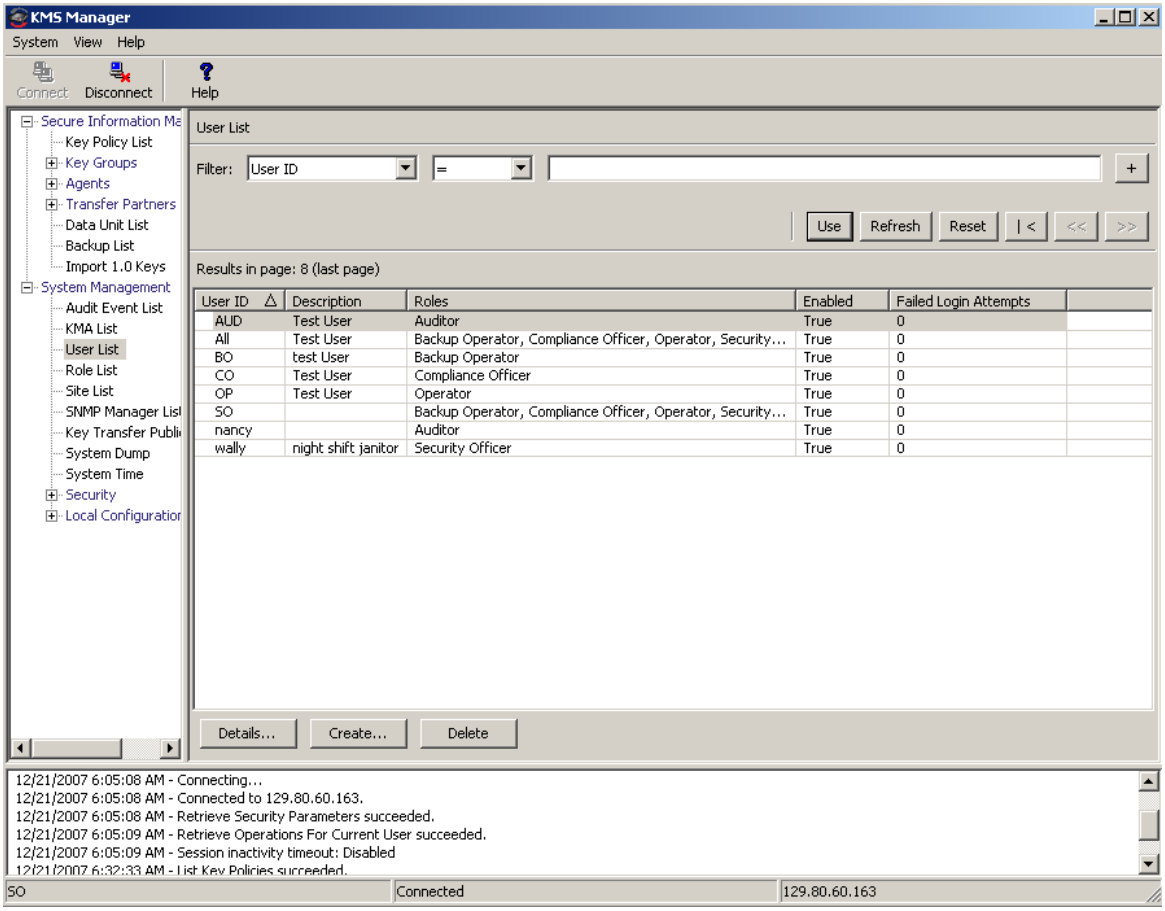
KMS 管理操作の詳細区画

操作ツリー区画の右側は、KMS Manager の管理操作の詳細区画です。ここには、操作が選択された場合に、その選択された操作に必要なコンポーネントが表示されます。リストパネルに表示された項目には、フィルタを適用できます。次に、操作ツリー区画で「System Management」メニューの「User List」メニューオプションを選択した場合の「User List」の例を示します。



セッション監査ログ区画

操作ツリー区画と操作の詳細区画の下がセッション監査ログ区画です。ここには、最近のセッションイベントのスクロール可能なリストが表示されます。

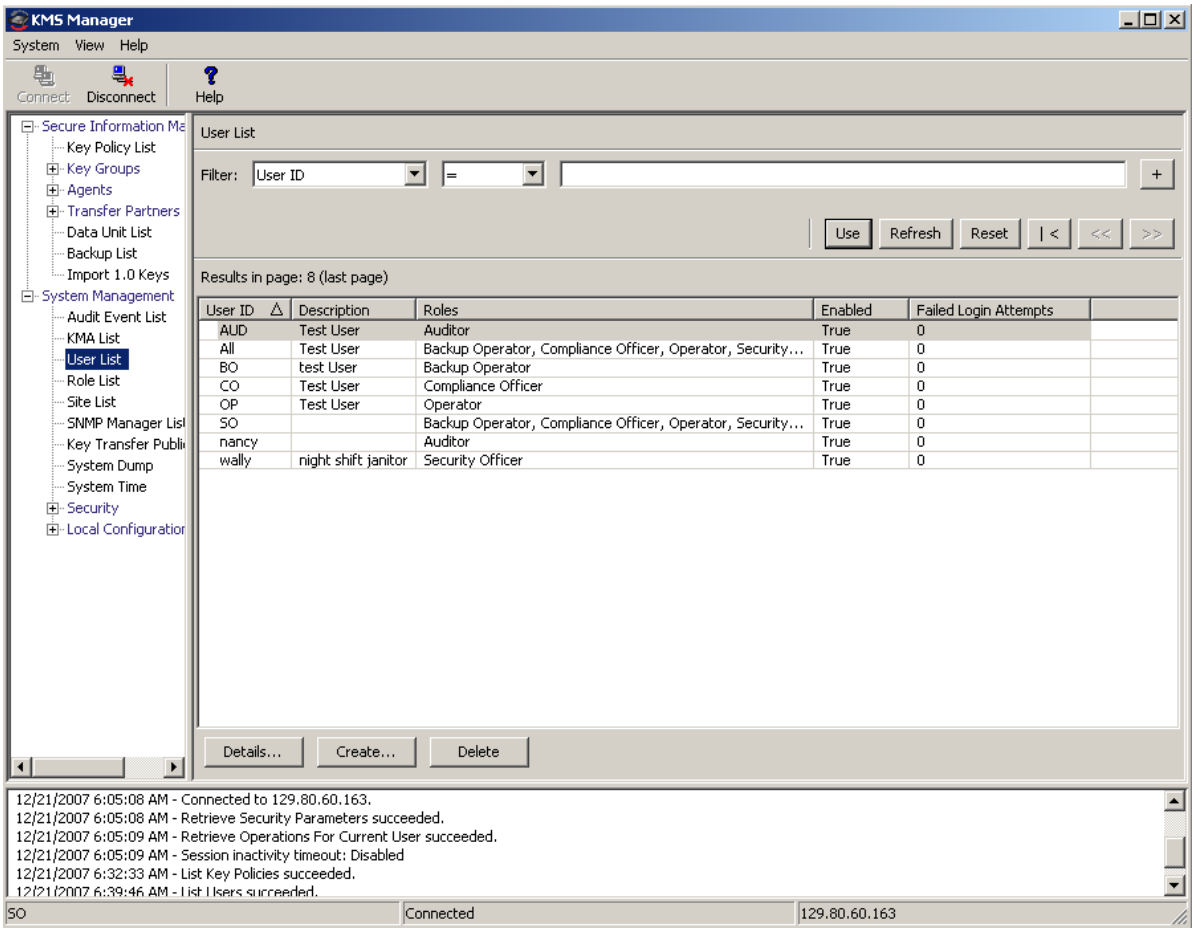


ステータスバー

画面最下部にあるステータスバーは、次のフィールドで構成されています。

- **ユーザー名**: 現在ログインしているユーザーのユーザー名が表示されます。次に示す画面では、セキュリティー責任者 (SO) がログインしています。
- **接続状態**: 現在の接続の状態が表示されます。次の画面では、Connected が表示されています。
- **KMA IP アドレス**: 管理ネットワーク IP アドレスとターゲット KMA の名前が表示されます。

KMA に接続していない場合、状態フィールドは空白になります。



パネル

KMS Manager の各画面には、共通のパネルコンポーネントがあります。ここでは、各コンポーネントについて説明します。

タイトル

画面のタイトルが表示されます。

フィルタ

特定のキーを使用してデータベースをフィルタできます。次のコンポーネントが含まれます。

テーブルラベル: フィルタ処理を適用するテーブルを指定します。

フィルタ属性コンボボックス: フィルタ処理の対象となるフィールドを示します。

フィルタ演算子 1 コンボボックス: フィルタ値 1 に適用されるフィルタ演算子を指定します。フィルタ演算子は、次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 コントロール: 単一の値として使用されるか、またはフィルタキーの範囲の開始値として使用されます。

フィルタ値 2 コントロール: 単一の値として使用されるか、またはフィルタキーの範囲の終了値として使用されます。

「Use」ボタン: 表示されているリストにフィルタを適用します。

Refresh:

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

注 – 出力されるレコードの数が「Query Page Size」より大きい場合は、複数のページが表示されます。フィルタの下の各ボタンをクリックすると、ページ間を移動できます。

ソート:

列見出しをクリックすると、そのフィールドでリストがソートされます。出力に複数のページが必要である場合は、結果の全体がソートされてから、対応するページが返されます。

メッセージ

データベースクエリーに関連するメッセージが表示されます。これは、「Database View」リストと連動して動作します。次のコンポーネントが含まれます。

- 静的テキストラベル: 次のようなエラーメッセージが表示されます。

  ```
  Result limit exceeded. 10,000 results returned. Use a filter to
  reduce the filter size.
  ```

KMS Manager ソフトウェアのアンインストール

KMS ソフトウェアのアンインストールを開始するには、次の 2 つのオプションがあります。

- アンインストールプログラムが存在するディレクトリへ移動し、そこで実行可能ファイルを起動します。
- (Windows ユーザーのみ)「プログラムの追加と削除」処理を開始します。

いずれの場合も、この手順が完了すると「Preparing Setup」ウィンドウが表示されます。69 ページの「アンインストール処理の完了」を参照してください。

実行可能ファイルの起動

KMS Manager ソフトウェアをアンインストールするには、次の手順を実行します。

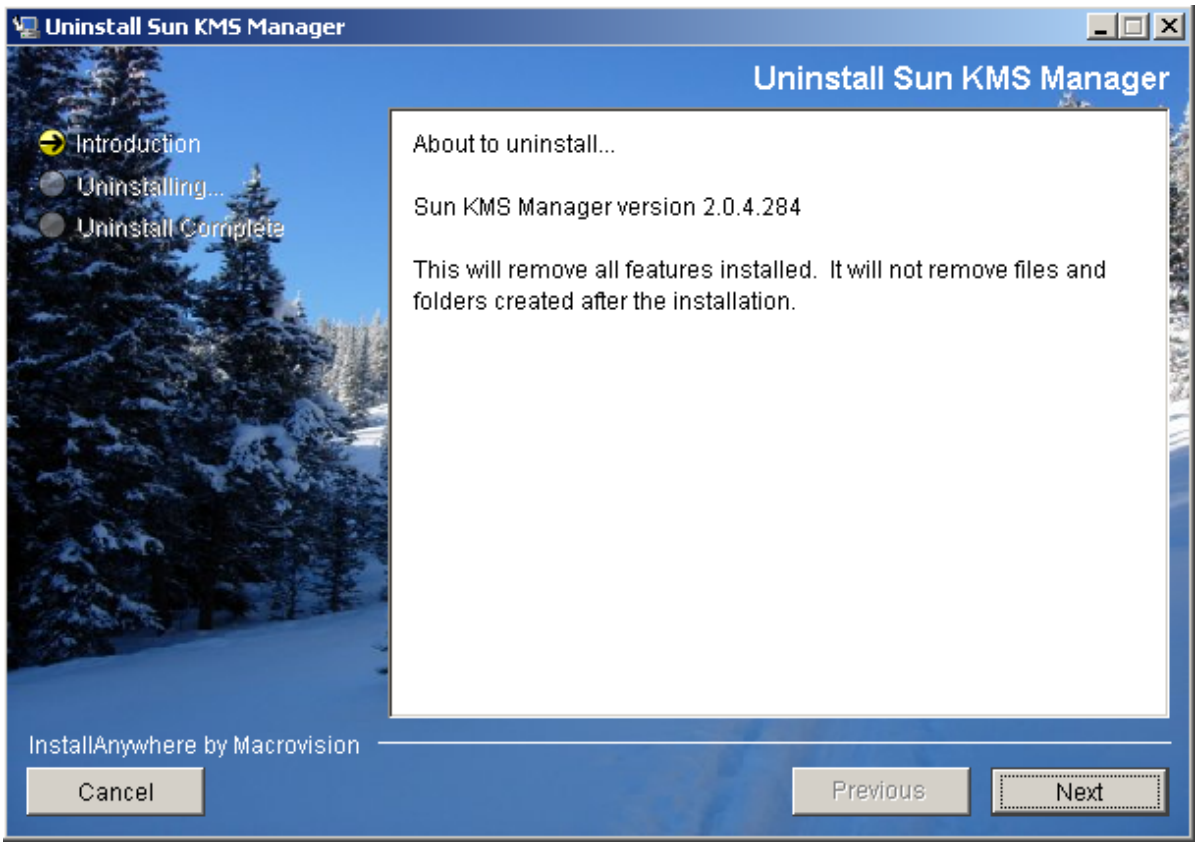
1. Uninstall_Sun KMS Manager ディレクトリへ移動します。このディレクトリは KMS Manager がインストールされたディレクトリの下にあります。
2. Windows の場合は「Uninstall Sun KMS Manager」実行可能ファイル、Solaris の場合は「Uninstall_Sun_KMS_Manager」実行可能ファイルを起動して、アンインストール処理を開始します。
3. インストールおよびアンインストールプログラムによってアンインストール処理の準備が行われる間、「Preparing Setup」ウィンドウが表示されています。

「プログラムの追加と削除」の起動 (Windows のみ)

1. 「**スタート**」、「**設定**」、「**コントロールパネル**」の順にクリックし、「**プログラムの追加と削除**」をダブルクリックします。「プログラムの追加と削除」ウィンドウが表示されます。KMS Manager ソフトウェアがリストに表示されていない場合は、リストをスクロールダウンして Sun KMS Manager を選択し、「変更と削除」ボタンをクリックします。
2. インストールおよびアンインストールプログラムによってアンインストール処理の準備が行われる間、「Preparing Setup」ウィンドウが表示されています。

アンインストール処理の完了

「KMS uninstall」ダイアログボックスが表示され、選択したアプリケーションとそのすべての機能の削除を確認するように求められます。



1. 「Next」ボタンを選択して続行するか、「Cancel」ボタンを選択して処理を中止し、「プログラムの追加と削除」ウィンドウ (Windows) またはシェルプロンプト (Solaris) に戻ります。

注 – 接続プロファイルは削除されません。

---

2. アンインストール処理が完了すると、「Uninstall Complete」ウィンドウが表示されます。「Finish」ボタンを選択して、このウィンドウを閉じます。このウィンドウを閉じて、「プログラムの追加と削除」ウィンドウ (Windows) またはシェルプロンプト (Solaris) に戻ります。

第4章

「System」メニューの使用法

この章では、KMS Manager を使用して KMA に接続する手順について詳しく説明します。また、「System」メニューのその他のオプションを使用する手順についても説明します。

クラスタへの接続

重要 – KMA に接続する前に、1 つ以上のクラスタプロファイルが存在し、KMA 上でユーザーを作成して有効にしておく必要があります。

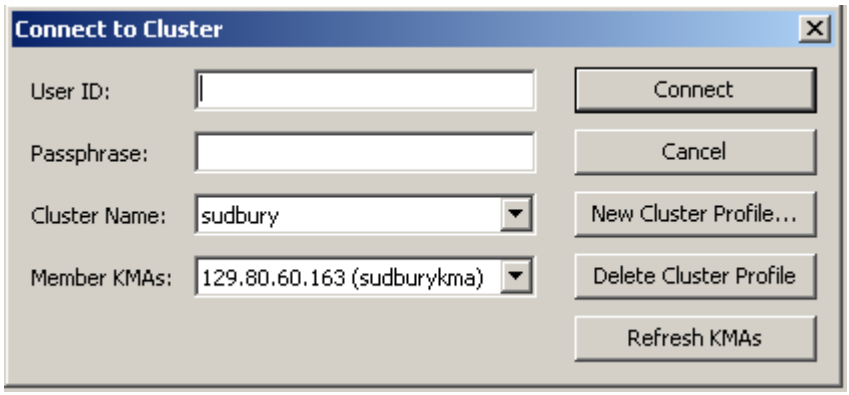
この節では、KMS Manager を使用して KMA に接続する手順について説明します。はじめて KMA に接続する場合は、最初にクラスタプロファイルを定義する必要があります。これ以降は、作成したクラスタプロファイルを使用して、KMA に接続できるようになります。KMS Manager は、クラスタプロファイルの情報を使用して、クラスタ (KMA IP アドレス) との通信を開始します。

クラスタプロファイルの作成

クラスタプロファイルを作成するには、次の手順を実行します。

1. 「System」メニューから「Connect」を選択するか、またはツールバーの 

を選択します。「Connect to Cluster」ダイアログボックスが表示されます。既存のプロファイルがある場合は、「Cluster Name」フィールドと「IP Address」フィールドに、クラスタプロファイル名とその IP アドレスが表示されます。



2. 「New Cluster Profile」ボタンを選択します。「Create Cluster Profile」ダイアログボックスが表示されます。

3. 次のパラメータを設定します。

Cluster Name

クラスタプロファイル名を一意に識別する値を入力します。

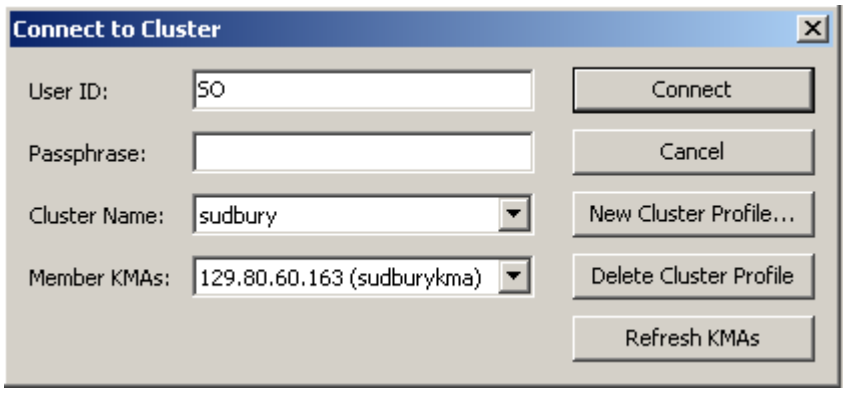
Initial IP Address or Host Name

接続先となる、このクラスタ内の最初の KMA のサービスネットワーク IP アドレスまたはホスト名を入力します。接続先として選択するネットワークは、KMS Manager が実行されているコンピュータシステムがどのようなネットワークに接続されているかによって決まります。

注 – クラスタプロファイルは、クラスタ全体を対象としており、エージェントのすべてのユーザーがこれを使用できるため、1 つ作成するだけで済みます。2 つめのクラスタを確立したり、現在のクラスタ内にあるすべての KMA の IP アドレスを変更した場合にかぎり、別のクラスタプロファイルの作成が必要になります。

---

4. 「OK」ボタンを選択します。「Connect to Cluster」ダイアログボックスが表示され、作成したクラスタプロファイルの情報が示されます。



5. 次のパラメータを設定し、「Connect」ボタンを選択します。

User ID

指定された KMA に接続するユーザーの名前を入力するか、または最初の QuickStart 処理を実行したあとにはじめて KMA に接続する場合は、QuickStart の処理中に作成されたセキュリティー責任者の名前を入力します。

Passphrase

選択したユーザーのパスフレーズを入力します。

Cluster Name

接続先のクラスタを選択します。

Member KMAs

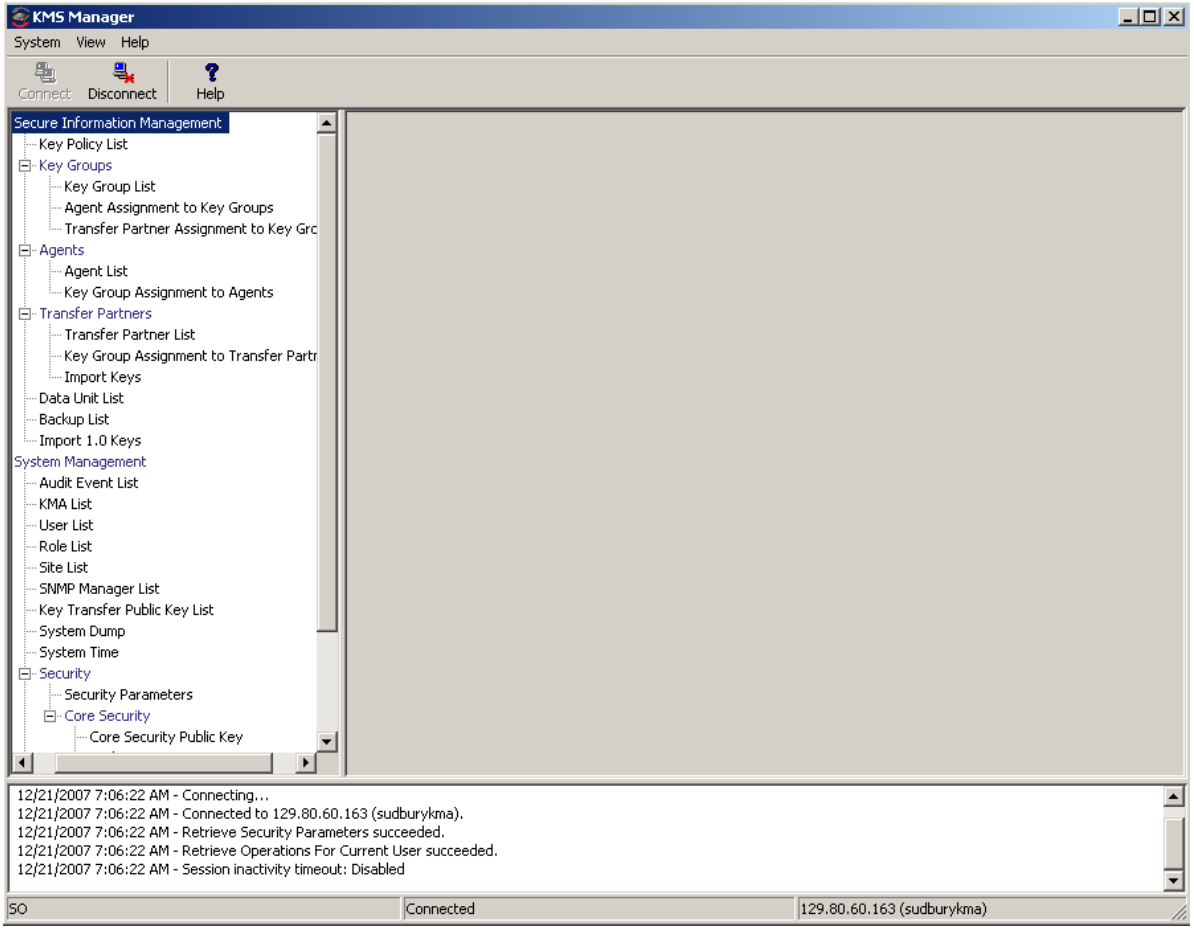
このクラスタ内の接続先となる KMA を選択します。

注 – 以前ユーザーがクラスタに接続したあとでこのクラスタに加わった KMA は、「Member KMAs」リストには表示されません。リストを更新するには、ユーザー名とパスフレーズを入力し、クラスタプロファイルを選択して「Refresh KMAs」ボタンを選択します。

重要 – KMA によって、ユーザー ID とパスフレーズが認証されます。返される KMA IP アドレスのリストは、クラスタプロファイルの生成に使用され、ホストに格納されます。次回ユーザーが KMA に接続する場合は、ユーザー名とパスフレーズを入力し、クラスタプロファイルを指定して KMA を選択できます。

---

6. 接続が成功すると、KMS Manager GUI のステータスバーに、ユーザー名とエイリアス、KMA の接続状態 (Connected)、および KMA の IP アドレスが表示されます。



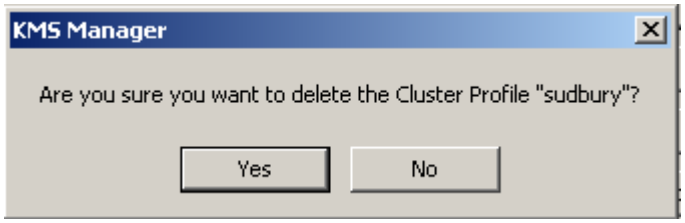
7. これで、KMS Manager を使用してさまざまな操作を実行できるようになります。さまざまなユーザーのロールで実行できる操作については、第 5 章～第 9 章を参照してください。

注 – KMA 管理操作のツリー区画に表示されるタスクは、ロールの割り当てによって異なります。

クラスタプロファイルの削除

クラスタプロファイルを削除するには、次の手順を実行します。

1. 「Connect to Cluster」ダイアログボックスで、「Cluster Name」フィールドの横の下矢印を選択して削除するクラスタプロファイルを強調表示し、「Delete Cluster Profile」ボタンを選択します。「Delete Cluster Profile」ダイアログボックスが表示され、選択したクラスタプロファイルの削除の確認が求められます。



2. 「Yes」ボタンを選択して、プロファイルを削除します。クラスタプロファイルが削除され、「Connect to Cluster」ダイアログボックスに戻ります。

KMA からの切断

KMA から切断するには、次の手順を実行します。

1. 「System」メニューから「Disconnect」を選択するか、またはツールバーの

をクリックします。KMA および KMS クラスタからただちに切断されます。セッション監査ログ区画に、KMA から切断した日時が表示されます。

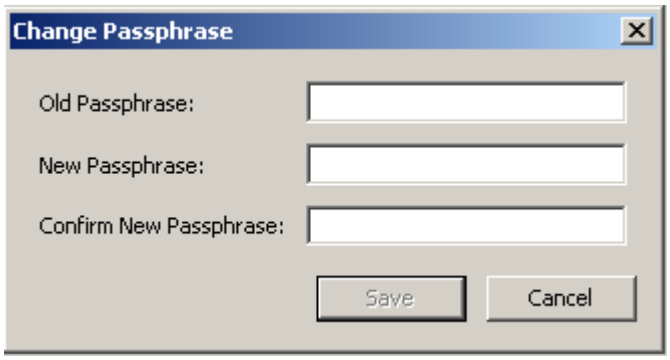
パスフレーズの変更

注 – このメニューオプションは、ユーザーがプロファイルを使用して KMA に接続されている場合にのみ使用可能です。

この機能を使用すると、ユーザーは自分のパスフレーズを変更できます。この機能によって、ユーザーの現在の証明書が無効になることはありません。

接続されているユーザーのパスフレーズを変更するには、次の手順を実行します。

1. 「System」メニューから、「Change Passphrase...」を選択します。「Change Passphrase」ダイアログボックスが表示されます。



2. 次のパラメータを設定し、「OK」ボタンを選択します。

Old Passphrase

ユーザーの現在のパスフレーズを入力します。

New Passphrase

ユーザーの新しいパスフレーズを入力します。

Confirm New Passphrase

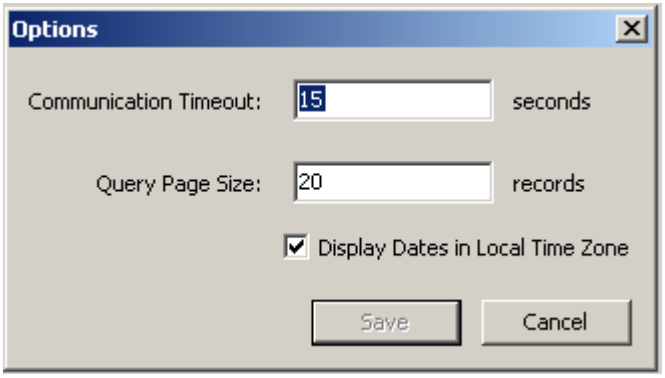
同じパスフレーズを再入力します。

3. セッション監査ログ区画に、ユーザーのパスフレーズを変更した日時を示すメッセージが表示されます。

構成設定値の指定

構成設定値を指定するには、次の手順を実行します。

1. 「System」メニューから、「Options....」を選択します。「Options」ダイアログボックスが表示され、現在の構成設定値が示されます。



2. 必要に応じて、次のパラメータを変更し、「Save」ボタンを選択します。

Communication Timeout

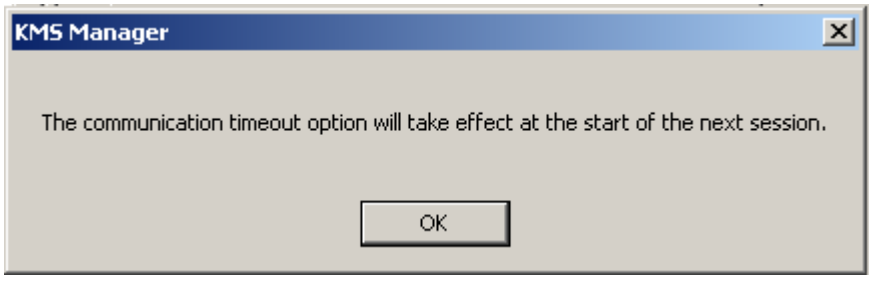
接続されている KMA との通信のタイムアウト期間 (秒単位) を入力します。指定したタイムアウト値が経過するまでに KMA が応答しない場合は、KMS Manager によって通信が切断されます。最小値は 1、最大値は 60 です。デフォルトは 15 です。

Query Page Size

画面、ダイアログ、または項目リストを表示するダイアログのタブに表示される、項目の最大数を入力します。ページングを使用すると、項目数がこの制限よりも多いリストを表示できます。最小値は 1、最大値は 1000 です。デフォルトは 20 です。

Display Dates in Local Time Zone

UTC ではなく、KMS Manager が実行されているローカルマシンのタイムゾーンですべての日時を表示する場合は、このチェックボックスを選択します。デフォルトでは選択されています。次の確認メッセージが表示されます。



KMS Manager の終了

KMS Manager を終了するには、次の手順を実行します。

1. 「System」メニューから「Exit」を選択するか、またはタイトルバーの  をクリックします。KMS Manager が閉じ、Windows のデスクトップに戻ります。
2. KMS Manager が接続されている場合は、接続をただちに切断して終了します。

第5章

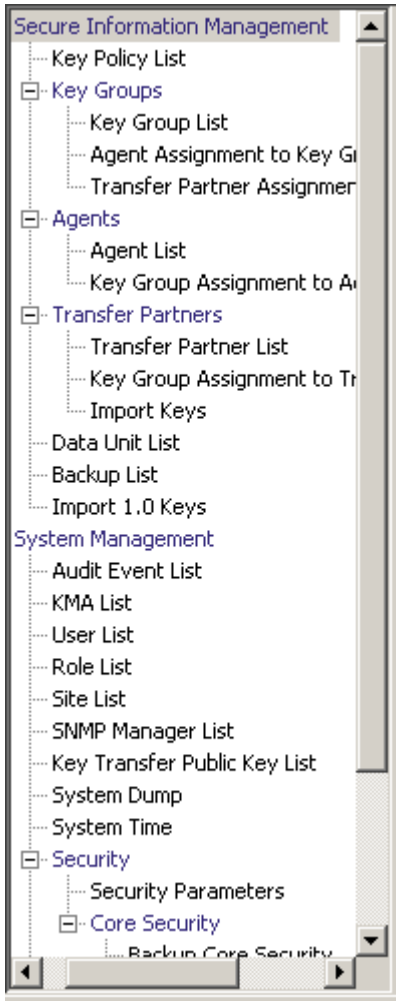
セキュリティー責任者の操作

セキュリティー責任者は、セキュリティー設定、ユーザー、サイト、および転送パートナーを管理します。この章では、次の項目について説明します。

- セキュリティー責任者ロールが付与されたユーザーが実行できる操作。複数のロールが割り当てられている場合は、そのロールを実行する手順について、該当する章を参照してください。
- 技術サポートアカウントを有効または無効にする手順。

セキュリティー責任者ロール

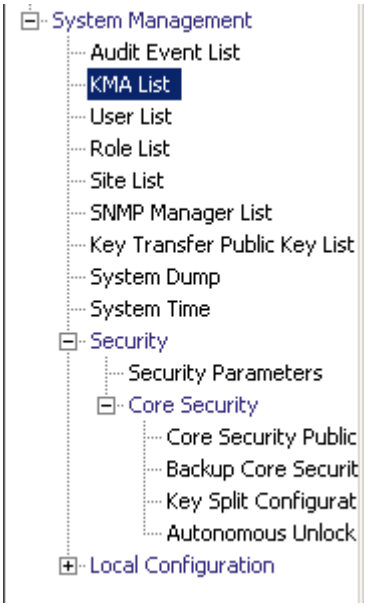
セキュリティー責任者は、実体 (KMA、ユーザー、サイト、転送パートナー) およびシステムのさまざまなセキュリティーの側面を管理できます。



「KMA List」メニュー

「KMA List」メニューオプションを使用すると、次の操作を行うことができます。

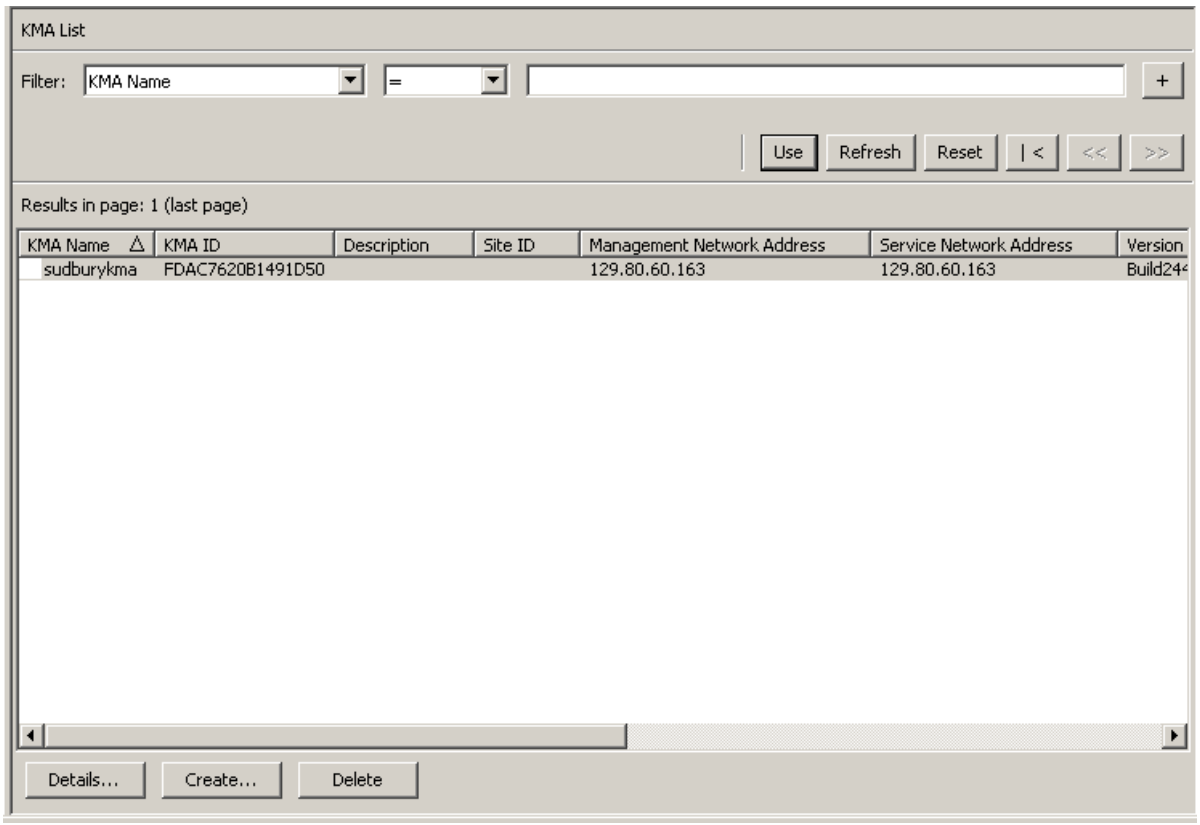
- KMA の表示
- KMA の作成
- KMA の情報の変更
- KMA の削除



KMA の表示

KMA を表示するには、次の手順を実行します。

「System Management」メニューから、「KMA List」を選択します。「KMA List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで KMA リストにフィルタを適用することもできます。

- KMA Name
- KMA ID
- Description
- Site ID
- Management Network Address
- Service Network Address
- Version
- Failed Login Attempts
- Responding
- Response Time
- Replication Lag Size
- Key Pool Ready

- Enrolled

表示されている KMA リストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- KMA Name
- Description
- Site ID
- Management Network Address
- Service Network Address
- Version
- Failed Login Attempts
- Enrolled

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 ボックス:

このフィールドに値を入力します。

Use:

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

KMA Name

クラスタ内の各 KMA を識別するユーザー指定の識別子が表示されます。

KMA ID

KMA を識別する一意のシステム生成識別子が表示されます。

Description

KMA の説明が示されます。

Site ID

KMA が属するサイトが示されます。

Management Network Address

管理ネットワークでの KMA の IP アドレスが表示されます。

Service Network Address

サービスネットワークでの KMA のサービスネットワークアドレスが表示されます。

Version

KMA ソフトウェアのバージョン番号が表示されます。

Failed Login Attempts

ログオンに失敗した回数が表示されます。

Responding

KMA が動作中かどうかが示されます。True または False の値を取ります。

Response Time

KMA が要求に応答するまでの時間がミリ秒単位で表示されます。

Replication Lag Size

複製を待機している更新の数が表示されます。

Key Pool Ready

使用可能な未割り当ての鍵のパーセンテージが表示されます。

Enrolled

KMA が追加されているかどうか、または KMA がクラスタに正常にログインしているかどうかが示されます。True または False の値を取ります。

KMA を作成する場合は、「Create」ボタンを選択します。詳細は、85 ページの「KMA の作成」を参照してください。

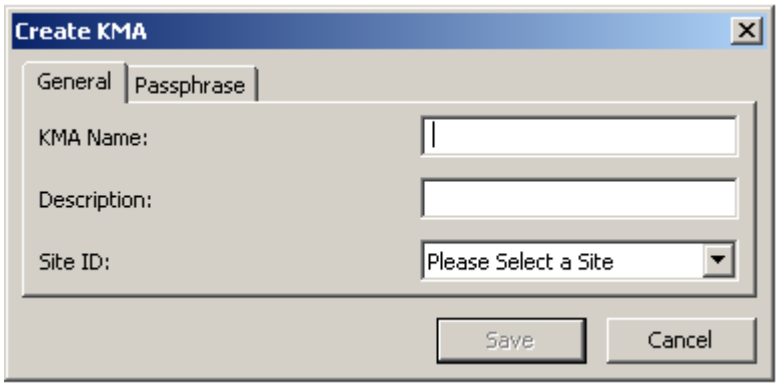
KMA の詳細を表示または変更する場合は、その KMA を強調表示して「Details」ボタンを選択します。詳細は、88 ページの「KMA の詳細の表示および変更」を参照してください。

KMA を削除する場合は、「Delete」ボタンを選択します。詳細は、90 ページの「KMA の削除」を参照してください。

KMA の作成

KMA を作成するには、次の手順を実行します。

1. 「KMA List」画面で、「Create」ボタンを選択します。「Create KMA」ダイアログボックスが表示され、「General」タブがアクティブになっています。



2. 次のパラメータを設定します。

「General」タブ

KMA Name

クラスタ内の KMA を一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

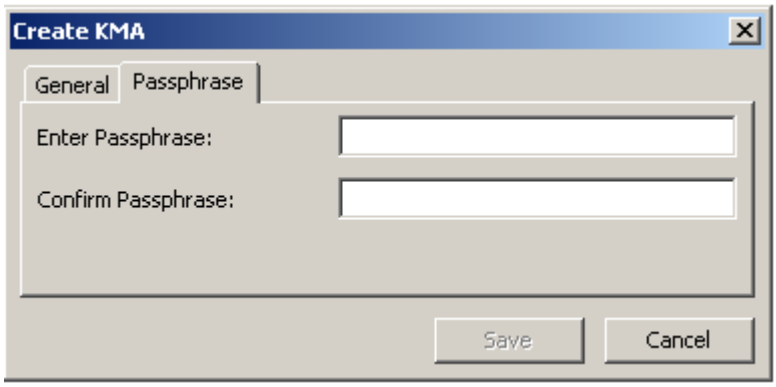
Description

KMA を一意に説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Site ID

下矢印ボタンをクリックし、KMA が属するサイトを選択します。このフィールドは省略可能です。

3. 「Passphrase」タブを開きます。



4. 次のパラメータを設定し、「Save」ボタンを選択します。

Enter Passphrase

このユーザーのパスフレーズを入力します。最小文字数は 8 文字、最大文字数は 64 文字です。デフォルト値は 8 です。

パスフレーズの要件は、次のとおりです。

- パスフレーズに、ユーザーの KMA 名を含めないでください。
- パスフレーズには、大文字、小文字、数値、または特殊文字の 4 つの文字クラスのうち 3 つを使用する必要があります。

  使用可能な特殊文字は、次のとおりです。

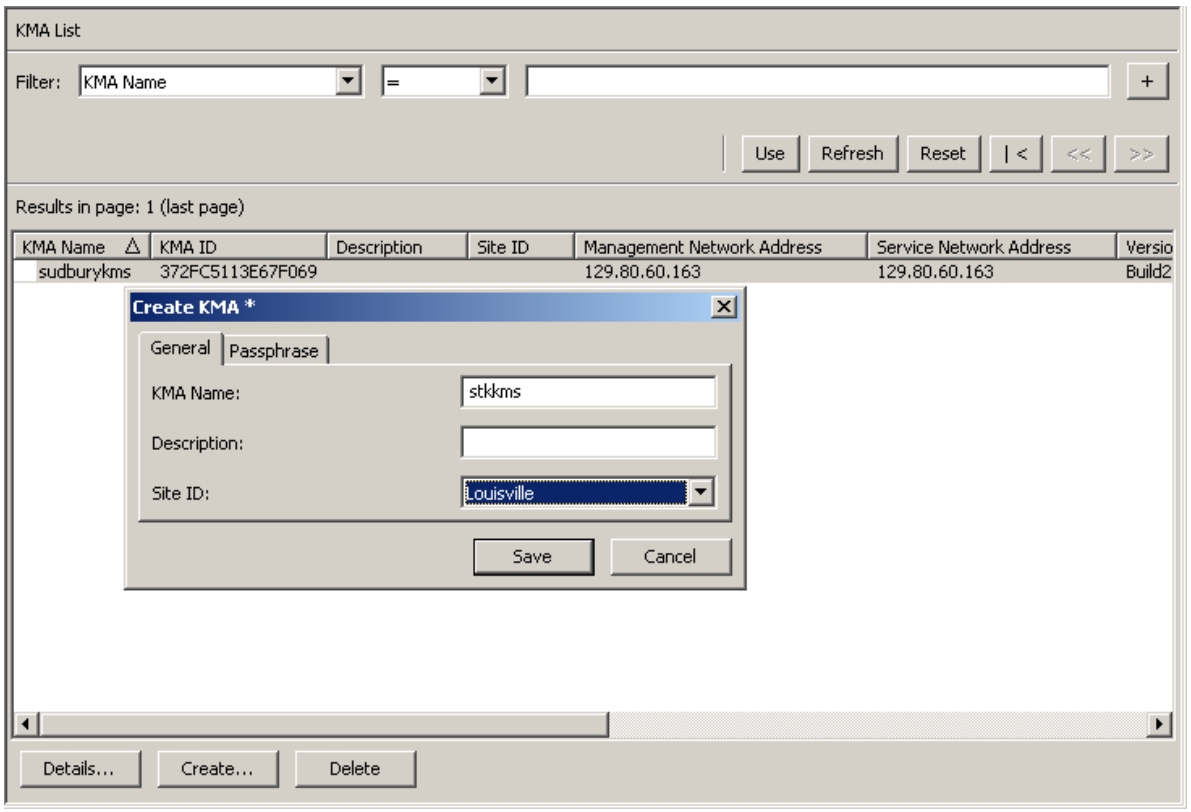
  ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ ” < > , . / ?
- タブ、改行などの制御文字は使用できません。

注 – パスフレーズの最小文字数の要件を変更する方法については、148 ページの「セキュリティーパラメータの変更」を参照してください。

Confirm Passphrase

「Enter Passphrase」フィールドに入力した値と同じ値を入力します。

5. KMA レコードがデータベースに追加され、そのエントリが「KMA List」画面に表示されます。



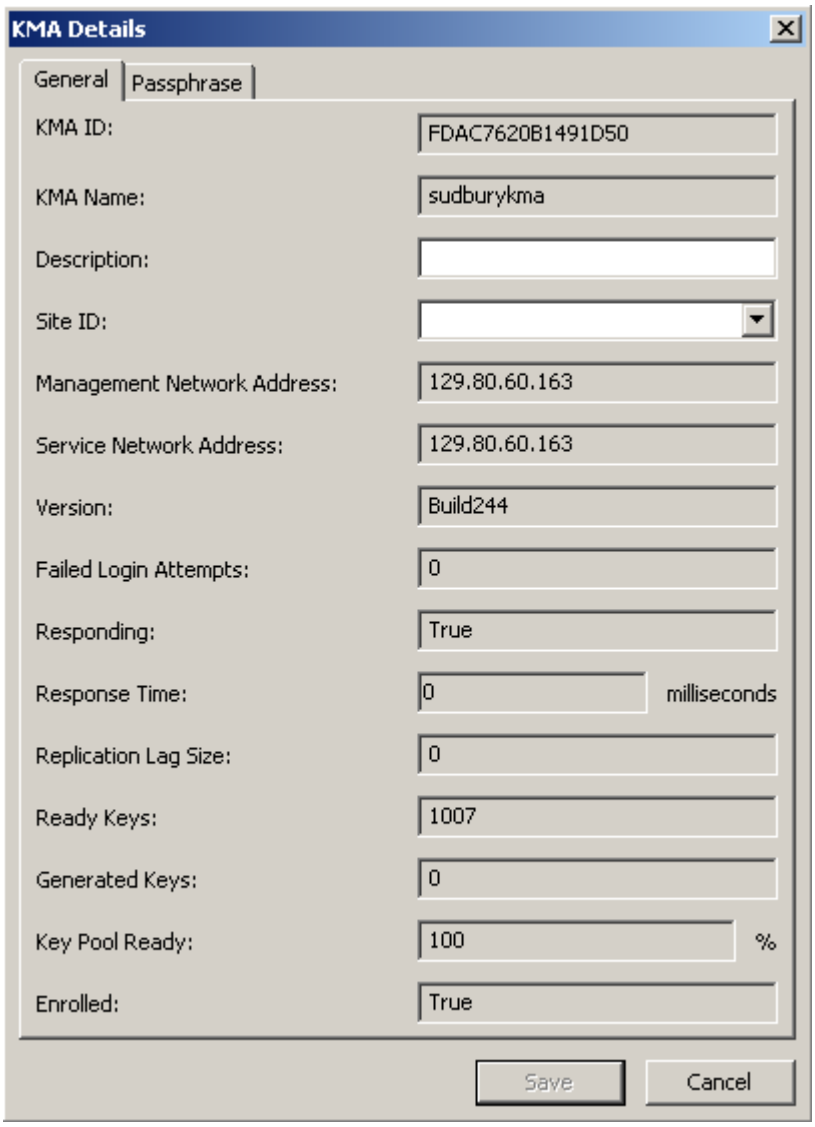
6. 作成した KMA で QuickStart プログラムを実行し、KMA がクラスタに参加できるようにします。クラスタへの参加の手順については、37 ページの「既存のクラスタへの参加」を参照してください。

KMA の詳細の表示および変更

注 – セキュリティー責任者以外のユーザーが KMA の詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。

KMA の詳細を変更するには、次の手順を実行します。

1. 「KMA List」画面で、詳細情報を表示する KMA エントリをダブルクリックするか、または KMA エントリを強調表示して「Details」ボタンを選択します。「KMA Details」画面が表示されます。



2. 「General」タブで、次のフィールドを変更します。

- Description

- Site ID

3. 「Passphrase」タブを開き、次のパラメータを変更します。
- Passphrase
- Confirm Passphrase (同じパスフレーズを再入力)

4. 終了したら、「Save」ボタンを選択します。データベース内の KMA レコードが変更されます。

KMA のパスフレーズの設定

注 – KMA に接続されていない場合に、KMA のパスフレーズを変更できます。

新しいクラスタを作成する場合、新しいクラスタの作成に使用される KMA には、ランダムなパスフレーズが自動的に割り当てられます。証明書の期限切れによって、KMA が実体の証明書をクラスタ内の別の KMA から取得する必要がある場合には、この機能を使用して、パスフレーズを既知の値に設定します。

KMA のパスフレーズを設定するには、次の手順に従います。

1. 「KMA List」画面で、KMA エントリをダブルクリックするか、または KMA エントリを強調表示して「Details」ボタンを選択します。「KMA Details」ダイアログボックスが表示され、「General」タブがアクティブになっています。

2. 「Passphrase」タブを開き、次のパラメータを変更します。
- Passphrase
- Confirm Passphrase (同じパスフレーズを再入力)

3. 「Save」ボタンを選択して、変更内容を保存します。KMA のデータベースエントリが変更されます。

4. コンソールを使用して、パスフレーズが変更された KMA で、KMA をクラスタにログインする機能を選択します。再度ログインするまで、KMA はクラスタと通信できません。

KMA の削除

重要 – KMA を削除する前に、コンソールの「Shutdown KMA」機能を使用して、KMA をオフラインにする必要があります。KMA をオフラインにしておかないと、KMA はクラスタ外で機能し続けて、エージェントとユーザーに「古い情報」を送信します。

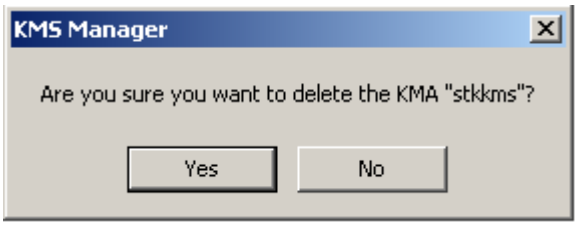
通常、このコマンドは、クラスタから障害のある KMA を削除する場合にのみ使用されます。ただし、使用しなくなった KMA を削除するために使用されることもあります。しかし、このような場合には、コンソールの「Reset KMA」機能でゼロ化オプションを使用することをお勧めします。この機能は、クラスタから KMA を削除し、使用しなくなった KMA のディスクからすべての情報を完全に消去します。

削除した KMA をクラスタに再度参加させる場合は、KMA を出荷時のデフォルトにリセットし、QuickStart プログラムからオプション 2 を選択する必要があります。

このオプションを使用すると、セキュリティー責任者は、使用していない KMA を削除できます。

KMA を削除するには、次の手順を実行します。

1. 「KMA List」画面で、削除する KMA を強調表示して「Delete」ボタンを選択します。次のように、選択した KMA の削除を確認するダイアログボックスが表示されます。

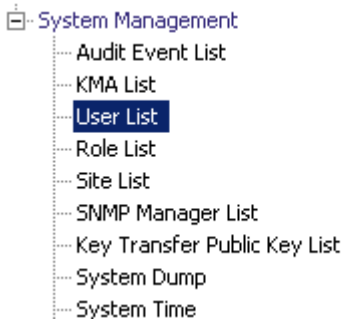


2. 「Yes」ボタンを選択して、KMA を削除します。現在選択している KMA が削除され、「KMA List」画面に戻ります。また、この KMA に関連付けられていて、その他の実体では使用されていないエントリもすべて削除されます。

「User List」メニュー

「User List」メニューオプションを使用すると、次の操作を行うことができます。

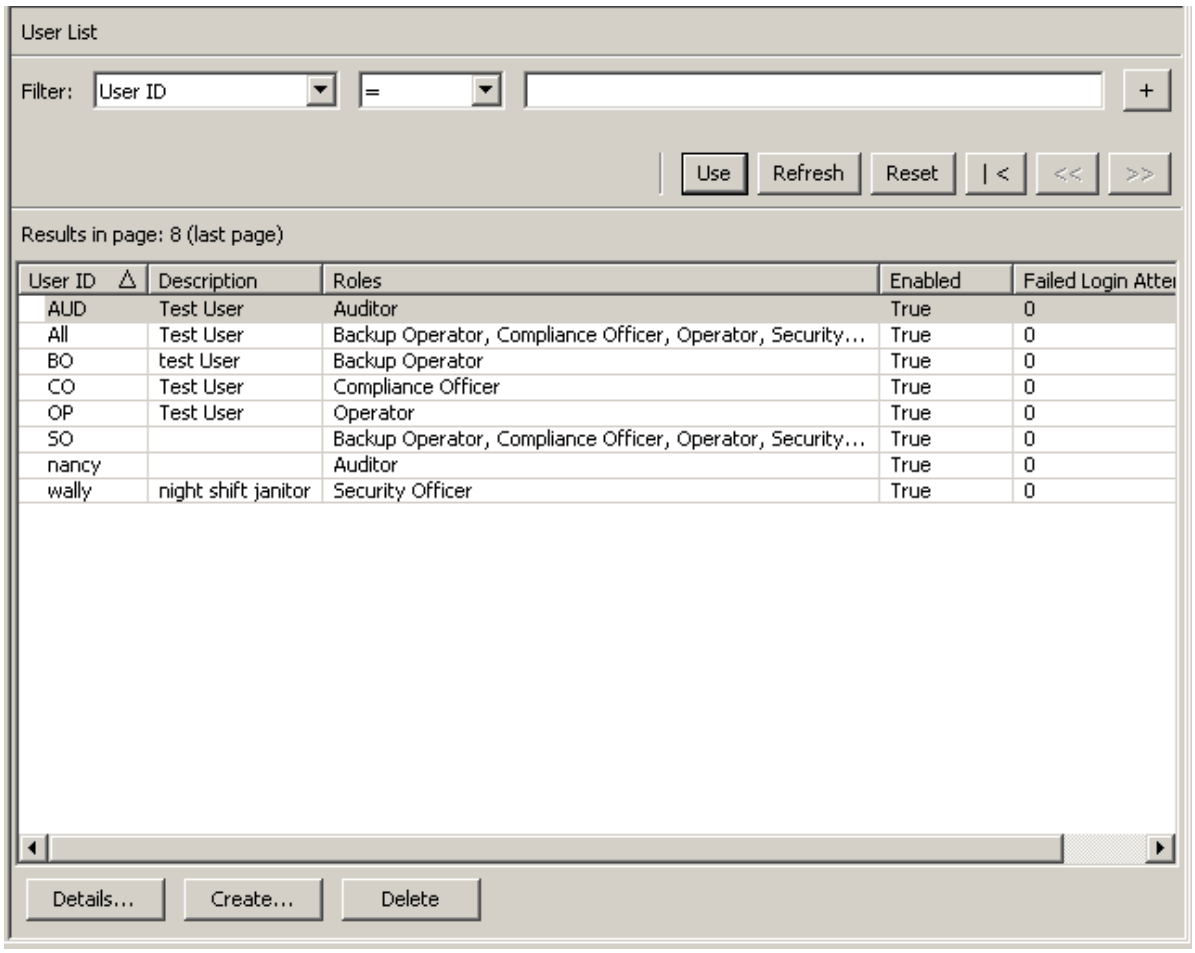
- ユーザーの表示
- ユーザーの作成
- 既存のユーザー情報の変更
- 既存のユーザーの削除



ユーザーの表示

ユーザーを表示するには、次の手順を実行します。

「System Management」メニューから、「User List」を選択します。「User List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでユーザーリストにフィルタを適用することもできます。

- User ID
- Description
- Roles
- Enabled
- Failed Login Attempts

表示されているユーザーリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- User ID
- Description
- Enabled
- Failed Login Attempts

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 ボックス:

このフィールドに値を入力します。

Use:

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

User ID

クラスタ内の各ユーザーを識別する一意の識別子が表示されます。これは通常、「ユーザー名」と呼ばれます。

Description

ユーザーの説明が示されます。

Roles

ユーザーのセキュリティーロールのリストが表示されます。ロールによって、ユーザーはさまざまな操作を実行できます。

Enabled

ユーザーのステータスが示されます。True または False の値を取ります。

Failed Login Attempts

ログインに失敗した回数が示されます。

ユーザーを作成する場合は、「Create」ボタンを選択します。詳細は、95 ページの「ユーザーの作成」を参照してください。

ユーザーの詳細を変更する場合は、そのユーザーを強調表示して「Details」ボタンを選択します。詳細は、97 ページの「ユーザーの詳細の表示および変更」を参照してください。

ユーザーを削除する場合は、「Delete」ボタンを選択します。詳細は、99 ページの「ユーザーの削除」を参照してください。

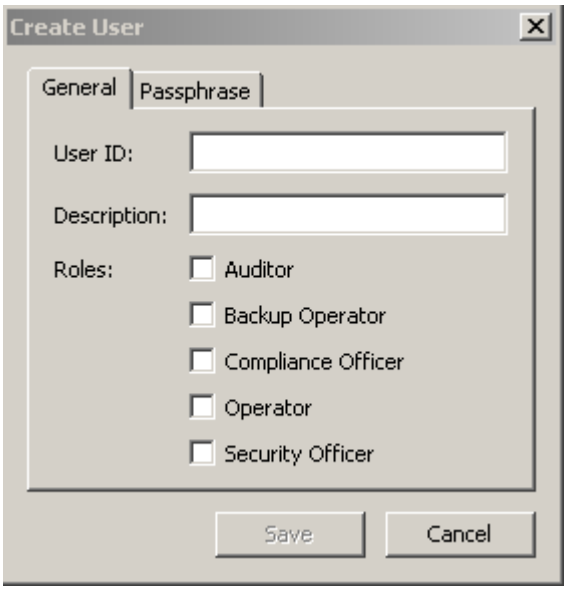
ユーザーのパスフレーズまたは証明書、あるいはその両方が危殆化されている場合、セキュリティー責任者は、ユーザーのパスフレーズを設定できます。ユーザーのパスフレーズを設定する手順については、98 ページの「ユーザーのパスフレーズの設定」を参照してください。

また、ユーザーが自身のパスフレーズを変更することもできます。手順については、76 ページの「パスフレーズの変更」を参照してください。

ユーザーの作成

ユーザーを作成するには、次の手順を実行します。

1. 「User List」画面で、「Create」ボタンを選択します。「Create User」ダイアログボックスが表示され、「General」タブがアクティブになっています。



2. 次のパラメータを設定します。

「General」タブ

User ID

ユーザーを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

Description

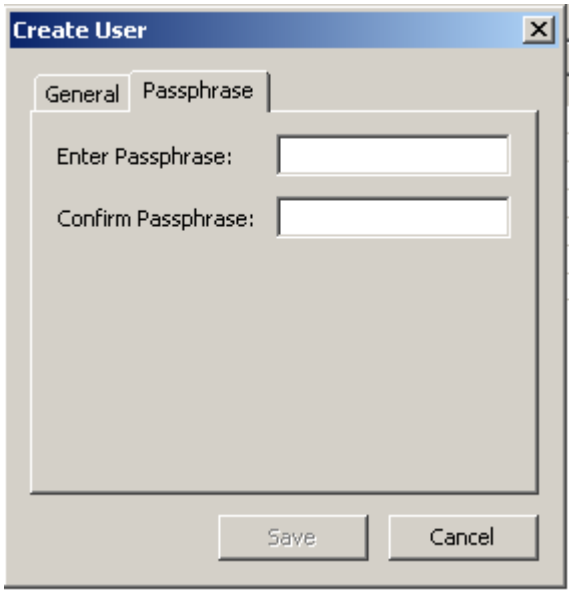
ユーザーを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Roles

ユーザーに付与するロールの横にあるチェックボックスを選択します。

「Passphrase」タブ

3. 「Passphrase」タブを開きます。



4. 次のパラメータを設定します。

Enter Passphrase

このユーザーのパスフレーズを入力します。最小文字数は 8 文字、最大文字数は 64 文字です。デフォルト値は 8 です。

パスフレーズの要件は、次のとおりです。

- パスフレーズに、ユーザーのユーザー ID を含めないでください。
- パスフレーズには、大文字、小文字、数値、または特殊文字の 4 つの文字クラスのうち 3 つを使用する必要があります。

  使用可能な特殊文字は、次のとおりです。

  ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ ” < > , . / ?
- タブ、改行などの制御文字は使用できません。

注 – パスフレーズの最小文字数の要件を変更する方法については、148 ページの「セキュリティーパラメータの変更」を参照してください。

Confirm Passphrase

「Enter Passphrase」フィールドに入力した値と同じ値を入力します。

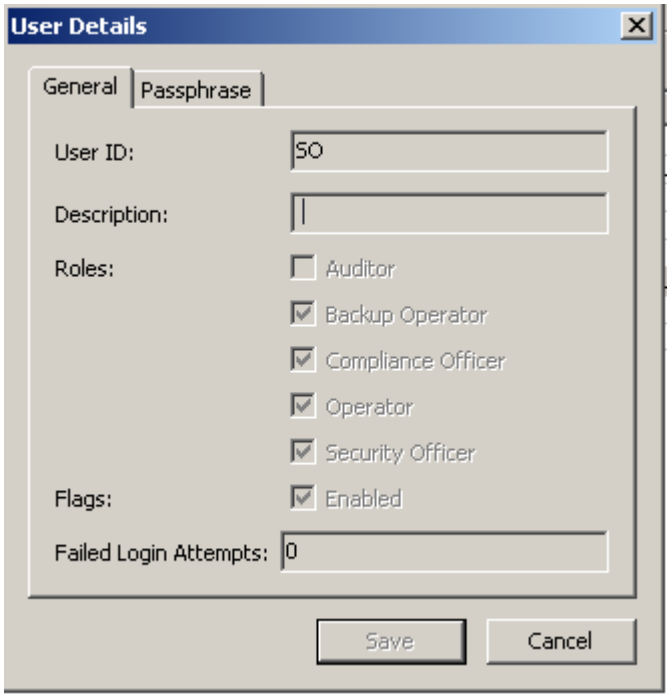
5. 「Save」ボタンを選択します。ユーザーレコードがデータベースに追加されます。新しいユーザーが「User List」に表示されます。

ユーザーの詳細の表示および変更

注 – 現在ログインしているセキュリティー責任者は、自身のレコードを変更できません。

ユーザー情報を変更するには、次の手順を実行します。

1. 「Users List」画面で、詳細情報を表示するユーザーをダブルクリックするか、またはユーザーレコードを強調表示して「Details」ボタンを選択します。「User Details」画面が表示され、「Save」ボタンを含むすべてのフィールドが使用不可になっています。



2. 「General」タブで、次のパラメータを変更します。

- User ID
- Description
- Roles
- Flags - Enabled
- Failed Login Attempts

「Failed Login Attempts」フィールドには、ログインに失敗した回数が表示されます。

3. 「Passphrase」タブを開き、次のパラメータを変更します。

- Passphrase
- Confirm Passphrase

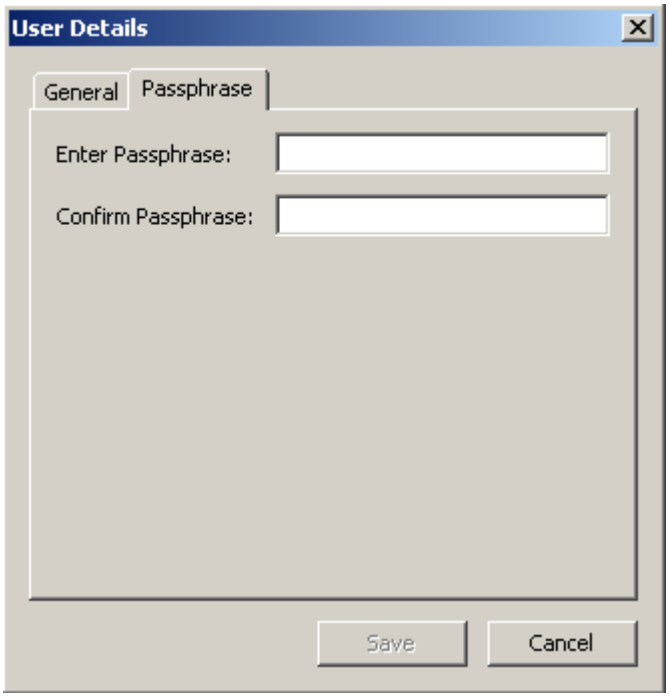
4. 終了したら、「Save」ボタンを選択します。データベース内のユーザーレコードが変更されます。

ユーザーのパスフレーズの設定

ユーザーのパスフレーズまたは証明書、あるいはその両方が危殆化されていると思われる場合、セキュリティー責任者は、ユーザーのパスフレーズを設定できます。ユーザーが新しいパスフレーズを使用して KMA にログオンすると、新しい証明書が生成されます。

ユーザーのパスフレーズを設定するには、次の手順を実行します。

1. 「User List」画面で、パスフレーズを設定するユーザーをダブルクリックするか、またはユーザーを強調表示して「Details」ボタンを選択します。
2. 「User Details」画面が表示されます。「Passphrase」タブを開きます。



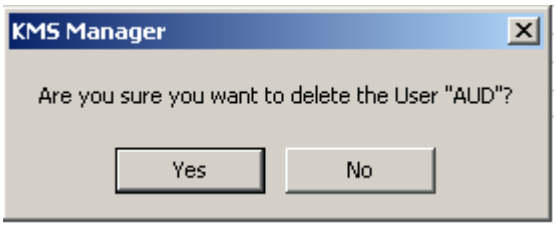
3. 「Enter Passphrase」フィールドで、ユーザーアカウントの作成時にセキュリティー責任者によって割り当てられたパスフレーズを入力します。
4. 「Confirm Passphrase」フィールドに、手順 3 で入力した値と同じ値を入力します。ユーザーレコードの新しいパスフレーズが保存されます。「User List」画面に戻ります。

ユーザーの削除

ユーザーは、ユーザー自身を削除できません。

ユーザーを削除するには、次の手順を実行します。

1. 「Users List」画面で、削除するユーザーを選択して「Delete」ボタンを選択します。次のように、選択したユーザーの削除を確認するダイアログボックスが表示されます。



2. 「Yes」ボタンを選択して、ユーザーを削除します。現在選択しているユーザーが削除され、「User List」画面に戻ります。削除したユーザーは表示されなくなります。

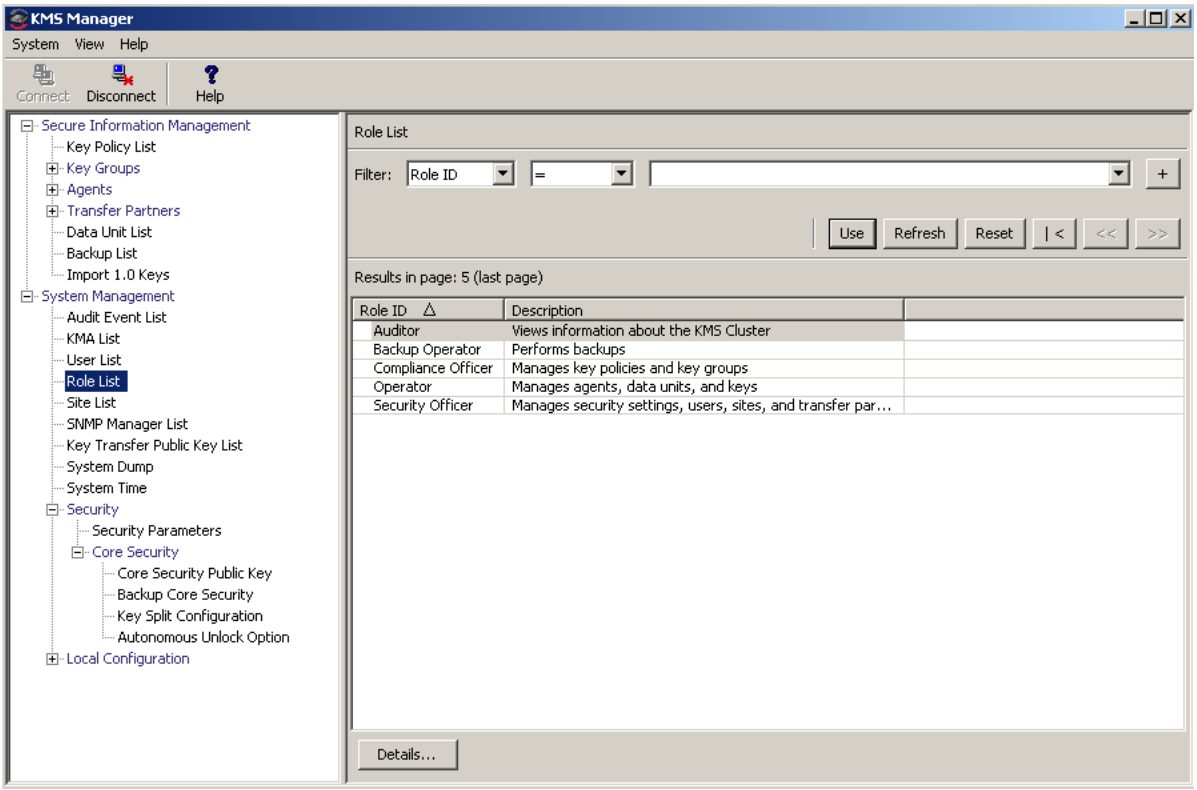
「Role List」メニュー

「Role List」メニューオプションを使用すると、ユーザーのロールを表示できます。ロールとは、ユーザーが実行できるさまざまなシステム操作の、固定された論理グループを指します。1 人のユーザーに複数のロールを付与できます。

ロールの表示

ロールを表示するには、次の手順を実行します。

「System Management」メニューから、「Role List」を選択します。「Role List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでロールリストにフィルタを適用することもできます。

- Role ID
- Description

表示されているリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Role ID
- Description

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- 空白
- 空白以外

フィルタ値 1 ボックス:

このフィールドに値を入力します。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Role ID

各セキュリティーロールを識別する一意の識別子が表示されます。

Description

ロールの説明が示されます。

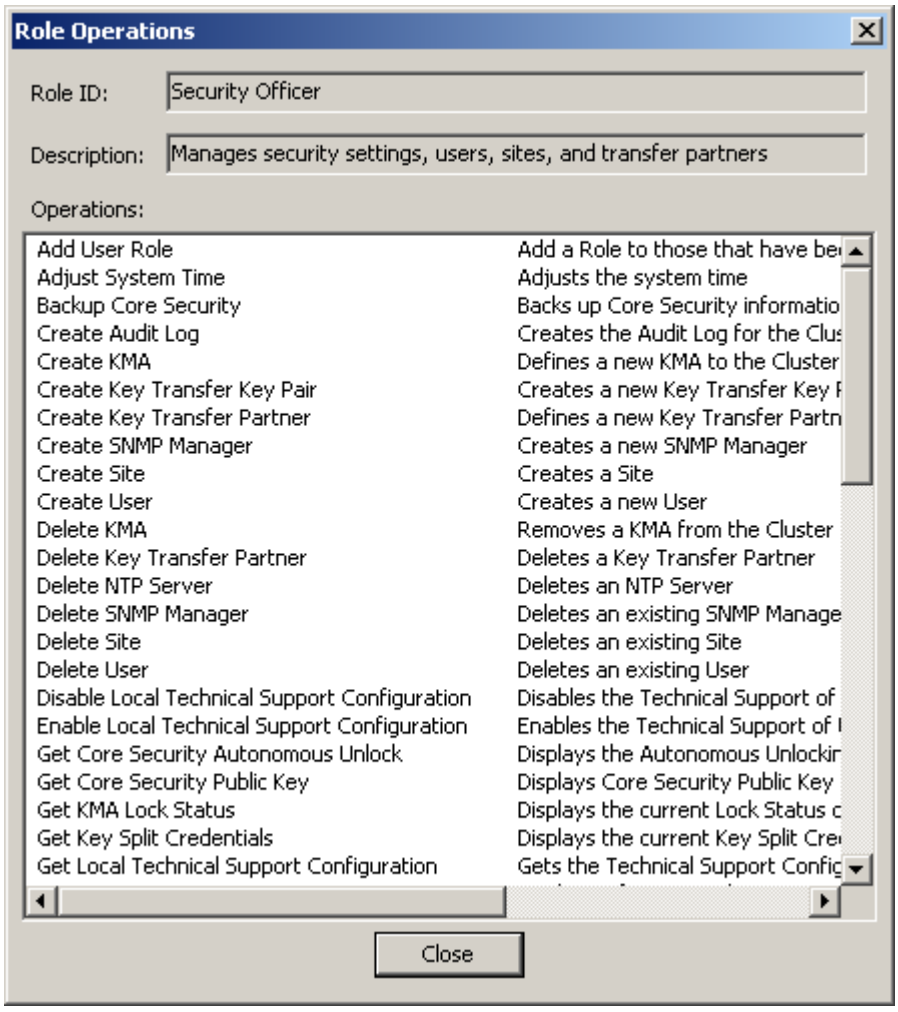
ロールの詳細情報を表示する場合は、そのロールエントリを強調表示して「Details」ボタンを選択します。詳細は、102 ページの「ロールの操作の表示」を参照してください。

ロールの操作の表示

「Role Operations」ダイアログボックスを使用すると、ロールとそのロールで許可されている操作を表示できます。

特定のロールの操作を表示するには、次の手順を実行します。

1. 「Role List」画面で、ロールを強調表示して「Details」ボタンを選択します。「Role Operations」ダイアログボックスが表示され、選択したロールの操作が示されます。



2. このダイアログボックスを閉じるには、「Close」ボタンを選択します。「Role List」画面に戻ります。

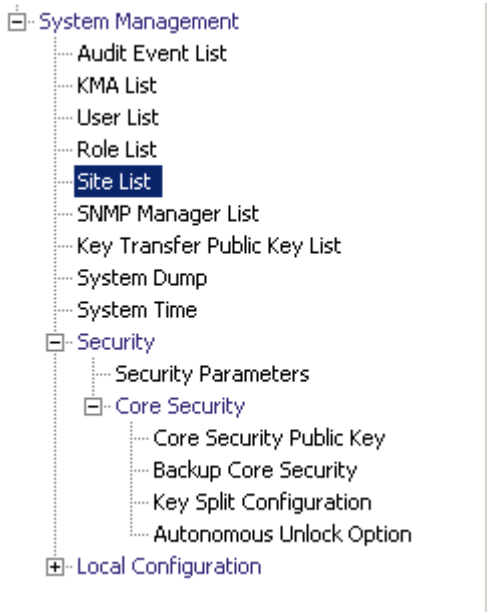
「Site List」メニュー

サイトとは、複数のエージェント (ホストと KMS クラスタ) の接続先となる、1 つ以上の KMA が存在する物理的な場所です。エージェントは、遠隔のサイトではなくローカルのサイトにある別の KMA に接続することによって、KMA の障害や負荷分散により効率的に対応できます。

「Site List」メニューオプションを使用すると、次の操作を行うことができます。

- サイトの表示
- サイトの作成
- サイトの情報の変更
- サイトの削除

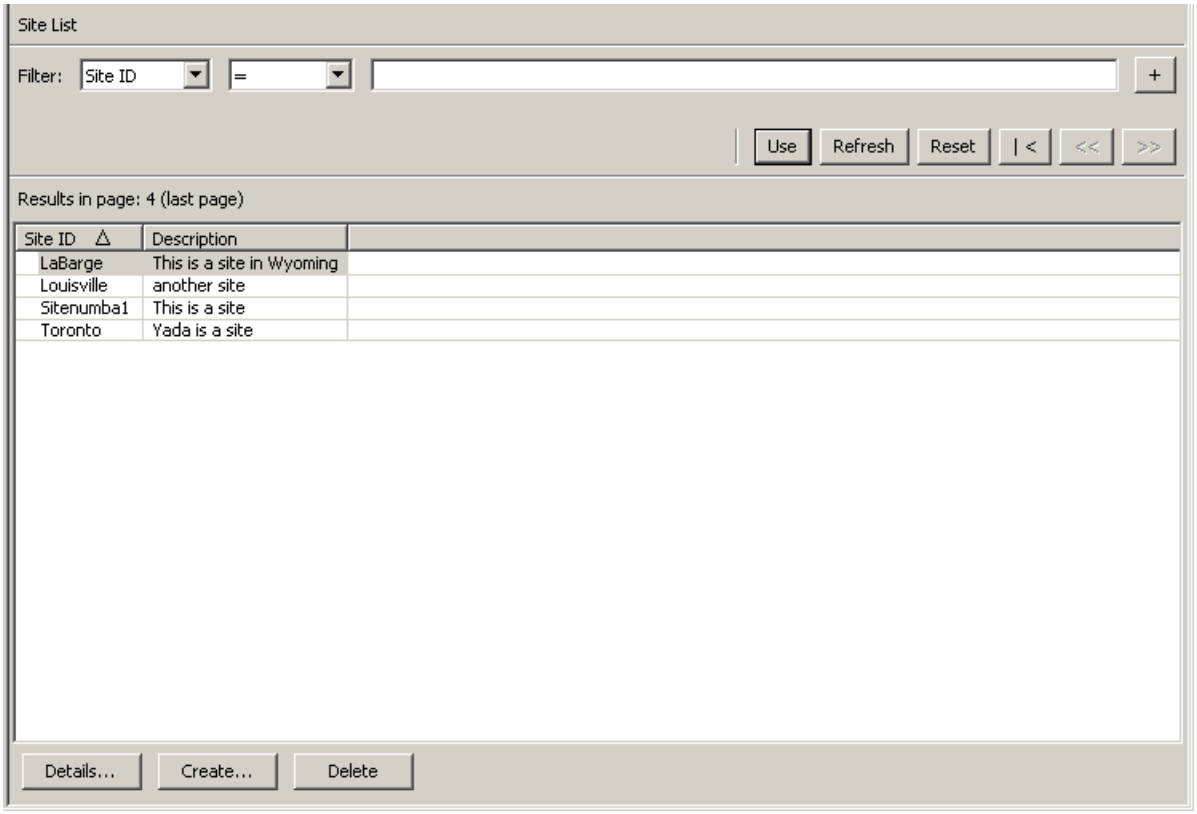
注 – オペレータは、サイトの表示のみを行うことができます。セキュリティー責任者は、サイトを管理できます。



サイトの表示

サイトを表示するには、次の手順を実行します。

「System Management」メニューから、「Site List」を選択します。「Site List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでサイトリストにフィルタを適用することもできます。

- Site ID
- Description

表示されているサイトリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Site ID
- Description

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~

フィルタ値 1 ボックス:

このフィールドに値を入力します。

Use:

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Site ID

サイトが一意に識別されます。

Description

サイトの説明が示されます。

サイトを作成するには、「Create」ボタンを選択します。詳細は、106 ページの「サイトの作成」を参照してください。

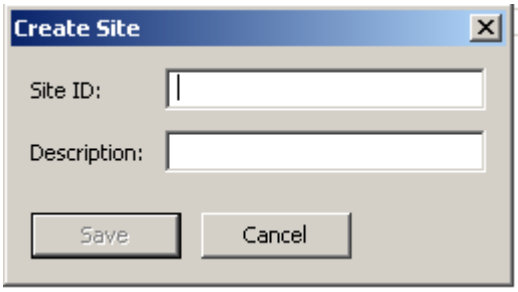
サイトの詳細情報を表示または変更する場合は、そのサイトを強調表示して「Details」ボタンを選択します。詳細は、108 ページの「サイトの詳細の表示および変更」を参照してください。

選択したサイトを削除するには、「Delete」ボタンを選択します。詳細は、109 ページの「サイトの削除」を参照してください。

サイトの作成

サイトを作成するには、次の手順を実行します。

1. 「Site List」画面で、「Create」ボタンを選択します。「Create Site」ダイアログボックスが表示されます。



2. 次のパラメータを設定します。

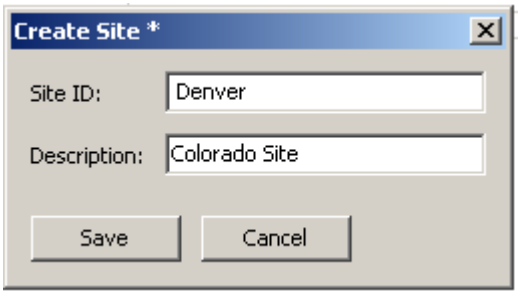
Site ID

サイトを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

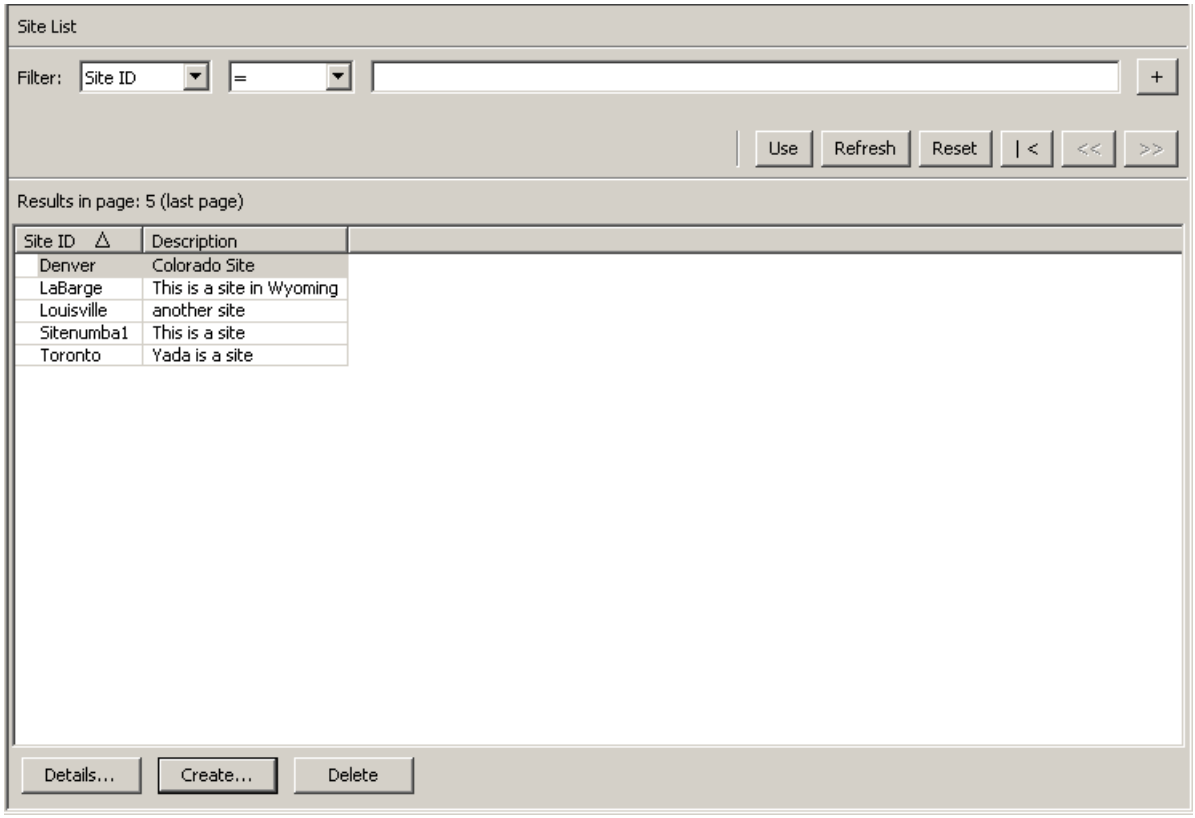
Description

サイトを一意に説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

次に、値を入力したダイアログボックスの例を示します。



3. 「Save」ボタンを選択します。新しいサイトが保存されてデータベースに格納され、「Site List」に表示されます。

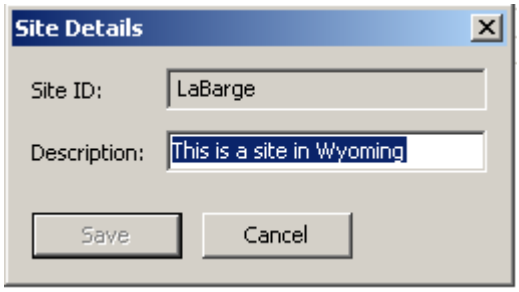

Site List
Filter:
Site ID
=
+
Use
Refresh
Reset
| <
<<
>>
Results in page: 5 (last page)
Site ID
Description
Denver
Colorado Site
LaBarge
This is a site in Wyoming
Louisville
another site
Sitenumba1
This is a site
Toronto
Yada is a site
Details...
Create...
Delete

サイトの詳細の表示および変更

注 – セキュリティー責任者以外のユーザーがサイトの詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。

サイトの詳細を変更するには、次の手順を実行します。

1. 「Site List」画面で、「Details」ボタンを選択します。「Site Details」ダイアログボックスが表示されます。



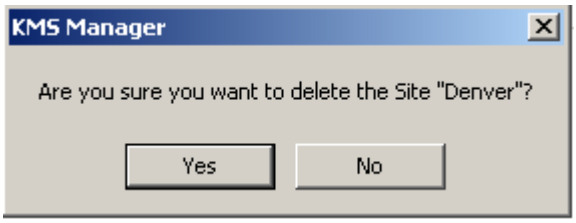
2. 「Description」フィールドを変更し、「Save」ボタンを選択します。サイトの詳細が変更され、データベースに格納されます。

サイトの削除

注 – サイトが使用されている場合、つまりサイトにエージェントまたは KMA が指定されている場合は、サイトを削除する前に、これらのエージェントや KMA を削除するか、または別のサイトに変更する必要があります。

サイトを削除するには、次の手順を実行します。

1. 「Site List」画面で、削除するサイトを強調表示して「Delete」ボタンを選択します。次のように、操作を確認するダイアログボックスが表示されます。



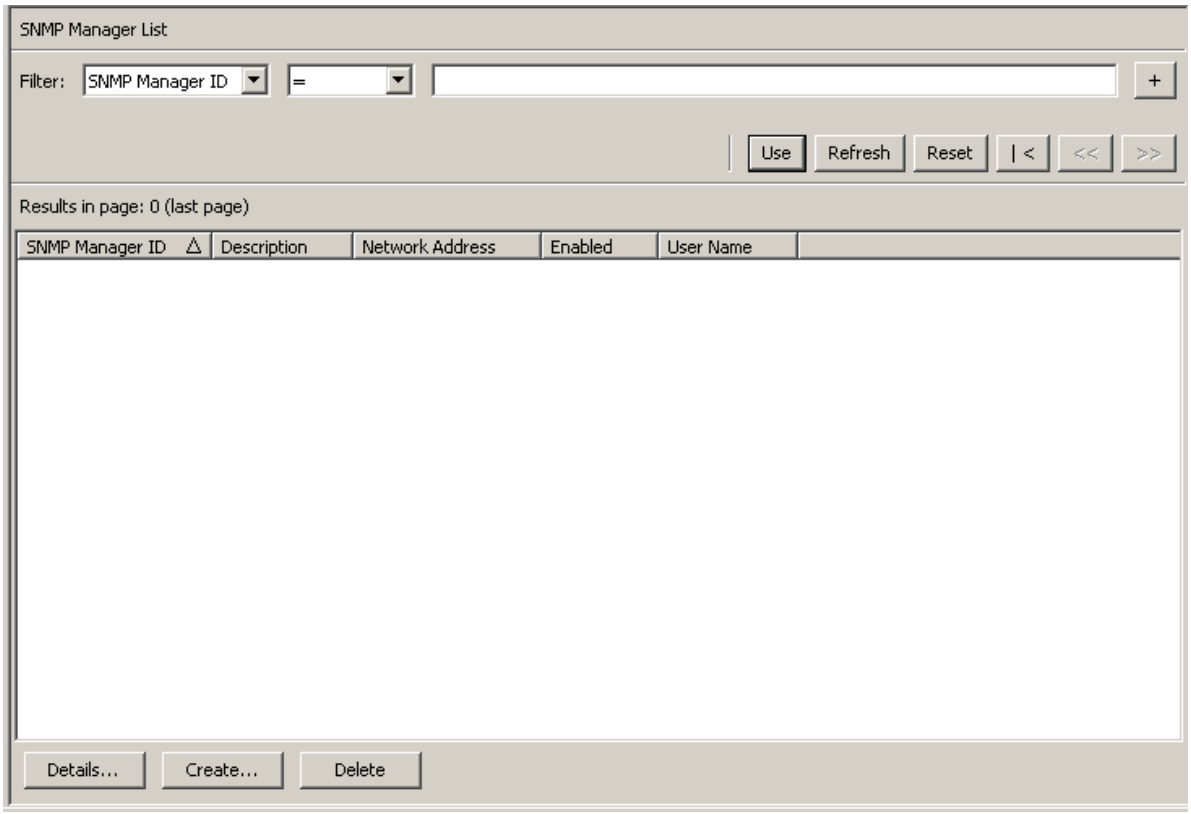
2. 「Yes」ボタンを選択して、サイトを削除します。現在選択しているサイトが削除され、「Site List」画面に戻ります。

「SNMP Manager List」メニュー

KMA の SNMP マネージャーの表示

SNMP マネージャーを表示するには、次の手順を実行します。

「System Management」メニューから、「SNMP Manager List」を選択します。「SNMP Manager List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで SNMP マネージャーリストにフィルタを適用することもできます。

- SNMP Manager ID
- Description
- Network Address
- Enabled
- User Name

表示されている SNMP マネージャーリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- SNMP Manager ID
- Description
- Network Address
- Enabled
- User Name

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 ボックス:

このフィールドに値を入力します。

Use:

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

SNMP Manager ID

ユーザーが定義した SNMP マネージャーの一意の識別子が表示されます。

Description

SNMP マネージャーの説明が表示されます。このフィールドは省略可能です。

Network Address

SNMP トラップの送信時に使用するネットワークアドレスが表示されます。

Enabled

SNMP マネージャーが使用可能かどうかが示されます。

User Name

この SNMP マネージャーに対してセキュリティー保護された信頼できる SNMPv3 接続を確立するときに使用されたユーザー名が表示されます。

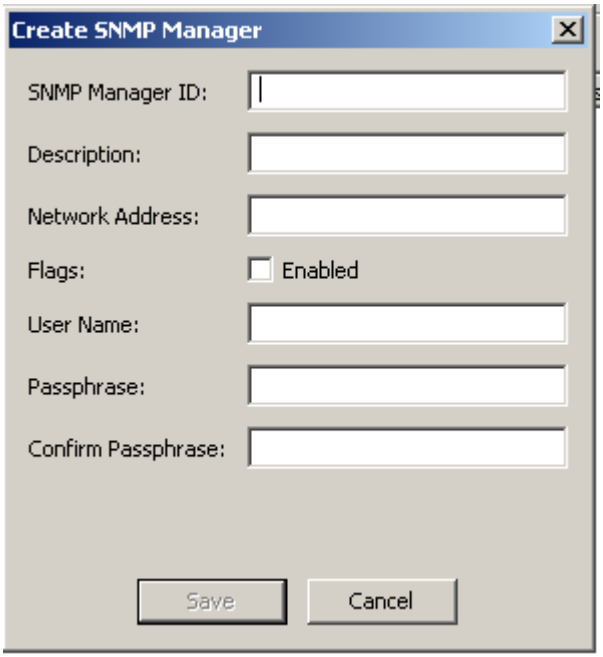
新しい SNMP マネージャーを作成するには、「Create」ボタンを選択します。詳細は、113 ページの「新しい SNMP マネージャーの作成」を参照してください。

SNMP マネージャーの詳細情報を表示または変更する場合は、そのエントリを強調表示して「Details」ボタンを選択します。詳細は、114 ページの「SNMP マネージャーの詳細の表示および変更」を参照してください。

選択した SNMP マネージャーを削除するには、「Delete」ボタンを選択します。詳細は、115 ページの「SNMP マネージャーの削除」を参照してください。

新しい SNMP マネージャーの作成

1. 「SNMP Manager List」画面で、「Create」ボタンを選択します。「Create SNMP Manager」ダイアログボックスが表示されます。



2. 次のパラメータを設定します。

SNMP Manager ID

SNMP マネージャーを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

Description

SNMP マネージャーを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Network Address

SNMP マネージャーのネットワークアドレスを入力します。

Flags - Enabled

このチェックボックスの選択によって、SNMP を使用可能にするかどうかを示します。

User Name

SNMP マネージャーの認証に使用するユーザー名を入力します。

Passphrase

SNMP マネージャーの認証に使用するパスフレーズを入力します。

Confirm Passphrase

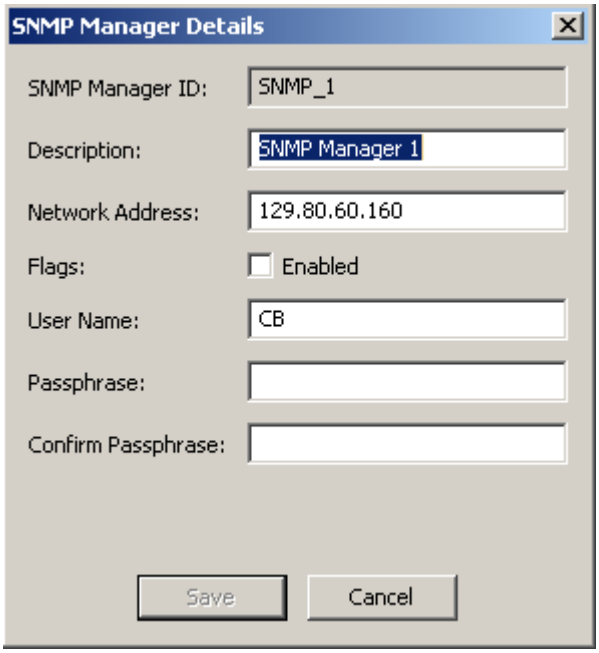
「Passphrase」フィールドに入力したパスフレーズと同じ値を入力します。

3. 終了したら、「Save」ボタンを選択して情報を保存します。新しい SNMP マネージャーエントリと、それに関連するプロファイルがデータベースに格納されます。

SNMP マネージャーの詳細の表示および変更

SNMP マネージャーの詳細を表示または変更するには、次の手順を実行します。

1. 「SNMP Manager List」画面で、詳細情報を表示する SNMP マネージャーエントリをダブルクリックし、「Details」ボタンを選択します。「SNMP Manager Details」ダイアログボックスが表示されます。



2. 必要に応じて、パラメータを変更します。

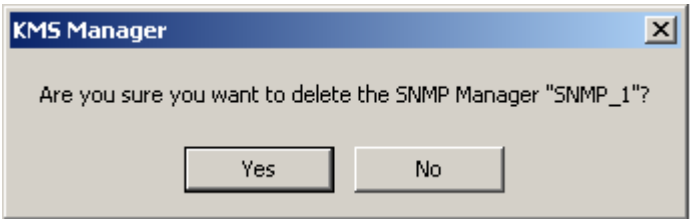
3. 終了したら、「Save」ボタンを選択して変更内容を保存します。

注 – SNMP マネージャーの詳細を変更するたびに、パスフレーズを再指定する必要があります。

SNMP マネージャーの削除

SNMP マネージャーを削除するには、次の手順を実行します。

1. 「SNMP Manager List」画面で、削除する SNMP マネージャーを強調表示して「Delete」ボタンを選択します。SNMP マネージャーの削除を確認するダイアログボックスが表示されます。



2. 「Yes」ボタンを選択して、SNMP マネージャーを削除します。現在選択している SNMP マネージャーが削除され、「SNMP Manager List」画面に戻ります。

鍵転送

概要

鍵転送は鍵共有とも呼ばれ、鍵と関連データユニットをパートナー間で安全に交換することを可能にします。また、暗号化された媒体を交換するためにも必要です。この処理では、転送の送信側と受信側の両方が公開鍵と非公開鍵のペアを設定して、相手側に公開鍵を提供する必要があります。

送信側と受信側はそれぞれ、相手側の公開鍵を自身の KMS クラスタに入力します。この初期設定が完了すると、送信側は鍵のエクスポートを使用して転送ファイルを生成します。このファイルが送信側から受信側に送信されます。次に、受信側が鍵のインポートを使用して、鍵とそれに関連付けられたデータユニットを受信側の KMS クラスタにインポートします。

転送ファイルは、送信側の非公開鍵を使用して署名され、受信側の公開鍵を使用して暗号化されます。これにより、受信側のみが自身の非公開鍵を使用して転送ファイルを復号化できます。受信側は、送信側の公開鍵を使用して、ファイルが実際に想定した送信側によって作成されたファイルであることを確認できます。

鍵転送パートナー機能

鍵転送パートナー機能を使用すると、KMS クラスタ間で鍵を移動できます。通常、会社間でテープを交換する場合、または多数のサイトに対処するために社内に複数のクラスタが構成されている場合に、この機能を使用できます。

鍵転送処理では、次の手順を実行します。

- 各 KMS クラスタで、別のクラスタを転送パートナーとして設定します。通常、この設定は 1 回だけ行います。
- ユーザーは、一方の KMS クラスタから鍵をエクスポートし、もう一方のクラスタにその鍵をインポートします。この手順は、何回でも実行できます。

鍵転送処理

KMS 内では、多数のタスクを特定の順序で実行する必要があります。これらのタスクには複数のユーザーロールが関連しているため、実際の手順については、このマニュアルの複数の章で説明します。

鍵転送パートナーの設定

鍵を移動するには、鍵の移動に関与する両方の KMS クラスタに鍵転送パートナーを設定します。

次の手順では、「C1」は 1 つめの KMS クラスタ、「C2」は 2 つめの KMS クラスタを指しています。

C1 管理者 (セキュリティー責任者ロール):

1. C1 (ユーザーのクラスタ) の公開鍵情報を取得します。この操作を行うには、「Key Transfer Public Key List」メニューに移動します。131 ページの「「Key Transfer Public Key List」の表示」および 134 ページの「鍵転送用公開鍵の詳細の表示」を参照してください。

2. 公開鍵 ID と公開鍵を電子メールまたはその他の合意済みの通信形式にカット&ペーストします。この情報を C2 管理者に送信します。

注 – C2 がこの情報を受信したとき、その情報は実際に C1 から送信されたものであると確信できるように、通信方法は十分にセキュリティー保護されている必要があります。情報が送信中に改ざんされることを防ぐために、フィンガープリントという機構があります。

C2 管理者 (セキュリティー責任者ロール):

3. C2 管理者: 「Transfer Partner List」メニューにアクセスし、C1 からの公開鍵情報を KMS クラスタに入力します。121 ページの「「Transfer Partner List」メニュー」を参照してください。

4. 「Create...」ボタンをクリックします。転送パートナーの名前、説明、および連絡先情報を入力します。このパートナーとの間で行う処理を設定します。125 ページの「転送パートナーの作成」を参照してください。

5. 「Public Keys」タブを選択します。C1 から提供された情報から、公開鍵 ID と公開鍵を入力します。

   公開鍵を入力すると、システムによってフィンガープリントが計算されます。C1 管理者と C2 管理者との間の通信には、鍵自体の転送に使用したものとは別の機構を使用することをお勧めします。

   両方の管理者は、各自の KMS で、フィンガープリントが一致することを確認する必要があります。フィンガープリントが一致しない場合は、転送中に鍵が壊れたか、または変更されたことを示します。

6. フィンガープリントが一致した場合は、「Save」をクリックします。システムから定足数の入力が求められます。定足数が求められるのは、この手順で使用可能にする鍵のエクスポート操作が、KMS クラスタから有効な鍵を抽出するために使用される可能性があるためです。これで、C1 は C2 KMS クラスタ内で転送パートナーとして設定されました。

C2 管理者 (セキュリティー責任者ロール):

7. 今度は C2 KMS クラスタで、手順 1 ～手順 2 を繰り返します。

C1 管理者 (セキュリティー責任者ロール):

8. 手順 3 ～手順 6 を繰り返して、C2 の公開鍵を C1 に追加します。

C1 管理者 (コンプライアンス責任者ロール):

9. C1 では、C2 に送信できる鍵グループを設定する必要があります。201 ページの「鍵グループ割り当ての表示」を参照してください。

C2 管理者 (コンプライアンス責任者ロール):

10. C2 では、C1 から鍵を受信できる鍵グループを設定する必要があります。201 ページの「鍵グループ割り当ての表示」を参照してください。

11. 必要な転送パートナーを選択します。

12. 許可されていない鍵グループを 1 つ以上選択し、「Move to」  ボタンをクリックして鍵グループリストに追加します。202 ページの「転送パートナーへの鍵グループの追加」を参照してください。

鍵のエクスポートおよびインポート

次の手順は、ある KMS クラスタから別のクラスタに対して、鍵のエクスポートおよびインポートを行う場合に使用します。この手順は、何回でも実行できます。

次の手順では、「C1」は 1 つめの KMS クラスタ、「C2」は 2 つめの KMS クラスタを指しています。この手順では、C2 で鍵をエクスポートし、その鍵を C1 にインポートできるようにする方法について説明します。

C2 管理者 (オペレータロール):

1. 鍵を交換するには、「Data Unit List」画面に移動します。233 ページの「データユニットの表示」を参照してください。
2. C2 から C1 に送信するデータユニット (テープ) を 1 つ以上選択します。外部タグは、テープ上のバーコードです。
3. 「Export Keys」ボタンをクリックし、ダイアログボックスを表示します。
4. 宛先の転送パートナーを選択し、必要に応じて鍵のエクスポートファイル名を選択して「Start」をクリックします。転送ファイルが作成されます。

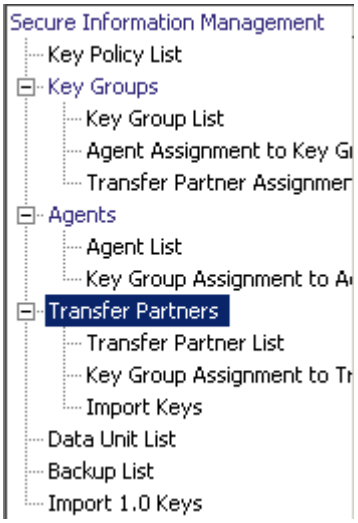
   C1 へのエクスポートが許可されている鍵グループに属する鍵のみがエクスポートされます。
5. 電子メールまたは別の合意済みの通信形式、またはファイルを移動するメカニズムを使用して、転送ファイルを C1 管理者に送信します。

C1 管理者 (オペレータロール):

6. 「Import Keys」画面を選択します。230 ページの「「Import Keys」メニュー」を参照してください。
7. 鍵のインポート先になる宛先の鍵グループ、鍵をエクスポートした送信側転送パートナー (この場合は C2)、および鍵転送のファイル名を指定します。選択する鍵グループは、C2 から鍵を受信するように設定された鍵グループである必要があります。
8. 「Start」をクリックします。

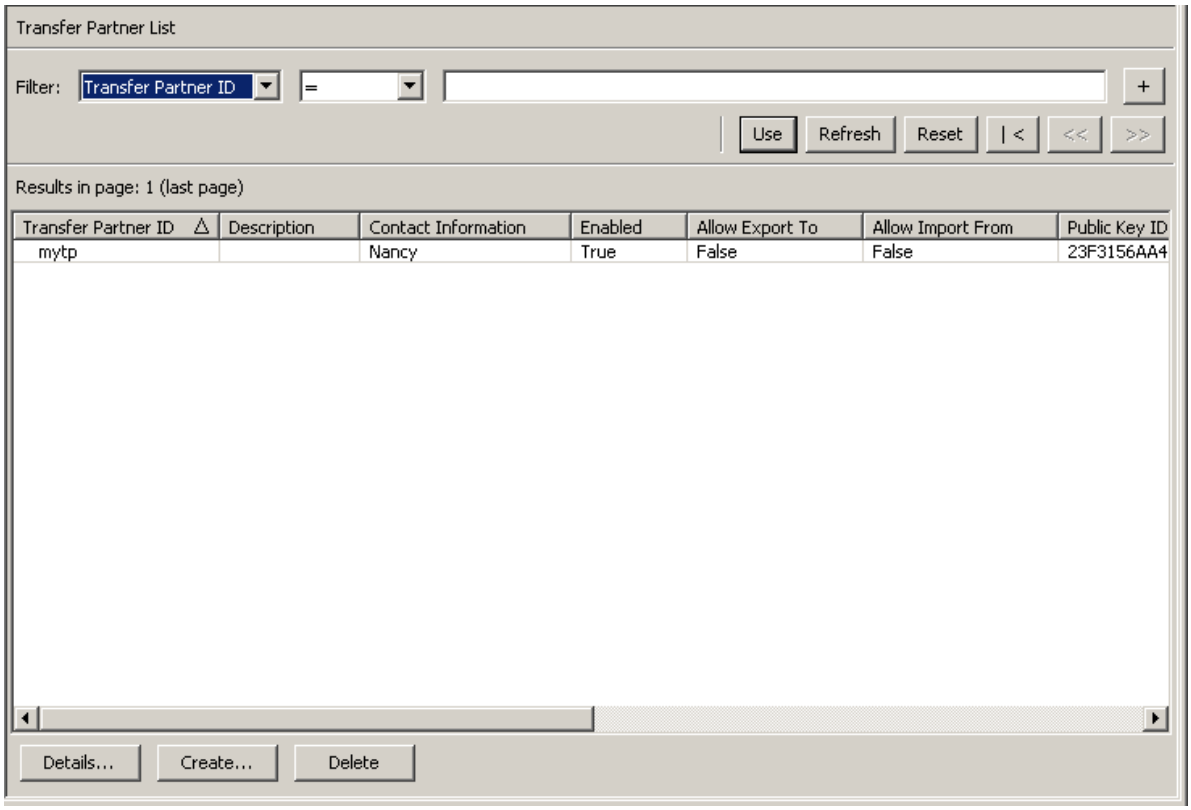
「Transfer Partners」メニュー

鍵転送パートナー機能を使用すると、KMS クラスタ間で鍵を移動できます。



「Transfer Partner List」メニュー

「Secure Information Management」メニューから、「Transfer Partner List」を選択します。



データベース全体をスクロールするか、次のいずれかのキーで転送パートナーリストにフィルタを適用することもできます。

- Transfer Partner ID
- Description
- Contact Information
- Enabled
- Allow Export To
- Allow Import From

表示されている転送パートナーリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

表示されている転送パートナーのリストにフィルタを適用するためのフィルタオプションを選択します。すべてのフィルタの条件を満たす転送パートナーのみが表示されます。

フィルタ属性コンボボックス:

下矢印ボタンをクリックし、フィルタ条件として使用する属性を選択します。次に示す値を取ります。

- Transfer Partner ID
- Description
- Contact Information
- Enabled
- Allow Export To
- Allow Import From

フィルタ演算子コンボボックス:

下矢印ボタンをクリックし、選択した属性に適用するフィルタ演算子を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス:

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス:

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

Use:

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

Refresh:

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、項目数に「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

Transfer Partner ID:

各転送パートナーを識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

Description:

転送パートナーについて説明します。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

Contact Information:

転送パートナーの連絡先情報が表示されます。この属性でソートするには、この列名をクリックします。

Enabled:

転送パートナーに鍵の共有が許可されているかどうかが示されます。True または False の値を取ります。このフィールドが False の場合、転送パートナーは鍵を共有できません。この属性でソートするには、この列名をクリックします。

Allow Export To:

転送パートナーに鍵のエクスポートが許可されているかどうかが示されます。True または False の値を取ります。このフィールドが False の場合、転送パートナーは鍵をエクスポートできません。この属性でソートするには、この列名をクリックします。

Allow Import From:

この転送パートナーから鍵をインポートできるかどうかが示されます。True または False の値を取ります。このフィールドが False の場合、この転送パートナーから鍵をインポートできません。この属性でソートするには、この列名をクリックします。

Public Key ID

各公開鍵を識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

Public Key Fingerprint

公開鍵のフィンガープリント (ハッシュ値) が表示されます。

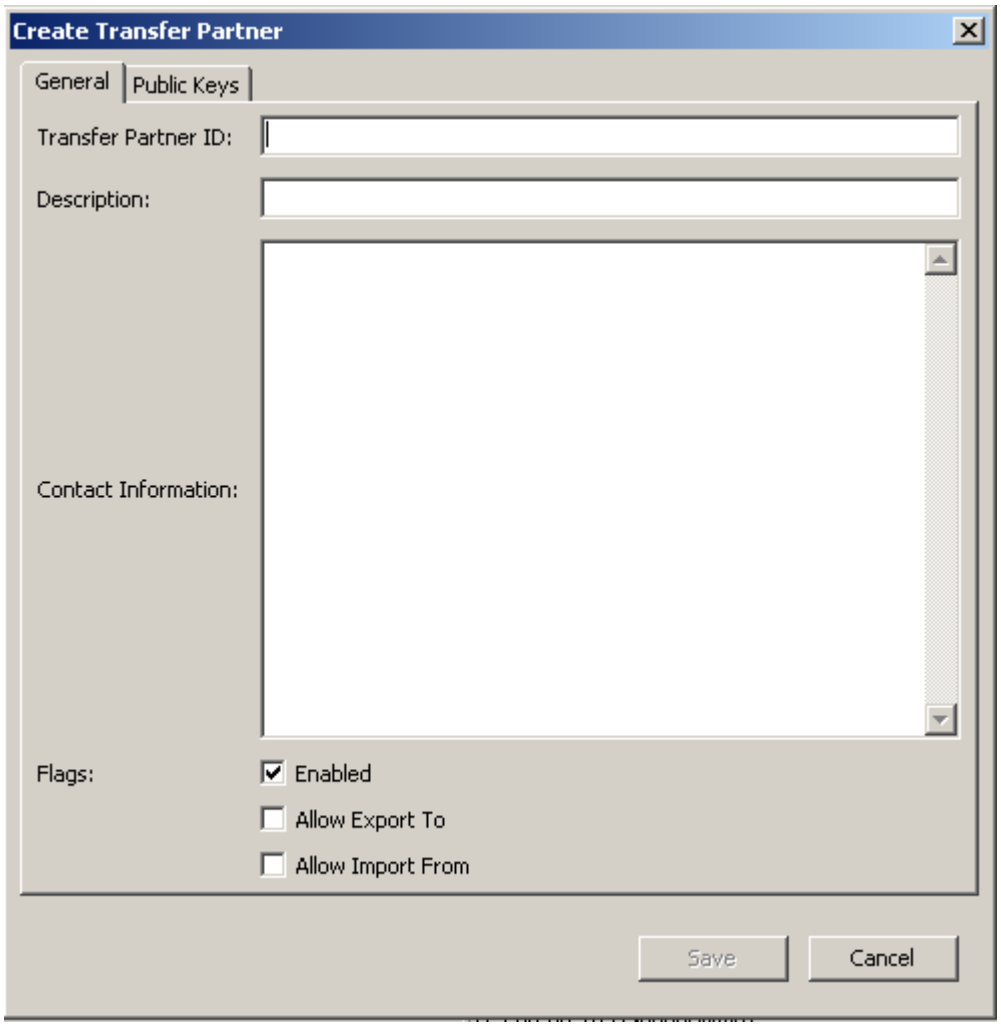
Entry Date

公開鍵が KMS クラスタに格納された日付が表示されます。

転送パートナーの作成

転送パートナーを作成するには、次の手順を実行します。

1. 「Transfer Partner List」画面で、「Create」ボタンを選択します。「Create Transfer Partner」ダイアログボックスが表示され、「General」タブがアクティブになっています。



2. 次のパラメータを設定します。

「General」タブ

Transfer Partner ID

転送パートナーが一意に識別されます。

Description

転送パートナーを一意に説明する値を入力します。この値は、1 ～ 64 文字で指定できます。このフィールドは、空白のままにすることができます。

Contact Information

転送パートナーの連絡先情報を識別する値を入力します。このフィールドは、空白のままにすることができます。

Flags - Enabled

この転送パートナーに鍵の共有を許可するには、このボックスにチェックマークを付けます。このフィールドが選択されていない場合、転送パートナーは鍵を共有できません。

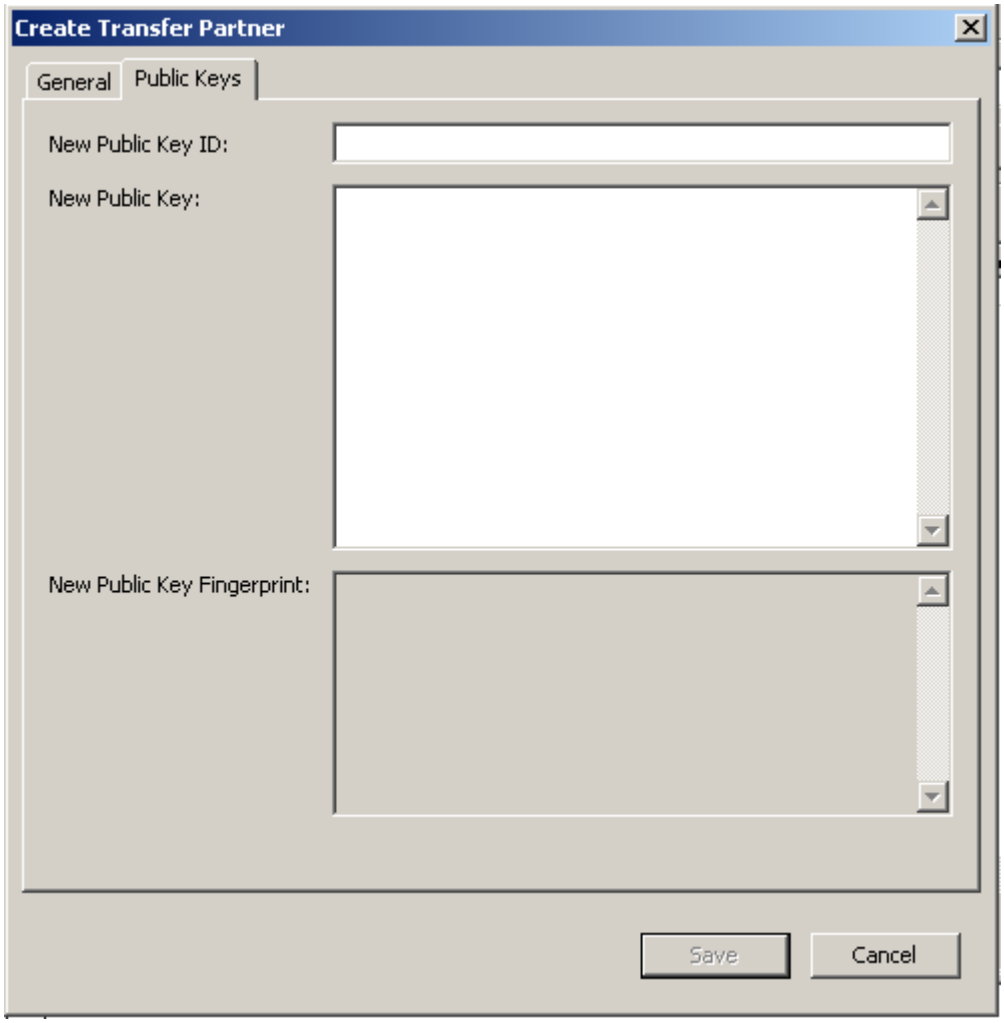
Allow Export To

転送パートナーへの鍵のエクスポートを許可するには、このボックスにチェックマークを付けます。このフィールドが選択されていない場合、転送パートナーは鍵のエクスポート操作を実行できません。

Allow Import From

この転送パートナーから鍵をインポートできるように指定するには、このボックスにチェックマークを付けます。このフィールドが選択されていない場合、この転送パートナーから鍵をインポートできません。

3. 「Public Keys」タブを開きます。



「Public Keys」タブ

New Public Key ID

転送パートナーから提供された公開鍵 ID を入力します。

New Public Key

転送パートナーから提供された公開鍵を入力します。

New Public Key Fingerprint

この読み取り専用のフィールドには、新しい公開鍵のフィンガープリント (ハッシュ値) が表示されます。このフィンガープリントをパートナーと照合して、伝送中に偶然または故意に公開鍵が改ざんされていないことを確認します。

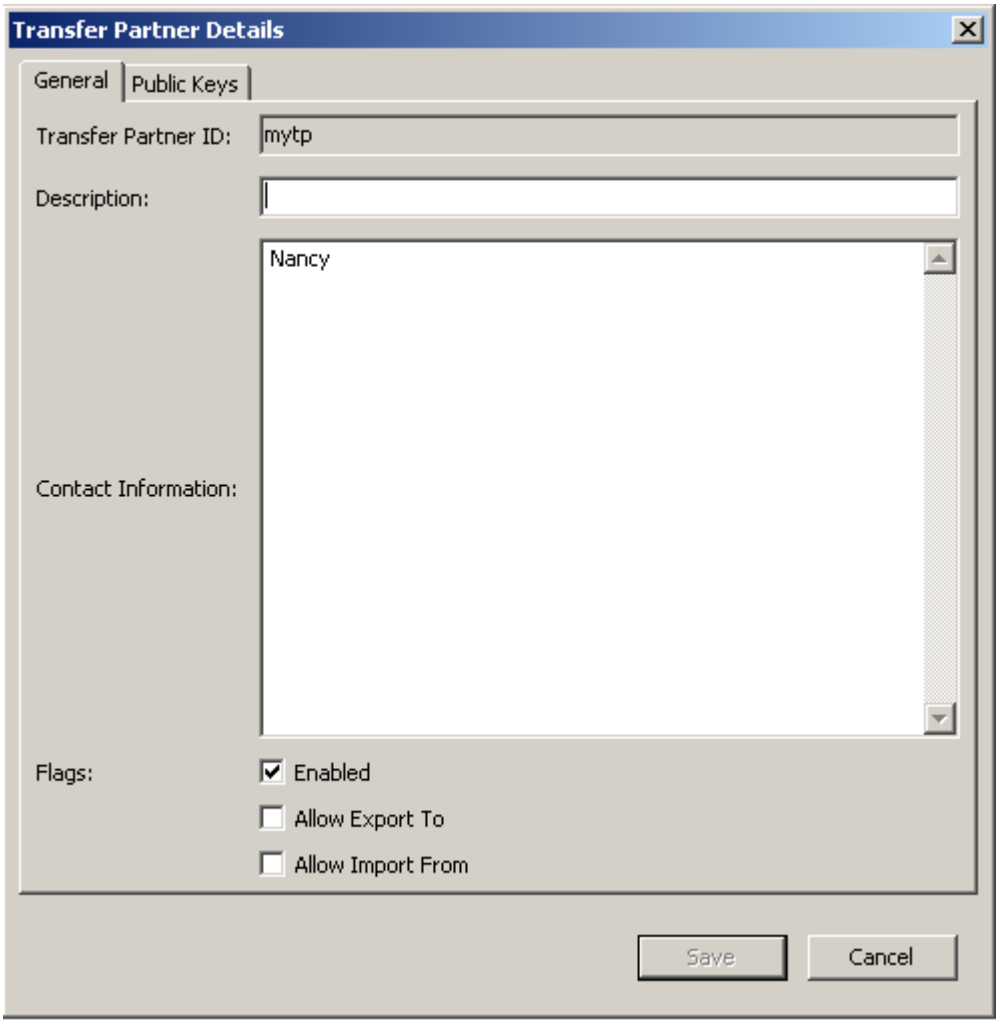
4. 終了したら、「Save」ボタンを選択します。

転送パートナーの詳細の表示および変更

「Transfer Partner Details」ダイアログボックスを使用すると、特定の転送パートナーに関する詳細情報を表示できます。

詳細を表示するには、次の手順を実行します。

1. 「Transfer Partner List」画面で、転送パートナー ID を強調表示して「Details」ボタンを選択します。「Transfer Partner Details」ダイアログボックスが表示されます。



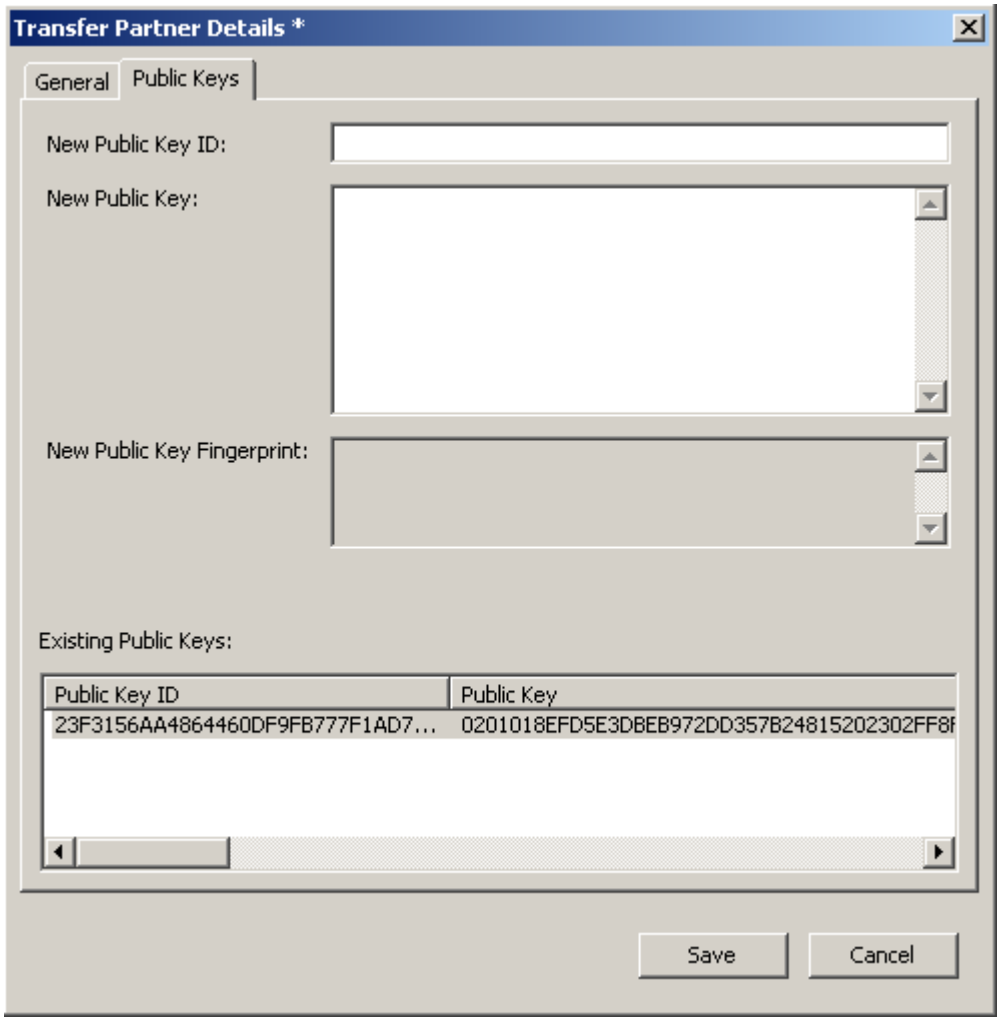
「General」タブ

2. 「General」タブでは、次のフィールドを変更できます。

- Description
- Contact Information
- Flags - Enabled
- Allow Export To
- Allow Import From

「Transfer Partner ID」フィールドは、読み取り専用です。

3. 終了したら、「Save」ボタンを選択します。データベース内の転送パートナーレコードが変更されます。
4. 「Public Keys」タブを開きます。



「Public Keys」タブ

5. 「Public Keys」タブでは、次のフィールドを変更できます。

New Public Key ID

転送パートナーから提供された新しい公開鍵 ID を入力します。

New Public Key

転送パートナーから提供された新しい公開鍵を入力します。

New Public Key Fingerprint

この読み取り専用のフィールドには、新しい公開鍵のフィンガープリント (ハッシュ値) が表示されます。この鍵が正しいかどうかを送信側転送パートナーに確認します。

Existing Public Keys

このリストには、この転送パートナーと関連付けられた公開鍵が表示されます。

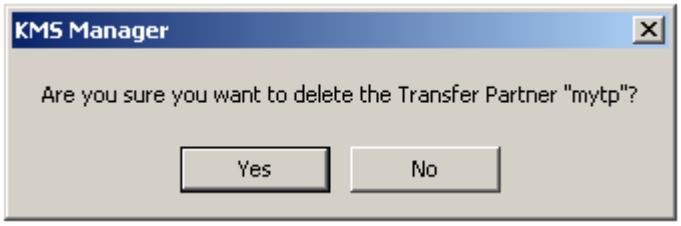
6. 終了したら、「Save」ボタンを選択します。

転送パートナーの削除

このオプションを使用すると、セキュリティー責任者は、転送パートナーを削除できます。

転送パートナーを削除するには、次の手順を実行します。

1. 「Transfer Partner List」画面で、削除する転送パートナー ID を強調表示して「Delete」ボタンを選択します。転送パートナーの削除を確認するダイアログボックスが表示されます。



2. 「Yes」ボタンを選択して、転送パートナーを削除します。現在選択している転送パートナーが削除され、「Transfer Partner List」画面に戻ります。

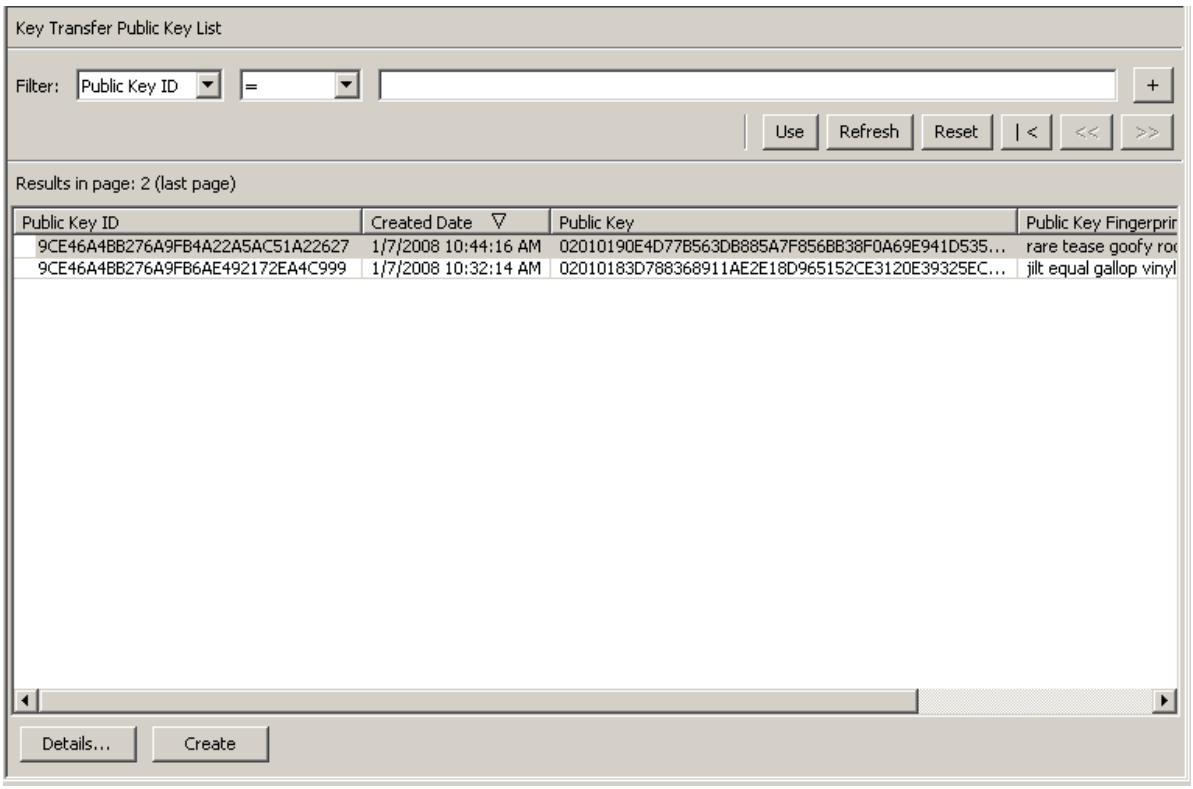
「Key Transfer Public Key List」メニュー

転送パートナー間で鍵を共有する場合、セキュリティー責任者は、まず自身の KMS クラスタの公開鍵情報にアクセスする必要があります。このメニューを使用すると、公開鍵情報を表示できます。このコマンドで表示される公開鍵と公開鍵 ID を、転送パートナーに送信する必要があります。

「Key Transfer Public Key List」の表示

鍵転送用の公開鍵リストを表示するには、次の手順を実行します。

「System Management」メニューから、「Key Transfer Public Key List」を選択します。



データベース全体をスクロールするか、次のいずれかのキーで鍵転送用公開鍵リストにフィルタを適用することもできます。

- Public Key ID
- Created Date
- Public Key

表示されている公開鍵リストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

表示されている公開鍵のリストにフィルタを適用するためのフィルタオプションを選択します。すべてのフィルタの条件を満たす鍵転送用公開鍵のみが表示されます。

フィルタ属性コンボボックス:

下矢印ボタンをクリックし、フィルタ条件として使用する属性を選択します。次に示す値を取ります。

- Public Key ID
- Created Date
- Public Key

フィルタ演算子コンボボックス:

下矢印ボタンをクリックし、選択した属性に適用するフィルタ演算子を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス:

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス:

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス:

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

Use:

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

Refresh:

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、項目数に「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

Public Key ID:

各公開鍵を識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

Created Date:

この公開鍵が作成された日時が表示されます。この属性でソートするには、この列名をクリックします。

もっとも最近作成された公開鍵に対応する非公開鍵は、エクスポートされたすべての鍵転送ファイルの署名に使用されます。

Public Key:

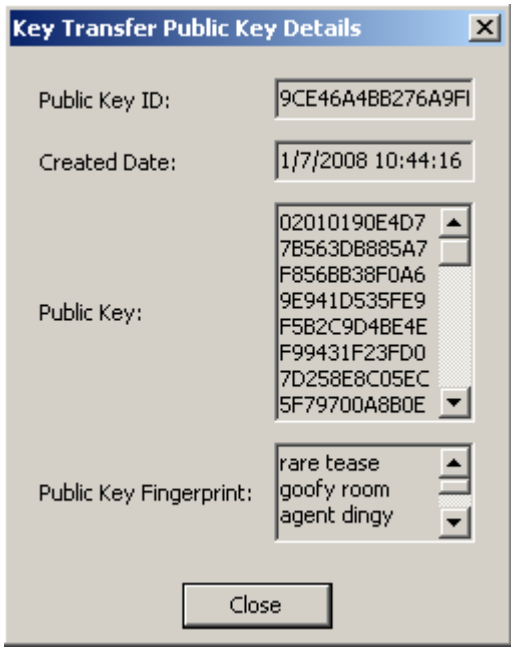
転送パートナー間での鍵転送の実行に使用される公開鍵が表示されます。この値は、Base 64 で表示されます。この属性でソートするには、この列名をクリックします。

Public Key Fingerprint:

公開鍵のハッシュ値が表示されます。これは公開鍵が正しく転送されたことを確認するために使用する値で、Base 64 で表示されます。

鍵転送用公開鍵の詳細の表示

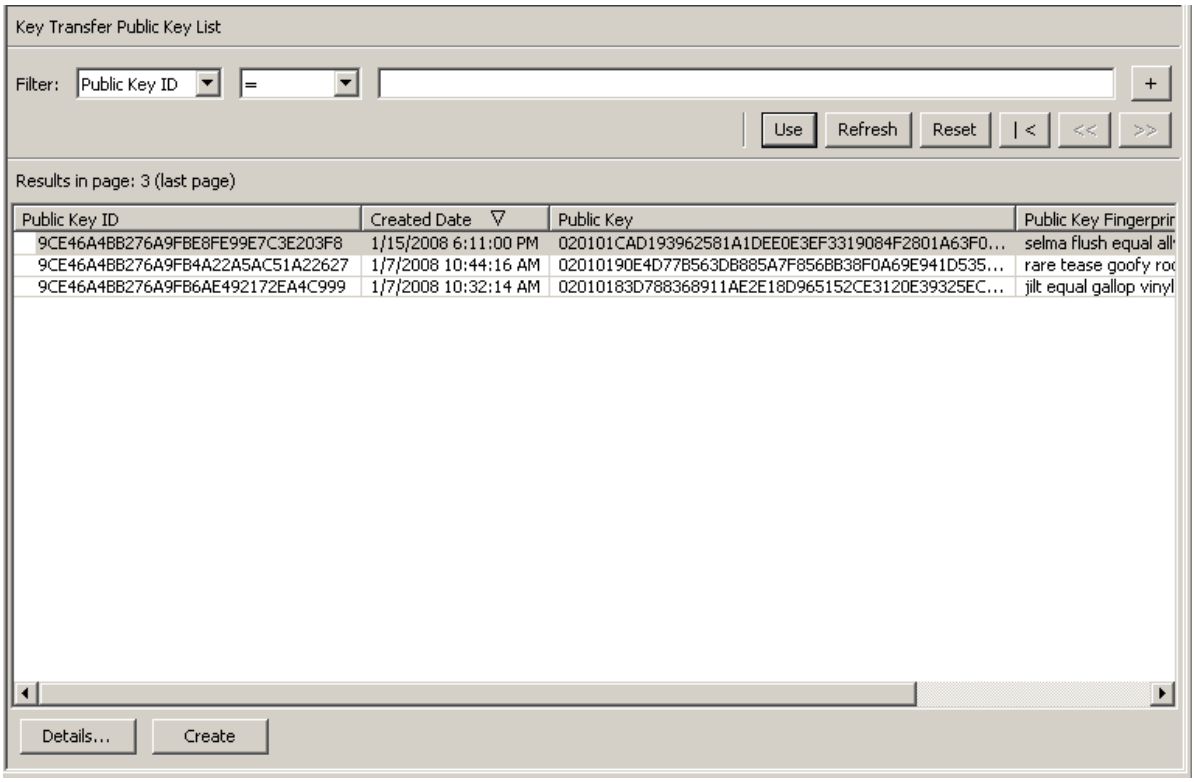
「Key Transfer Public Key Details」画面を表示するには、公開鍵を選択し、「Details」ボタンをクリックします。



鍵転送用公開鍵の作成

鍵転送用公開鍵を作成するには、「Create」ボタンをクリックします。

新しい鍵を作成したら、その鍵を既存のすべての転送パートナーに提供する必要があります。新しい鍵転送用公開鍵の作成後に作成したすべての鍵転送ファイルは、新しい鍵転送用公開鍵で署名されるため、パートナーに新しい鍵転送用公開鍵を提供しないと、パートナーは新しい鍵転送ファイルをインポートできません。



「Backup List」メニュー

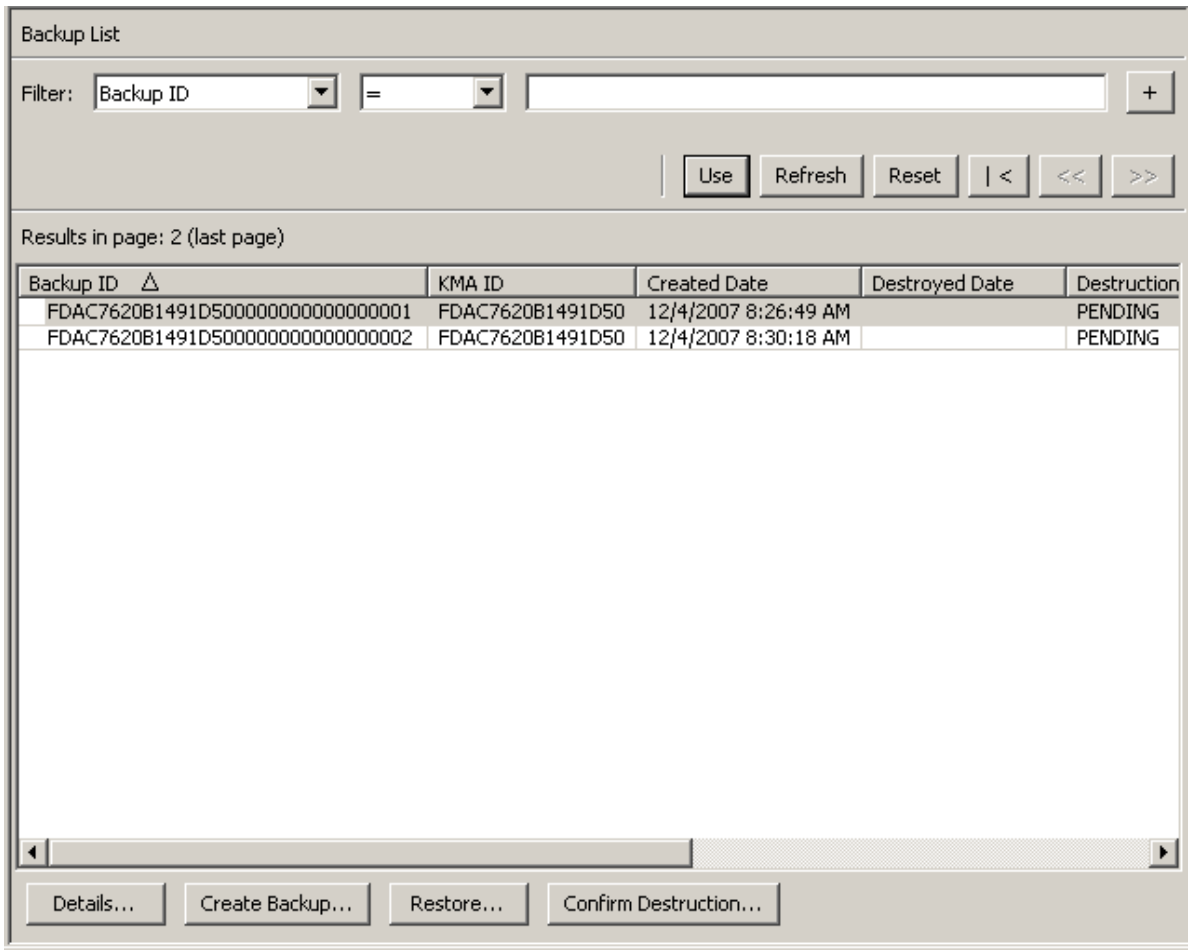
「Backup List」メニューオプションを使用すると、セキュリティー責任者は、次の操作を行うことができます。

- バックアップの履歴の表示
- バックアップファイルの詳細の表示
- バックアップの復元

バックアップファイルの履歴の表示

バックアップファイルの履歴を表示するには、次の手順を実行します。

「Secure Information Management」メニューから、「Backup List」を選択します。「Backup List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでバックアップファイルにフィルタを適用することもできます。

- Backup ID
- KMA ID
- Created Date
- Destroyed Date
- Destruction Status
- Destruction Comment

表示されているバックアップファイルのリストにフィルタを適用するには、「+」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Backup ID
- Created Date
- Destroyed Date
- Destruction Status
- Destruction Comment

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~

フィルタ値 1 ボックス:

日付フィルタを選択した場合は、「Set Date」をクリックして開始日時を指定します。値は、フィルタキーの範囲の開始値として表示されます。ほかのフィルタを選択した場合は、このフィールドに値を入力します。

フィルタ値 2 ボックス:

日付フィルタを選択した場合は、「Set Date」をクリックして終了日時を選択します。値は、フィルタキーの範囲の終了値として表示されます。

Use:

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Backup ID

各バックアップファイルを識別する一意のシステム生成識別子が表示されます。

KMA ID

バックアップファイルが生成された KMA が表示されます。

Created Date

バックアップが作成された日時が表示されます。

Destroyed Date

バックアップファイルが手動で破棄とマークされた日時が表示されます。

Destruction Status

破棄に関するバックアップの状態が表示されます。次に示す値を取ります。

NONE

バックアップファイルは破棄されておらず、ファイルには破棄されたデータユニットの鍵は含まれていません。

PENDING

バックアップファイルはまだ手動で破棄されておらず、ファイルには破棄されたデータユニットの鍵のコピーが含まれています。

DESTROYED

バックアップファイルは手動で破棄されています。

Destruction Comment

バックアップファイルの破棄に関するユーザーが指定した情報が表示されます。

Details:

このボタンをクリックすると、バックアップの詳細情報が表示されます。

Create Backup:

このボタンをクリックすると、バックアップが作成されます。セキュリティー責任者の場合、このボタンは使用不可になっています。

Restore:

このボタンをクリックすると、バックアップが復元されます。

Confirm Destruction:

このボタンをクリックすると、バックアップの破棄を確認できます。セキュリティー責任者の場合、このボタンは使用不可になっています。

バックアップの詳細情報を表示する場合は、そのバックアップを強調表示して「Details」ボタンを選択します。詳細は、140 ページの「バックアップの詳細の表示」を参照してください。

現在選択しているバックアップを復元するには、「Restore」ボタンを選択します。詳細は、142 ページの「バックアップの復元」を参照してください。

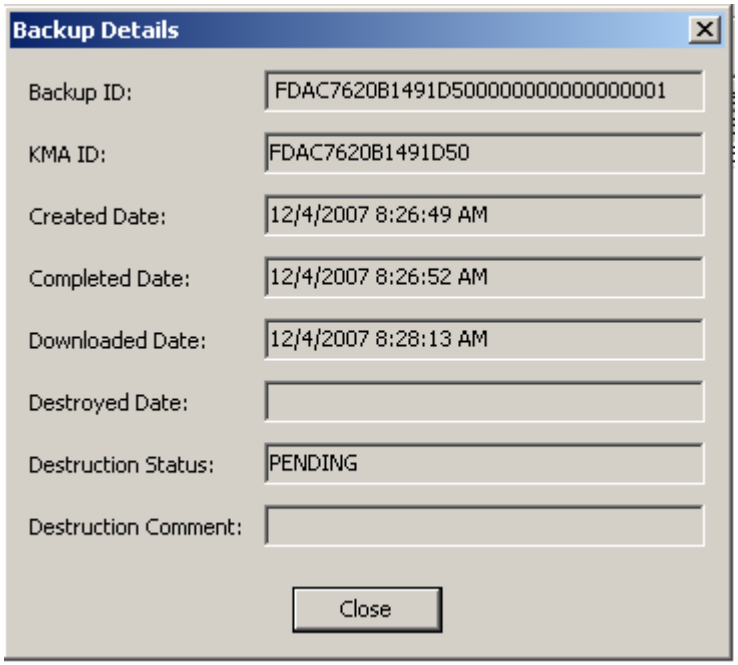
バックアップの詳細の表示

「Backup Details」ダイアログボックスは、バックアップファイルの詳細を表示する場合に使用します。

注 – バックアップファイルは KMA 上で作成および復元されます。

バックアップファイルの詳細を表示するには、次の手順を実行します。

1. 「Backups List」画面で、詳細情報を表示するバックアップエントリをダブルクリックするか、またはバックアップエントリを強調表示して「Details」ボタンを選択します。「Backup Details」ダイアログボックスが表示され、すべてのフィールドが読み取り専用になっています。



2. 次に、フィールドとその説明を示します。

Backup ID

各バックアップファイルを識別する一意のシステム生成識別子が表示されます。

KMA ID

このバックアップファイルが生成された KMA が表示されます。

Created Date

バックアップファイルが作成された日時が表示されます。

Completed Date

バックアップファイルの作成が完了した日時が表示されます。

Downloaded Date

バックアップファイルがダウンロードされた日時が表示されます。

Destroyed Date

バックアップファイルが破棄された日付が表示されます。

Destruction Status

破棄に関するバックアップの状態が表示されます。

Destruction Comment

バックアップファイルの破棄に関するユーザーが指定した情報が表示されます。

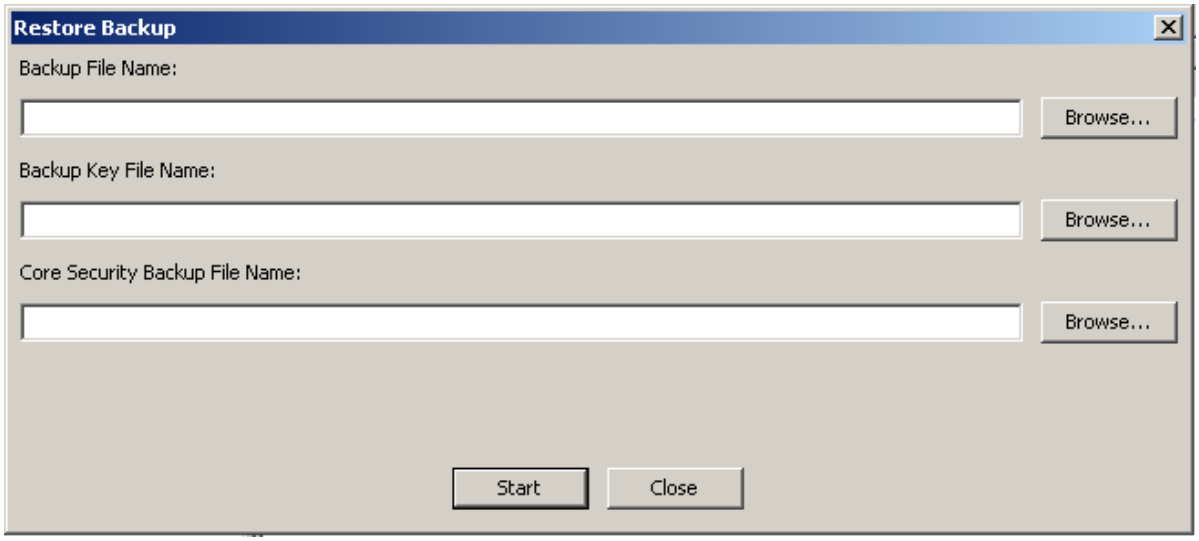
3. このダイアログボックスを閉じるには、「Close」ボタンを選択します。

バックアップの復元

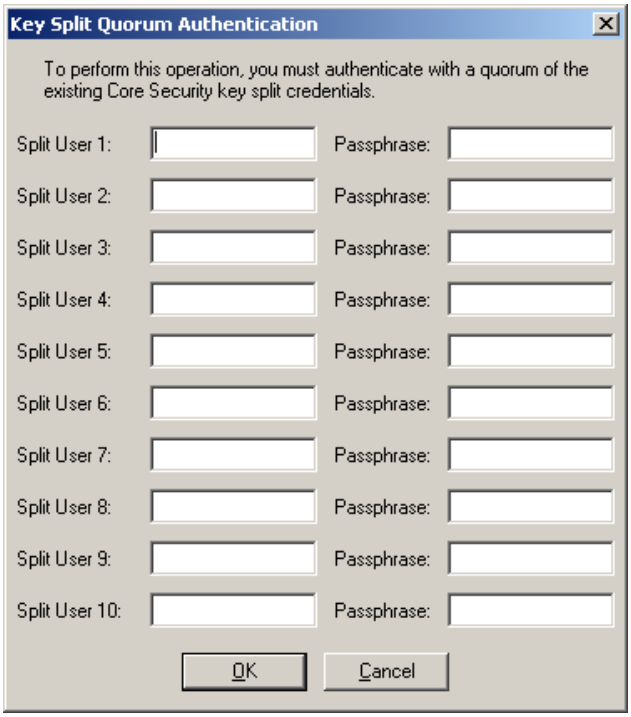
この機能を使用すると、ユーザーはバックアップファイルとバックアップ鍵ファイルで構成されるバックアップをアップロードして KMA に復元できます。バックアップファイルを KMA に復元する前に、認証に必要な定足数を満たしているかどうかを確認してください。

バックアップを復元するには、次の手順を実行します。

1. 「Backup List」画面で、復元するバックアップを強調表示して「Restore」ボタンを選択します。「Restore Backup」ダイアログボックスが表示されます。
2. 必要なコアセキュリティーバックアップ、バックアップ鍵ファイル、およびバックアップファイルを選択します。バックアップ鍵ファイルとバックアップは、一致している必要があります。つまり、同時に作成されている必要があります。コアセキュリティーバックアップは、バックアップ鍵ファイルとバックアップファイルより古い場合または新しい場合があります。コアセキュリティーバックアップファイルは、任意のバックアップ鍵ファイルおよびバックアップファイルとともに使用できます。
3. 「Start」ボタンを選択します。



4. アップロード処理が完了すると、「Restore Backup」ダイアログボックスに完了したことが示され、「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



5. 最後のユーザー名とパスフレーズを入力したあと「OK」ボタンを選択すると、ユーザー名とパスフレーズが KMA に送信され、認証が行われます。認証が成功すると、「Key Split Quorum Authentication」ダイアログボックスが閉じます。

   ユーザー ID とパスフレーズ、および必要とされる数 (定足数) が、コアセキュリティーバックアップの作成時に有効であった鍵分割資格と一致する必要があります。

6. 「Restore Backup」ダイアログボックスが表示され、復元処理の状態が示されます。

7. 次に、フィールドとその説明を示します。

Backup File Name

バックアップファイルの名前です。

Backup Wrapping Key File Name

バックアップ鍵ファイルの名前が表示されます。

Core Security Backup File Name

コアセキュリティー鍵データを含むバックアップファイルの名前です。

8. 復元が完了すると、完了を示すメッセージが表示されます。このダイアログボックスを閉じるには、「Close」ボタンを選択します。データベースとセキュリティー保護された鍵ストアが、KMA に復元されます。

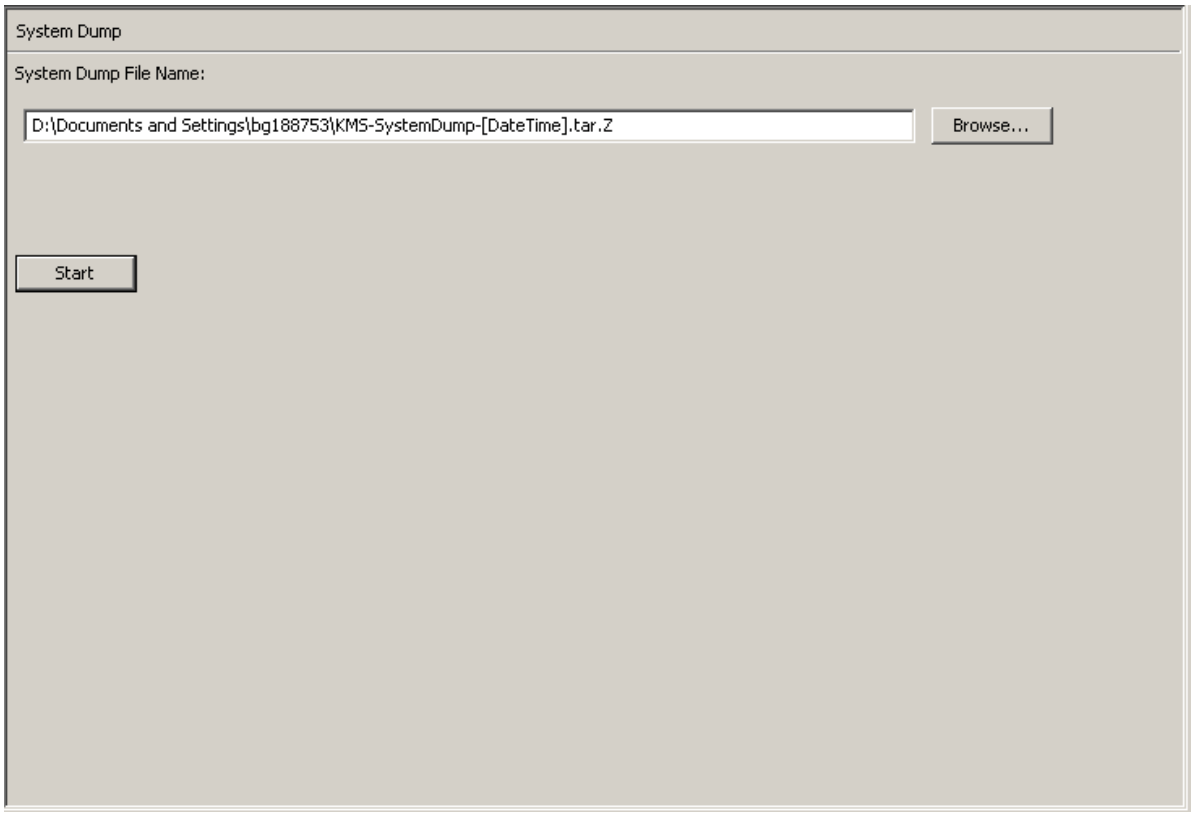
「System Dump」メニュー

「System Dump」メニューでは、問題解決のためのシステムダンプを作成し、KMS Manager が動作しているシステム上の圧縮ファイルにダウンロードします。ダウンロードしたファイルは、圧縮ユーティリティーで開くことができる形式になっています。

注 – ダンプには、鍵データまたは鍵を推測するために使用できる情報は含まれていません。

システムダンプの作成

1. システムダンプを作成するには、「System Management」メニューから、「System Dump」を選択します。画面が表示され、自動生成された *.tar.Z ファイルが表示されます。必要に応じて、「Browse」をクリックして出力先のパスを選択できます。
2. 「Start」ボタンをクリックして、ダウンロードを開始します。ダウンロードされたシステムダンプ情報のサイズをリアルタイムで示すメッセージが表示され、処理の完了が通知されます。
3. 出力先のパスに移動し、*.tar.Z ファイルを開いてシステムダンプ情報を表示します。



次に、フィールドとその説明を示します。

File Name:

自動生成された *.tar.gz ファイルが表示されます。

Browse:

このボタンをクリックすると、このファイルの場所を指定できます。

Start:

このボタンをクリックすると、ダウンロード処理が開始されます。

「Security Parameters」メニュー

「Security Parameters List」メニューを使用すると、セキュリティー責任者は、KMA のセキュリティーパラメータを表示および変更できます。

セキュリティーパラメータの取り出し

セキュリティーパラメータを取り出すには、次の手順を実行します。

「Security Parameters」メニューから、「Security Parameter List」を選択します。「Security Parameters List」画面が読み取り専用モードで表示されます。

次に、フィールドとその説明を示します。

Short Term Retention Audit Log Size Limit

エラーイベントの監査ログエントリの保持数が表示されます。この数を超えるとエントリは切り捨てられます。デフォルトは、10,000 です。最小値は 1000、最大値は 1,000,000 です。

Short Term Retention Audit Log Lifetime

短期監査ログエントリの保持期間 (日数) が表示されます。この期間を過ぎるとエントリは切り捨てられます。デフォルトは、7 日です。最小値は 7 日、最大値は 24,855 日です。

Medium Term Retention Audit Log Size Limit

エラーイベントの監査ログエントリの保持数が表示されます。この数を超えるとエントリは切り捨てられます。デフォルトは、100,000 です。最小値は 1000、最大値は 1,000,000 です。

Medium Term Retention Audit Log Lifetime

短期監査ログエントリの保持期間 (日数) が表示されます。この期間を過ぎるとエントリは切り捨てられます。デフォルトは、90 日です。最小値は 7 日、最大値は 24,855 日です。

Long Term Retention Audit Log Size Limit

長期保持監査ログエントリの保持数が表示されます。この数を超えるとエントリは切り捨てられます。デフォルトは、1,000,000 です。最小値は 1000、最大値は 1,000,000 です。

Long Term Retention Audit Log Lifetime

長期監査ログエントリの保持期間 (日数) が表示されます。この期間を過ぎるとエントリは切り捨てられます。デフォルトは、730 日です。最小値は 7 日、最大値は 24,855 日です。

Login Attempt Limit

失敗が許容されるログイン試行の回数が示されます。この回数を過ぎると実体は使用不可になります。デフォルトは、5 です。最小値は 1、最大値は 1000 です。

Passphrase Minimum Length

パスフレーズの最小文字数が表示されます。デフォルトは、8 文字です。最小文字数は 8 文字、最大文字数は 64 文字です。

Management Session Inactivity Timeout

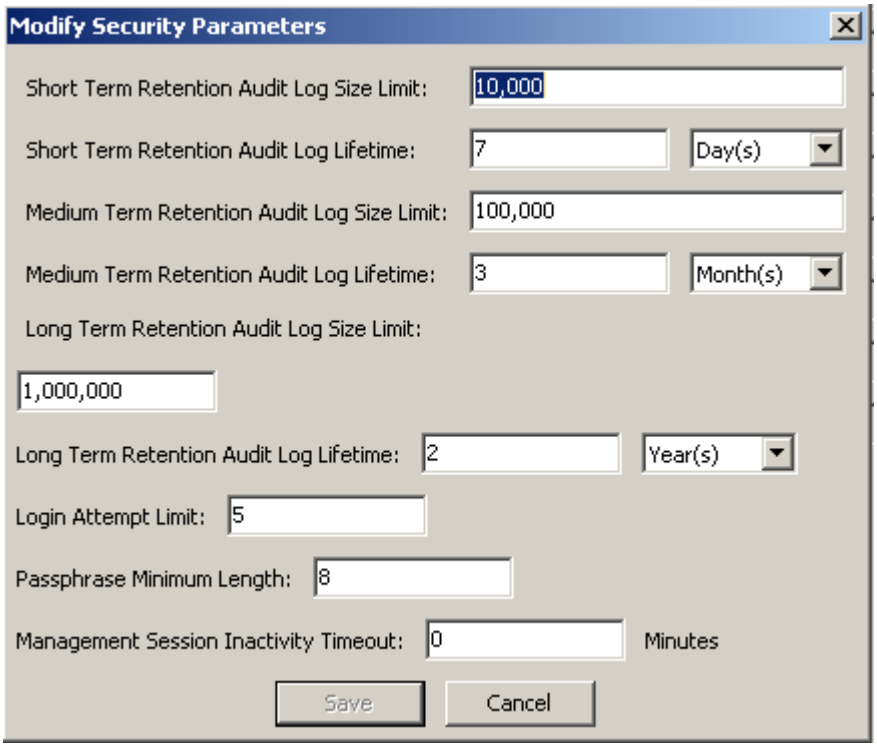
KMS Manager またはコンソールのログインセッションをアイドルにしておくことができる最長時間 (分単位) が表示されます。この時間を過ぎると、ログインセッションは自動的にログアウトされます。この値を変更しても、すでに進行中のセッションには影響を及ぼしません。デフォルトは、15 分です。最小値は 0 分 (アイドル時間なし)、最大値は 60 分です。

セキュリティーパラメータを変更する場合は、「Modify」ボタンを選択します。詳細は、148 ページの「セキュリティーパラメータの変更」を参照してください。

セキュリティーパラメータの変更

セキュリティーパラメータを変更するには、次の手順を実行します。

1. 「Security Parameters」画面で、「Modify」ボタンを選択します。「Modify Security Parameters」画面が表示されます。



2. 必要に応じて、セキュリティーパラメータを変更します。終了したら、「Save」ボタンを選択します。変更内容が KMA データベースに保存されます。

コアセキュリティー

コアセキュリティーコンポーネントの主な要素は、ルート鍵データです。ルート鍵データとは、クラスタの初期化時に生成される鍵データです。ルート鍵データによって、マスター鍵が保護されます。マスター鍵とは、KMA に格納されるデータユニット鍵を保護する対称鍵です。

コアセキュリティーは、鍵分割スキーマによって保護されます。このスキーマでは、ルート鍵データのラップを解除するために、鍵分割資格で定義された定足数のユーザーのユーザー名とパスフレーズを提供する必要があります。

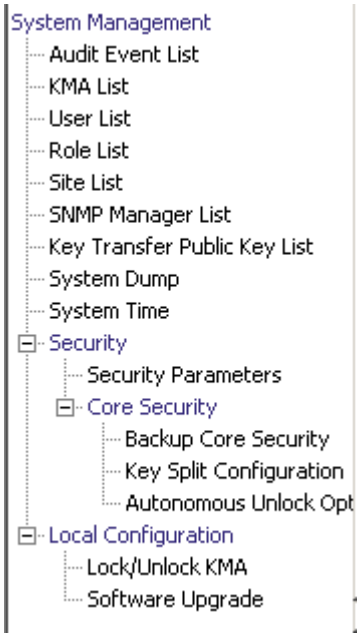
このセキュリティーメカニズムでは、KMA に対してロックとロック解除の 2 つの操作状態が有効になります。

ロック状態の KMA では、ルート鍵データのラップを解除できないため、データユニット鍵にアクセスできません。このため、KMA では、新しいデータユニットを登録するか、または既存のデータユニットのデータユニット鍵を取り出すエージェントの要求を処理できません。

ロック解除状態の KMA では、ルート鍵データを使用してデータユニット鍵にアクセスし、エージェントのデータユニット鍵の要求を処理できます。

「Core Security」メニュー

「Core Security」メニューには、次のメニューオプションがあります。



このメニューを使用すると、セキュリティー責任者は、次の操作を行うことができます。

- コアセキュリティーバックアップの作成
- 鍵分割資格の表示および変更
- 自律ロック解除オプションの使用可能および使用不可への切り替え

Backup Core Security

「Backup Core Security」オプションを使用すると、セキュリティー責任者は、コアセキュリティー鍵データをバックアップしてローカルシステムのファイルにダウンロードできます。

注意 – コアセキュリティーバックアップファイルは、注意して保護してください。コアセキュリティーバックアップファイルは、任意のバックアップファイルとバックアップ鍵ファイルのペアとともに使用できるため、以前のコアセキュリティーバックアップファイルでも使用できます。

コアセキュリティーバックアップの作成

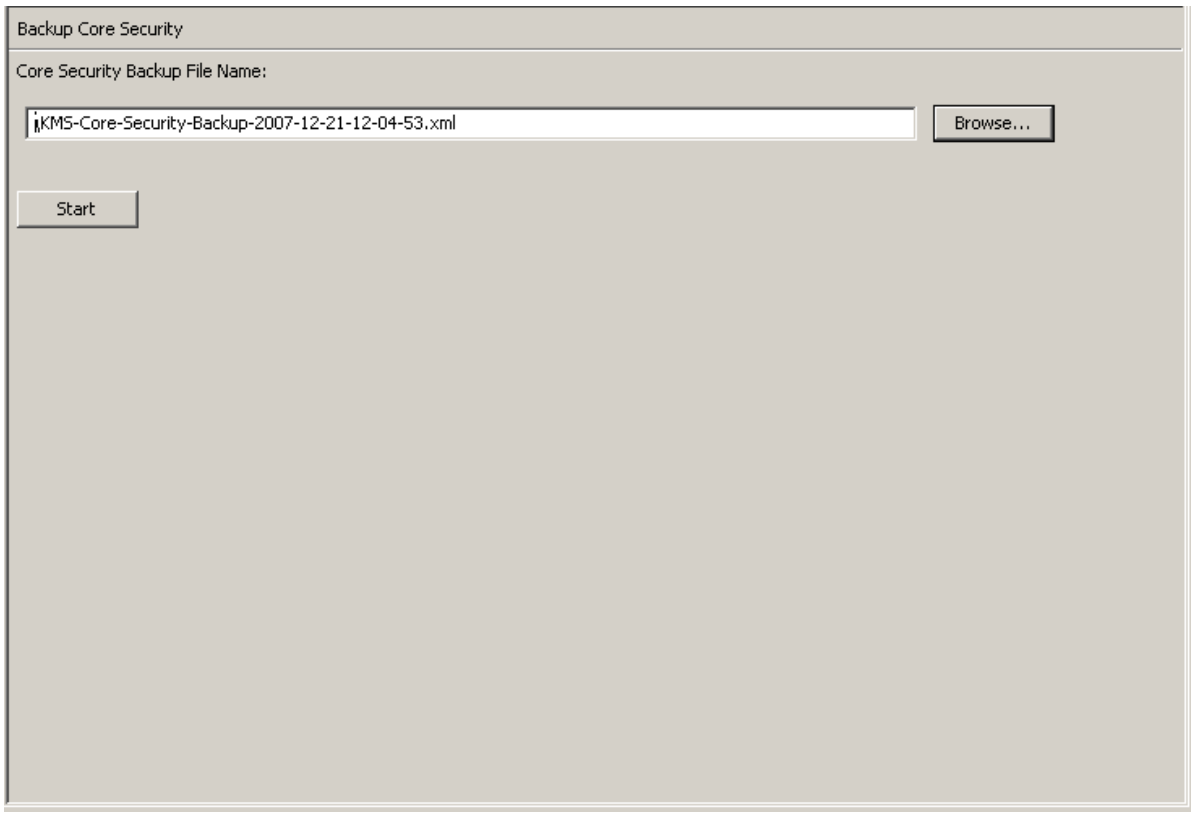
鍵分割資格の変更後は、新しいコアセキュリティーバックアップの実行が必要になります。

重要 – セキュリティー責任者がコアセキュリティー鍵データをバックアップしたあとでないと、バックアップ担当者はバックアップを作成できません。251 ページの「バックアップの作成」を参照してください。

---

1. 「Core Security」メニューから、「Backup Core Security」を選択します。「Backup Core Security」画面が表示されます。

注 – コアセキュリティーバックアップファイルの名前は、自動的に生成されます。ただし、名前を編集するか、「Browse」ボタンを選択して出力先のパスを選択することもできます。



2. 「Start」ボタンを選択してコアセキュリティーバックアップファイルを作成し、ユーザー指定の出力先にダウンロードします。
3. バックアップが完了すると、メッセージが表示されます。このダイアログボックスを閉じるには、「Close」ボタンを選択します。
4. 「Backup Core Security」画面に戻ります。

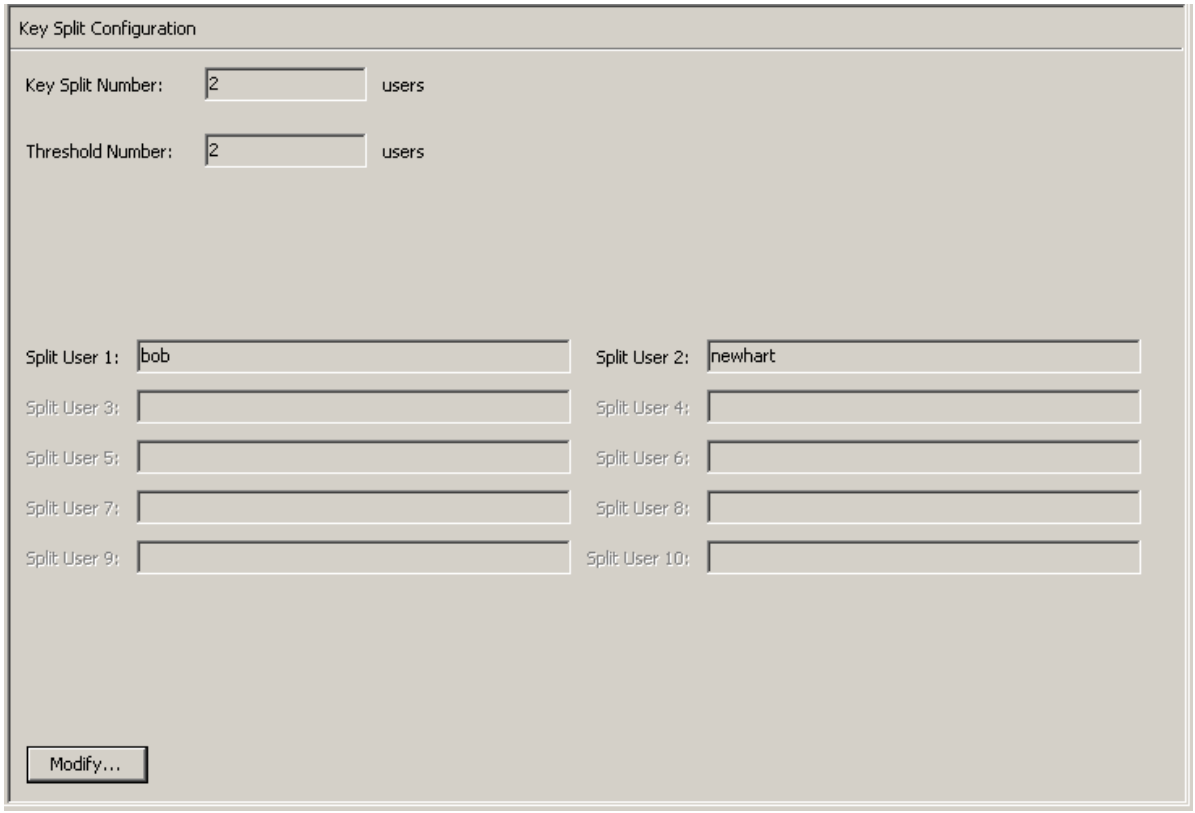
Key Split Configuration

「Key Split Configuration」メニューオプションを使用すると、セキュリティー責任者は、KMA の鍵分割資格を表示および変更できます。

鍵分割設定の表示

鍵分割設定を表示するには、次の手順を実行します。

1. 「Core Security」メニューから、「Key Split Configuration」を選択します。「Key Split Configuration」画面が表示されます。



次に、フィールドとその説明を示します。

Key Split Number

鍵の分割数が表示されます。最大数は 10 です。

Threshold Number

定足数の認証に必要なユーザー数が表示されます。

Split User (1 ～ 10)

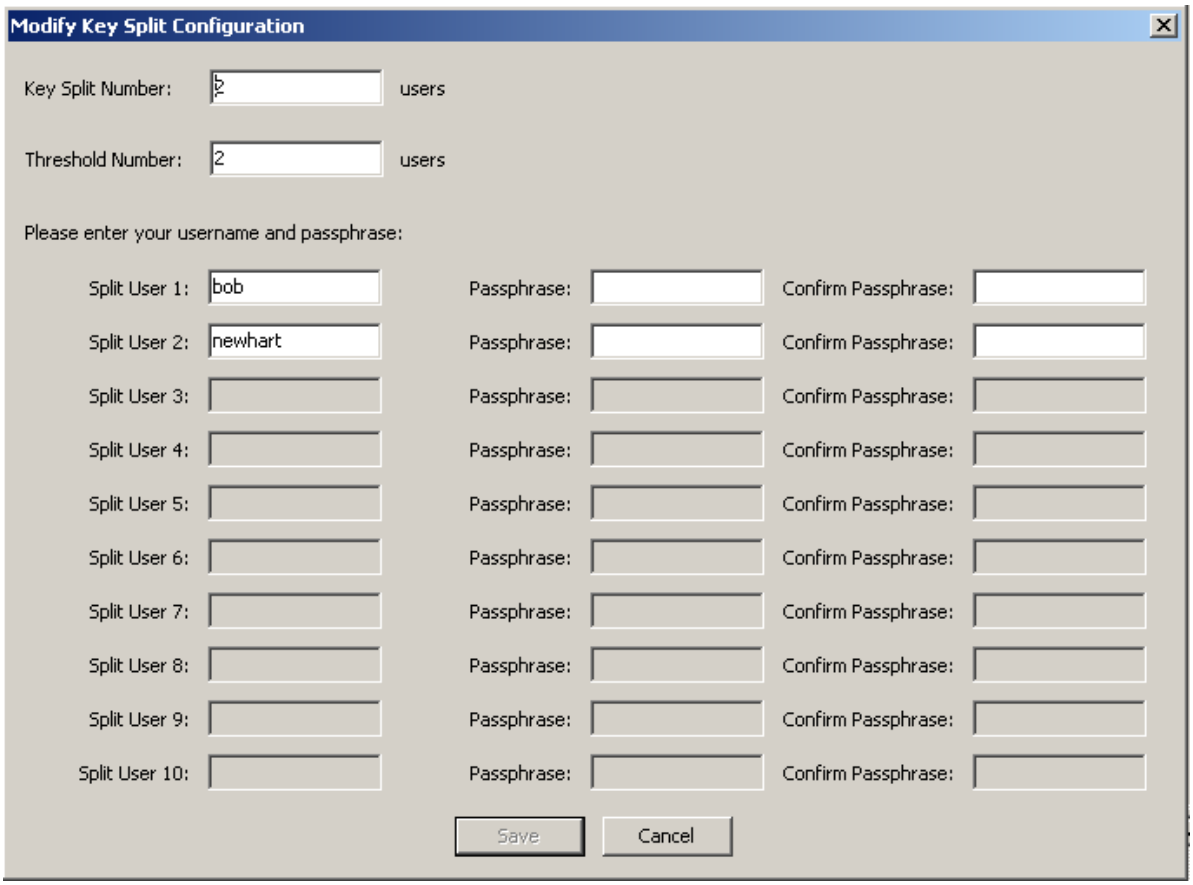
既存の分割のユーザー名が表示されます。

鍵分割のユーザー名、パスフレーズ、およびしきい値の数を変更する場合は、「Modify」ボタンを選択します。詳細は、155 ページの「鍵分割設定の変更」を参照してください。

鍵分割設定の変更

鍵分割設定を変更するには、次の手順を実行します。

1. 「Key Split Configuration」画面で、「Modify」ボタンを選択します。「Modify Key Split Configuration」ダイアログボックスが表示されます。



2. 次のパラメータを設定し、「OK」ボタンを選択します。

Key Split Number

鍵分割数の新しい値を入力します。最大数は 10 です。

Threshold Number

定足数を満たすために必要なユーザー数の新しい値を入力します。

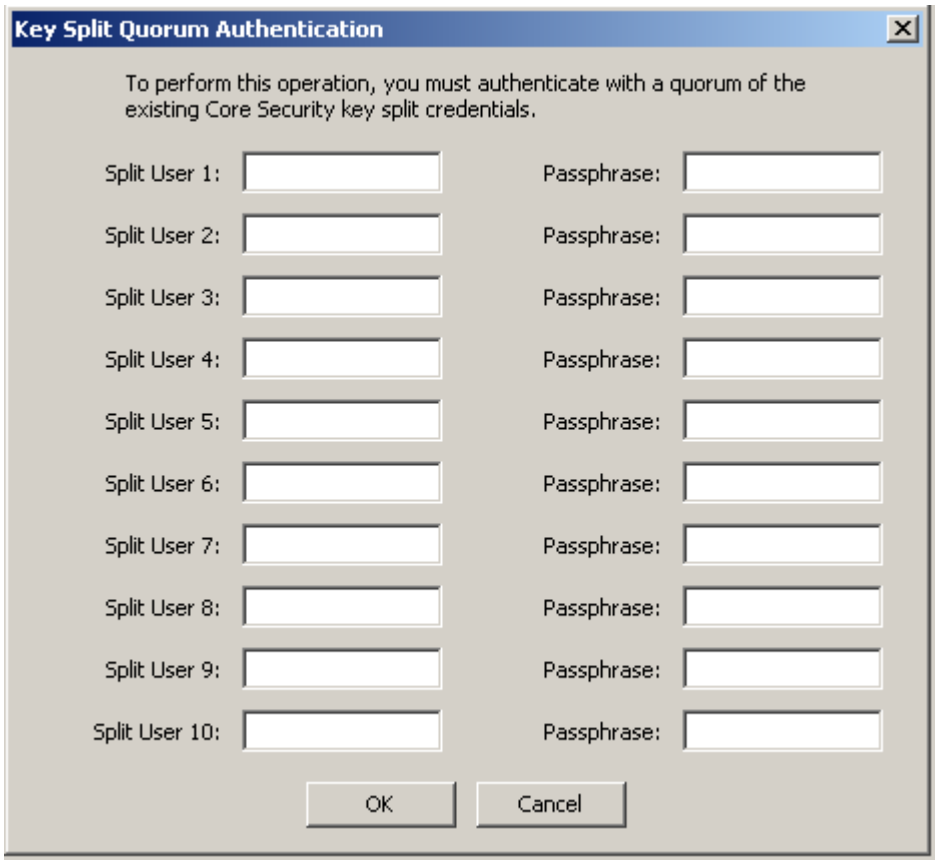
Split User x

ユーザー名を入力します。分割ユーザーごとに、関連する「Passphrase」フィールドと「Confirm Passphrase」に値を入力します。

注 – 入力できる分割ユーザーのフィールド数は、「Key Split Number」フィールドに入力した値によって決定されます。

---

3. 最後のユーザー名とパスフレーズを入力したあと、「Save」ボタンを選択します。
4. 新しい鍵分割資格が入力されると、「Key Split Quorum Authentication」ダイアログボックスが表示されます。既存の定足数資格のユーザー名とパスフレーズを入力し、「OK」ボタンを選択します。手順 2 および手順 3 の「新しい」資格を設定するには、この操作が必要です。



5. データベースの以前の設定情報が新しい設定に更新されます。新しい設定が「Key Split Credentials」画面に表示されます。

注 – 更新された鍵分割資格を使用して、コアセキュリティー鍵データがラップし直されます。

---

6. 新しいコアセキュリティーバックアップを作成します (151 ページの「コアセキュリティーバックアップの作成」を参照)。

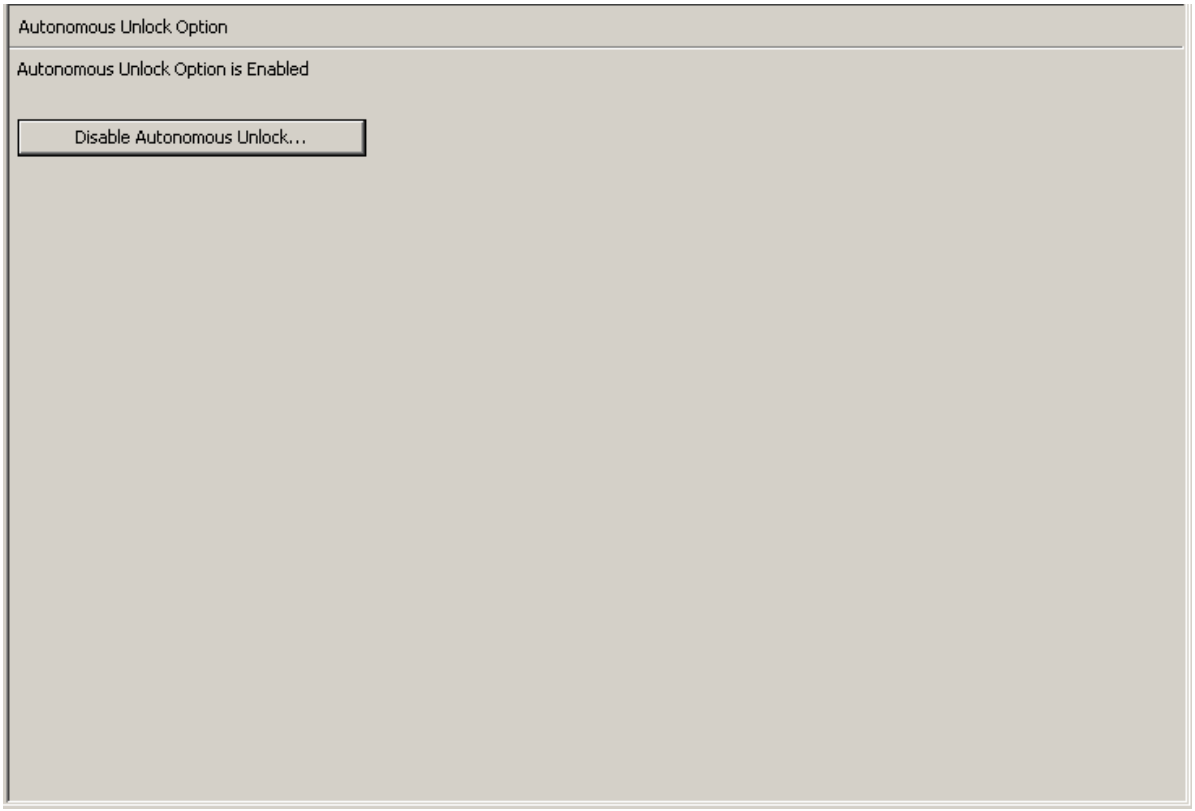
注 – 以前のコアセキュリティーバックアップファイルをすべて破棄して、以前の鍵分割資格がバックアップの破棄に使用できないようにする必要があります。

Autonomous Unlock Option

「Autonomous Unlock Option」メニューオプションを使用すると、セキュリティー責任者は、KMA の自律オプションを使用可能または使用不可に切り替えることができます。

自律ロック解除オプションを使用可能または使用不可に切り替えるには、次の手順を実行します。

1. 「Core Security」管理メニューから、「Autonomous Unlock Option」を選択します。「Autonomous Unlock Option」画面が表示され、現在の自律オプションの状態が示されます。



2. 現在の自律起動状態に従って、「Enable Autonomous Unlock」を選択してこのオプションを使用可能にするか、または「Disable Autonomous Unlock」を選択してオプションを使用不可にします。

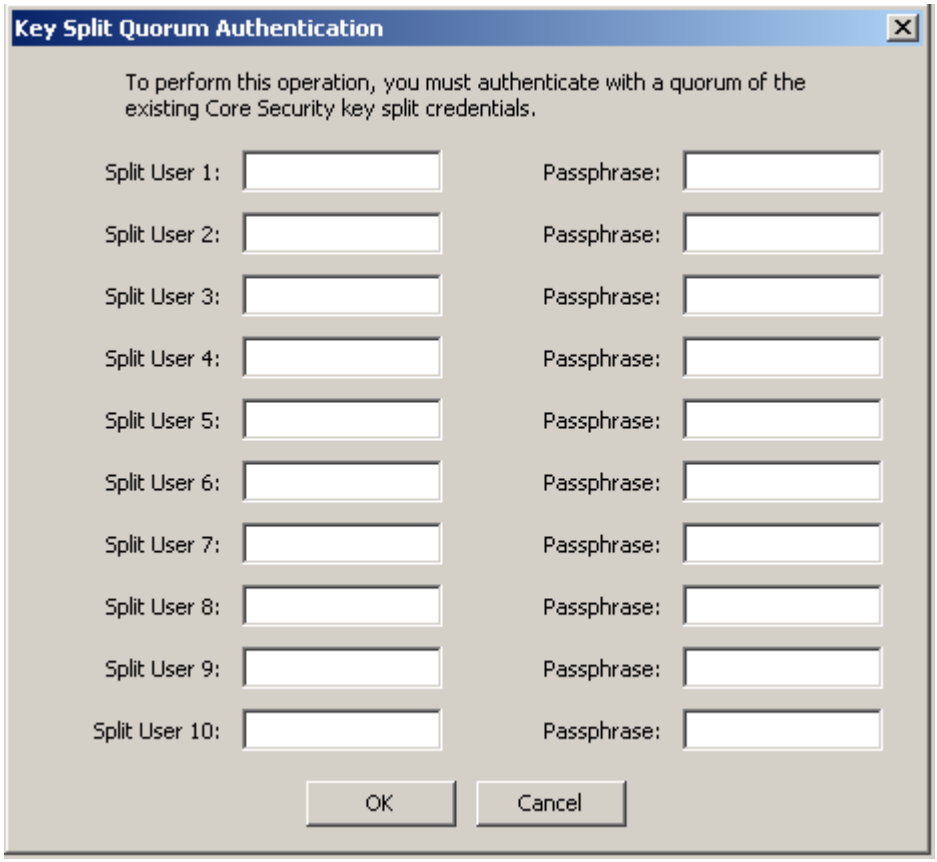
注 –

• 「Lock/Unlock」ボタンを使用すると、状態が切り替わり、KMA のロック状態が現在と反対の状態に設定されます。

• 自律ロック解除オプションを使用可能または使用不可にするには、定足数を満たす必要があります。

---

3. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



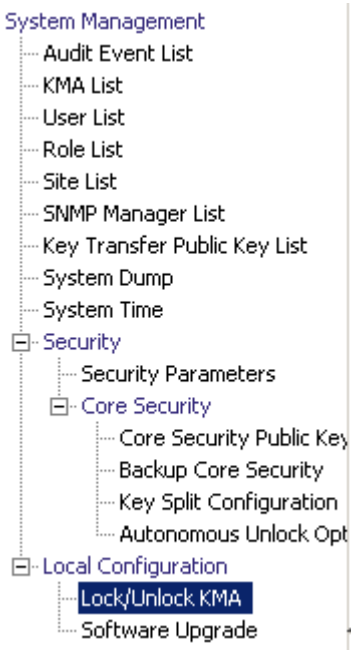
4. 最後のユーザー名とパスフレーズを入力したあと「OK」ボタンを選択すると、ユーザー名とパスフレーズが KMA に送信され、認証が行われます。

5. 認証が成功すると、「Key Split Quorum Authentication」ダイアログボックスが閉じ、KMA に新しい自律起動オプションが設定されます。

「Local Configuration」メニュー

「Local Configuration」メニューには、次のオプションがあります。

- KMA のロックとロック解除
- ソフトウェアのアップグレード



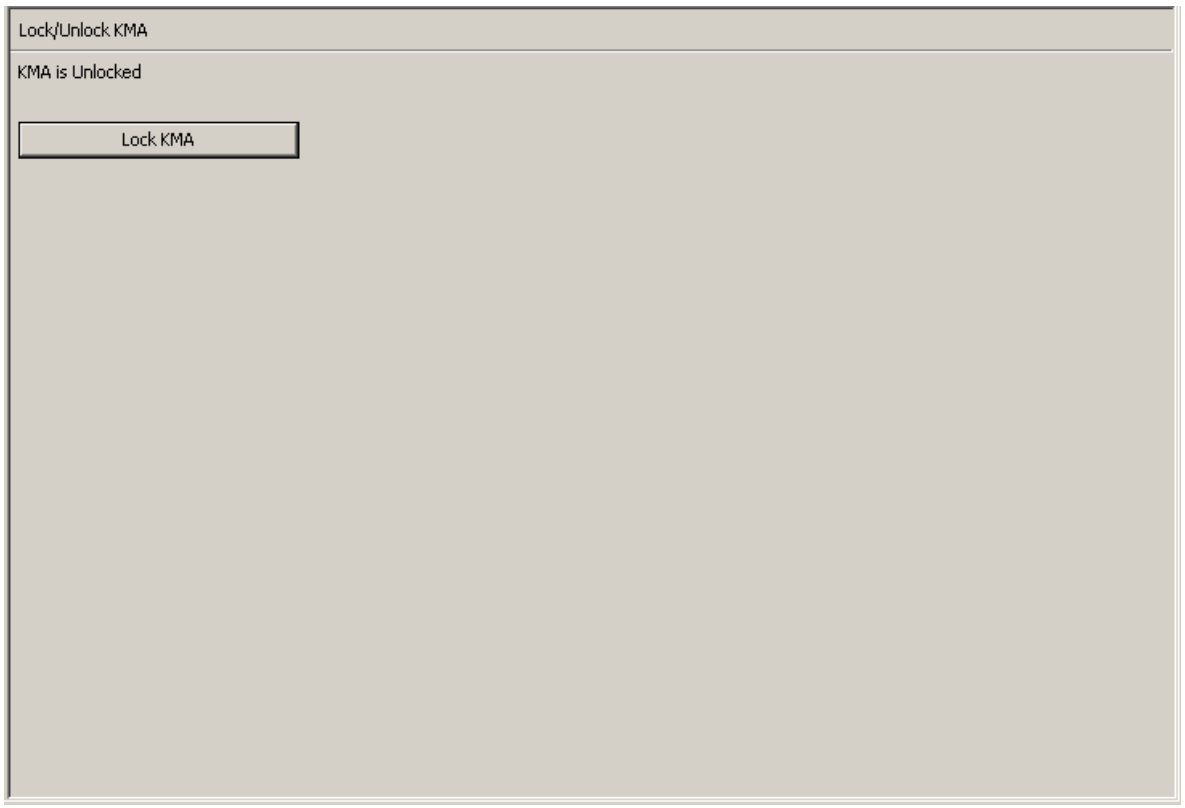
Lock/Unlock KMA

「Lock/Unlock KMA」メニューオプションを使用すると、セキュリティー責任者は、KMA のコアセキュリティーをロックまたはロック解除できます。コアセキュリティーと、コアセキュリティーがロックまたはロック解除されたときの KMA の動作の詳細は、149 ページの「コアセキュリティー」を参照してください。

KMA のロック

KMA をロックするには、次の手順を実行します。

1. 「Local Configuration」メニューから、「Lock/Unlock KMA」を選択します。
   「Lock/Unlock KMA」画面が表示され、KMA の状態が示されます。この例では、状態は「Unlocked」になっています。



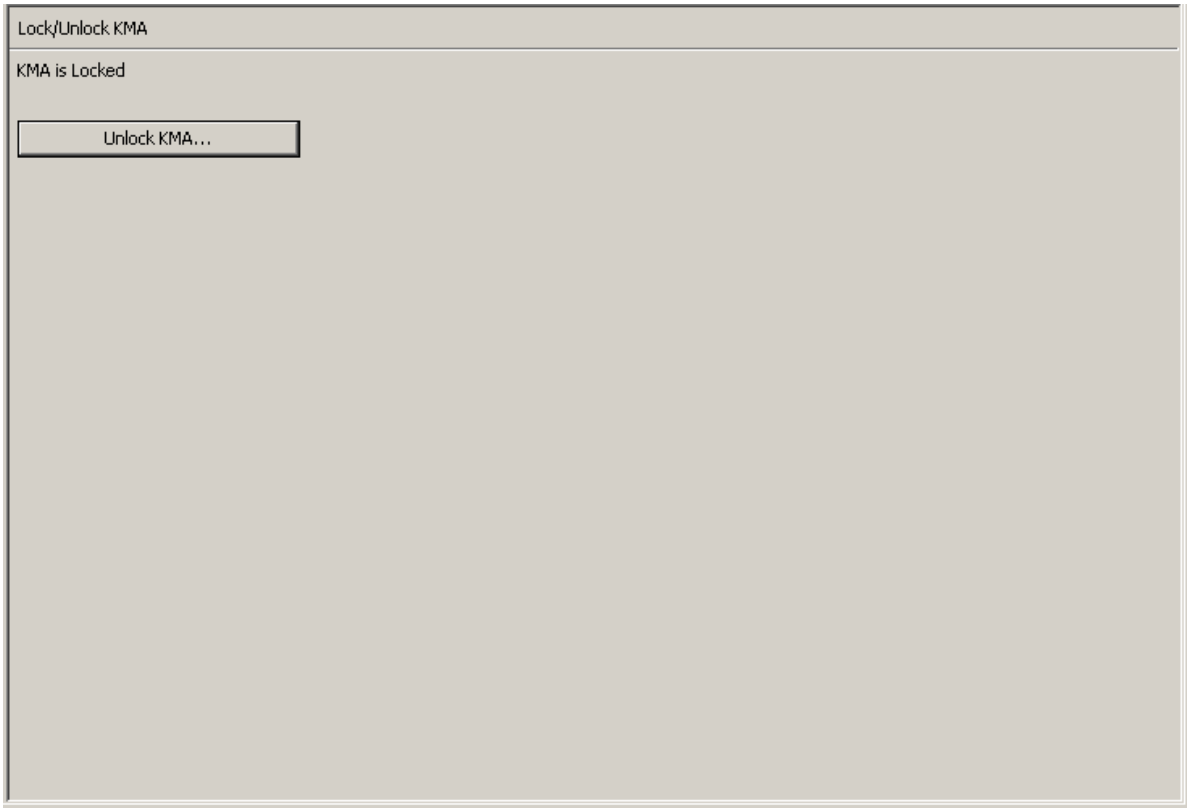
2. 「Lock KMA」ボタンを選択して、KMA をロックします。ボタンを 1 回押すと、このボタンは「Unlock KMA」に変わり、新しいロック状態と実行できる操作が示されます。これで、KMA はロックされました。

注 – 「Lock KMA」ボタンと「Unlock KMA」ボタンを使用すると状態が切り替わり、KMA のロック状態が現在と反対の状態に設定されます。ボタンを 1 回押すと、テキストラベルとボタンラベルが変わり、新しいロック状態と実行できる操作が示されます。

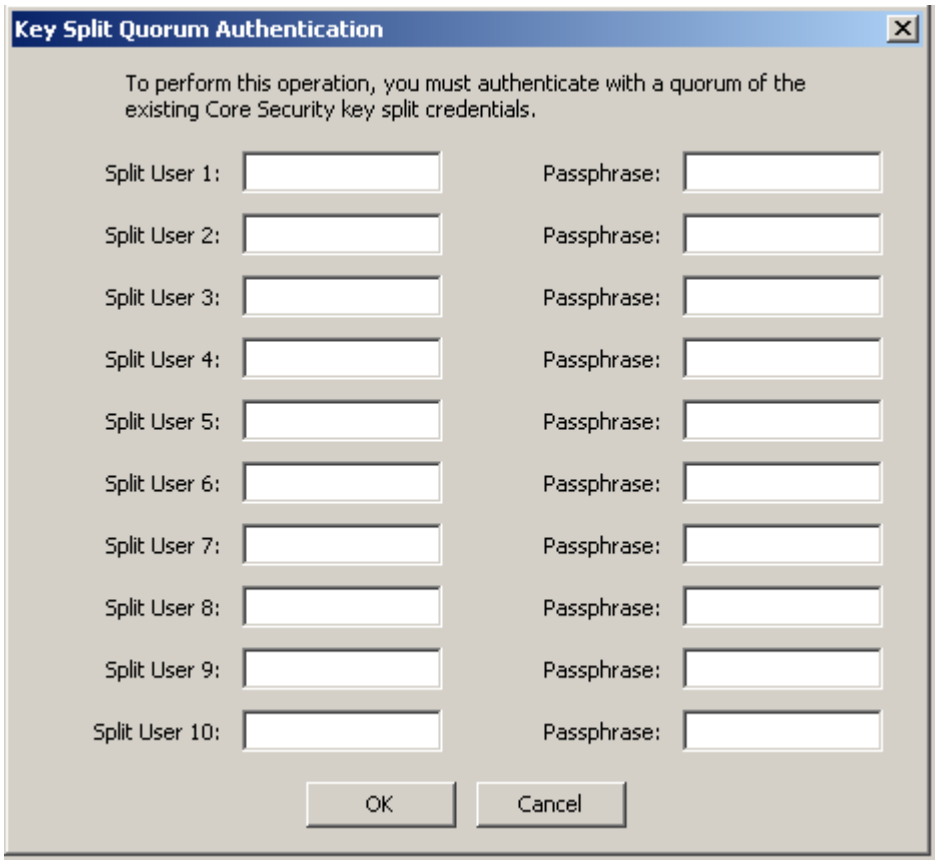
KMA のロック解除

KMA のロックを解除するには、次の手順を実行します。

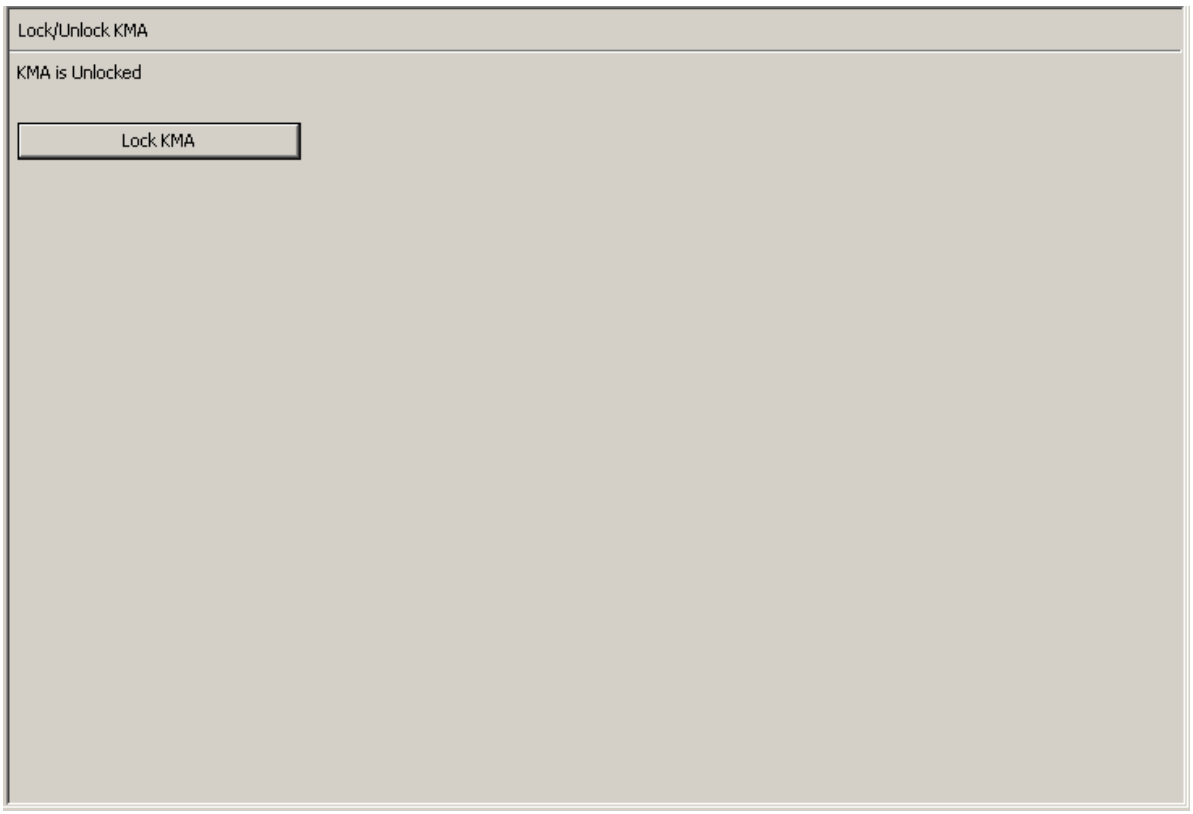
1. 「Lock/Unlock KMA」画面で、「Unlock KMA」ボタンを選択します。



2. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



3. 最後のユーザー名とパスフレーズを入力したあと、「OK」ボタンを選択します。ユーザー名とパスフレーズが、認証のため KMA に送信されます。
4. 認証が成功すると、「Key Split Quorum Authentication」ダイアログボックスが閉じ、KMA のロックが解除されます。


Lock/Unlock KMA
KMA is Unlocked
Lock KMA

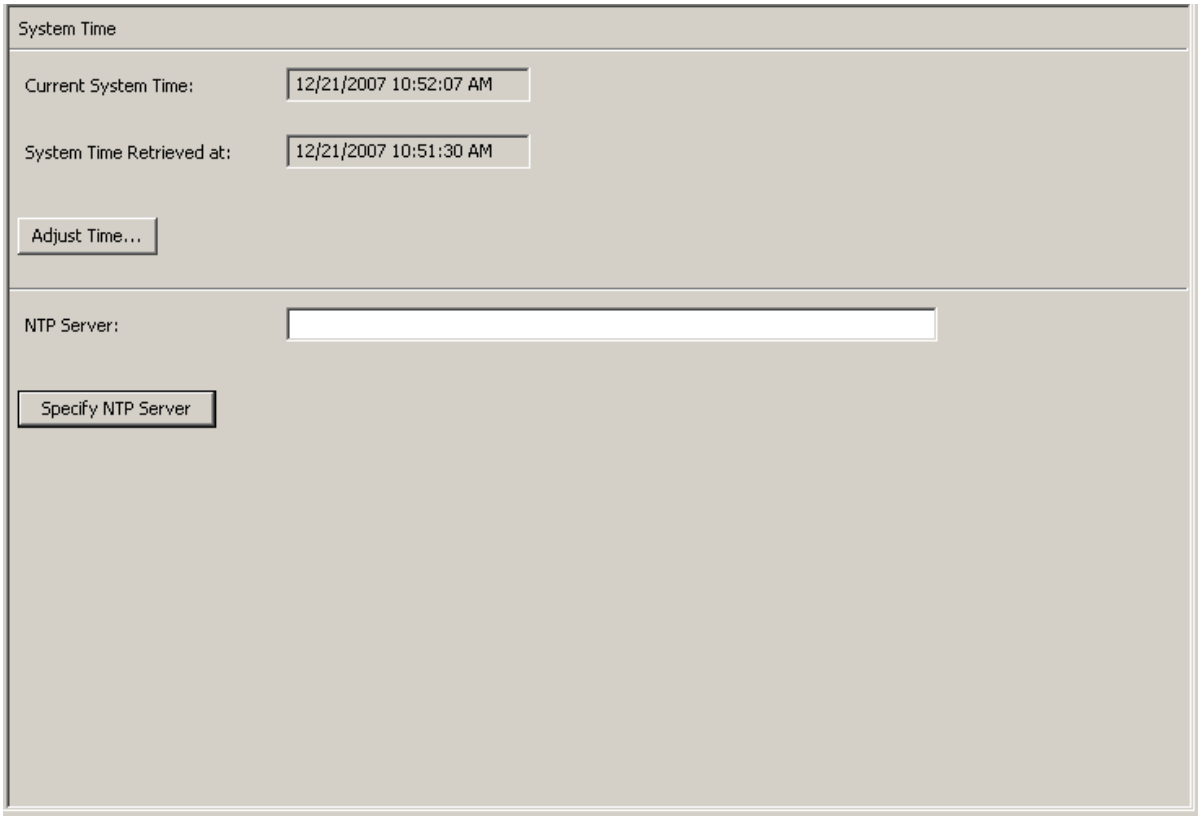
「System Time」メニュー

「System Time」メニューオプションを使用すると、ユーザーは、ユーザーが接続するシステムのクロックを設定できます。KMS ソリューションの操作を適切に実現するには、クラスタ内の各 KMA が報告する時刻を、互いに 5 分以内に更新することが非常に重要です。

ローカルクロック情報の取得

ローカルクロック情報を取得するには、次の手順を実行します。

「System Management」メニューから、「System Time」を選択します。「System Time」画面が表示されます。



次に、フィールドとその説明を示します。

Current System Time

現在のシステム時刻が表示されます。

System Time Retrieved At

KMA のシステム時刻を取得したときのローカルクライアント時刻が表示されます。

Adjust Time

このボタンをクリックすると、システム時刻を変更できます。

KMA のクロックを変更する場合は、「Adjust Time」ボタンを選択します。詳細は、166 ページの「KMA のローカルクロックの調整」を参照してください。

NTP Server

この KMA が使用する NTP サーバーが表示されます (使用している場合)。

Specify NTP Server

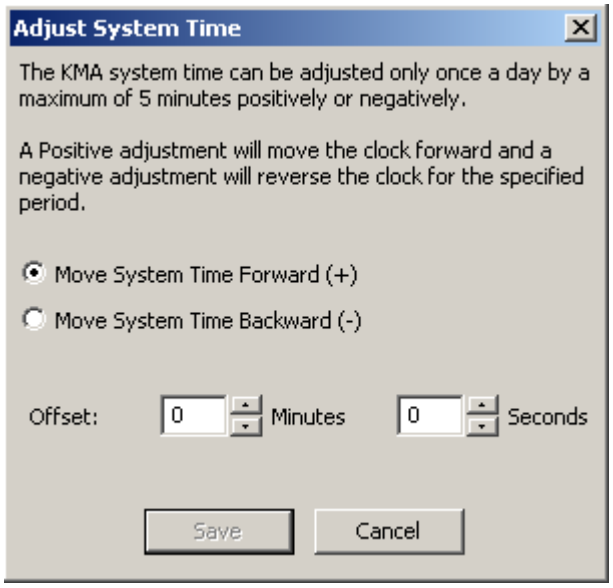
このボタンをクリックすると、この KMA で使用する NTP サーバーを指定できます。

KMA のローカルクロックの調整

KMA のクロックの調整では、1 日に一度だけ最大 5 分の範囲でクロックを進めるか、戻すことができます。正 (+) の調整では、クロックがゆっくりと先に進み、負 (-) の調整では、クロックがゆっくりと前に戻ります。

KMA のローカル時刻を調整するには、次の手順に従います。

1. 「System Time」画面で、「Adjust Time」ボタンを選択します。「Adjust System Time」ダイアログボックスが表示されます。



2. クロックに正の調整を行う場合は、「Move System Time Forward (+)」ラジオボタンを選択します。クロックに負の調整を行う場合は、「Move System Time Backward (-)」ラジオボタンを選択します。
3. 「Offset Minutes」テキストボックスで、数値を選択します。
4. 「Offset Seconds」テキストボックスで、数値を選択します。

注 – 指定した調整幅が大き過ぎるとエラーメッセージが表示され、より小さな値を入力するように求められます。「OK」ボタンを選択してこのダイアログボックスを閉じ、新しい値を入力します。

---

5. 「Save」ボタンを選択して、変更を適用します。システムクロックが調整されます。

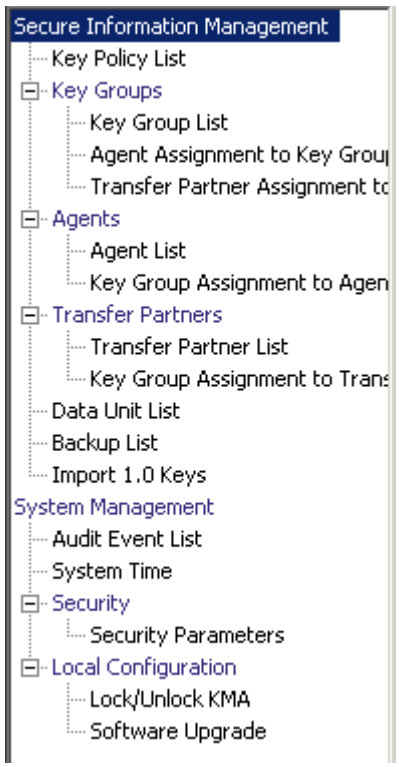
第6章

コンプライアンス責任者の操作

この章では、コンプライアンス責任者ロールが付与されたユーザーが実行できる操作について説明します。複数のロールが割り当てられている場合は、そのロールを実行する手順について、該当する章を参照してください。

コンプライアンス責任者ロール

コンプライアンス責任者は、組織内のデータの流れを管理し、データコンテキスト (鍵グループ) と、データの保護方法および最終的な破棄方法を決定する規則 (鍵ポリシー) を定義および配備できます。これらの機能に対応するメニューは次のとおりです。



鍵ポリシー

鍵ポリシーは、データ管理に関する指針を提供します。KMS Manager では、鍵ポリシーを使用して、データの保護方法および破棄方法を決定します。鍵を作成してエージェントに配信するには、あらかじめ鍵ポリシーを作成しておく必要があります。

鍵ポリシーを作成および変更できるのは、コンプライアンス責任者のみです。これによって、データが常にポリシーに準拠していることを確実にします。

「Key Policy List」メニュー

「Key Policies List」メニューでは、組織の鍵ポリシーを管理できます。

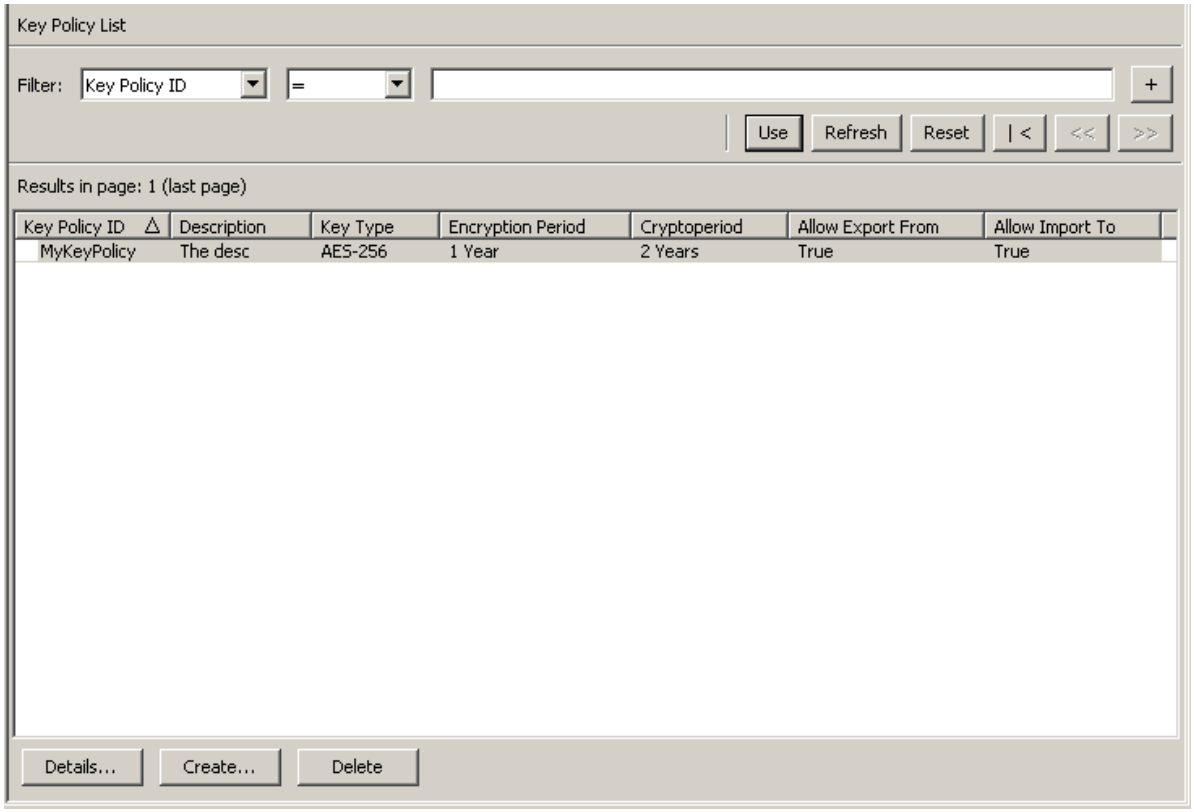
「Key Policy List」メニューオプションを使用すると、次の操作を行うことができます。

- 鍵ポリシーの表示
- 鍵ポリシーの詳細の表示および変更
- 鍵ポリシーの作成
- 既存の鍵ポリシーの削除

鍵ポリシーの表示

鍵ポリシーを表示するには、次の手順を実行します。

1. 「Secure Information Management」メニューから、「Key Policy List」を選択します。「Key Policy List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで鍵ポリシーリストにフィルタを適用することもできます。

- Key Policy ID
- Description
- Key Type
- Encryption Period
- Cryptoperiod
- Allow Export From
- Allow Import To

表示されている鍵ポリシーリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Key Policy ID
- Description
- Key Type
- Encryption Period
- Cryptoperiod
- Allow Export From
- Allow Import To

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス:

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス:

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

Use:

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Key Policy ID

各鍵ポリシーを識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。鍵ポリシー ID は、いったん作成すると変更できません。

Description

鍵ポリシーの説明が示されます。この値は、1 ～ 64 文字で指定できます。

Key Type

この鍵ポリシーに関連付けられている鍵で使用される暗号化アルゴリズムのタイプを示します。値は AES-256 になります。

注 – 「Encryption Period」および「Cryptoperiod」は、鍵がはじめてエージェントに割り当てられた時点から開始します。ポリシーの「Encryption period」および「Cryptoperiod」は変更できません。これは、鍵ポリシーの変更が多数の鍵に影響することを回避するためです。

Encryption Period

この鍵ポリシーに関連付けられている鍵を、データの暗号化または復号化に使用できる期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Cryptoperiod

この鍵ポリシーに関連付けられている鍵を、データの復号化に使用できる (しかし暗号化には使用できない) 期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Allow Export From

この鍵ポリシーに関連付けられているデータユニットをエクスポートできるかどうかが示されます。True または False の値を取ります。

Allow Import To

この鍵ポリシーに関連付けられているデータユニットをインポートできるかどうかが示されます。True または False の値を取ります。

鍵ポリシーを作成する場合は、「Create」ボタンを選択します。詳細は、173 ページの「鍵ポリシーの作成」を参照してください。

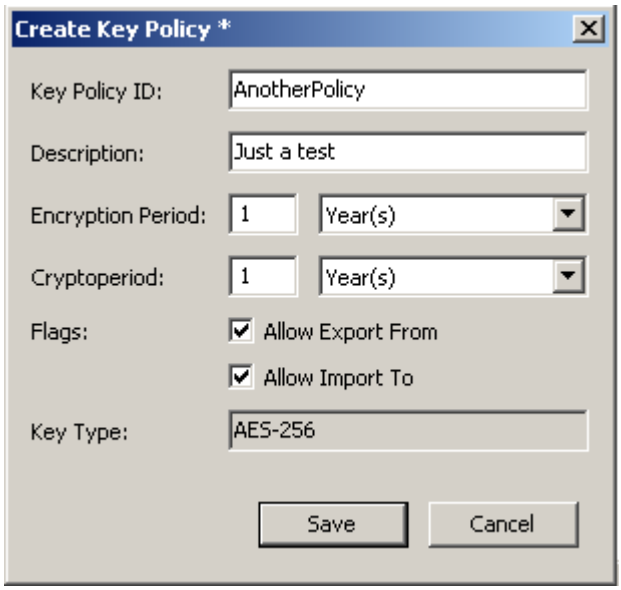
鍵ポリシーを表示または変更する場合は、その鍵ポリシーを強調表示して「Details」ボタンを選択します。詳細は、175 ページの「鍵ポリシーの表示および変更」を参照してください。

鍵ポリシーを削除する場合は、「Delete」ボタンを選択します。詳細は、176 ページの「鍵ポリシーの削除」を参照してください。

鍵ポリシーの作成

鍵ポリシーを作成するには、次の手順を実行します。

1. 「Key Policy List」画面で、「Create」ボタンを選択します。「Create Key Policy」画面が表示されます。



2. 次のパラメータを設定します。

Key Policy ID

ポリシーを識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

Description

ポリシーを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。このフィールドは、空白のままにすることができます。

Encryption Period

この鍵ポリシーに関連付けられている鍵を、データの暗号化または復号化に使用できる期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Cryptoperiod

この鍵ポリシーに関連付けられている鍵を、データの復号化に使用できる (しかし暗号化には使用できない) 期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Flags

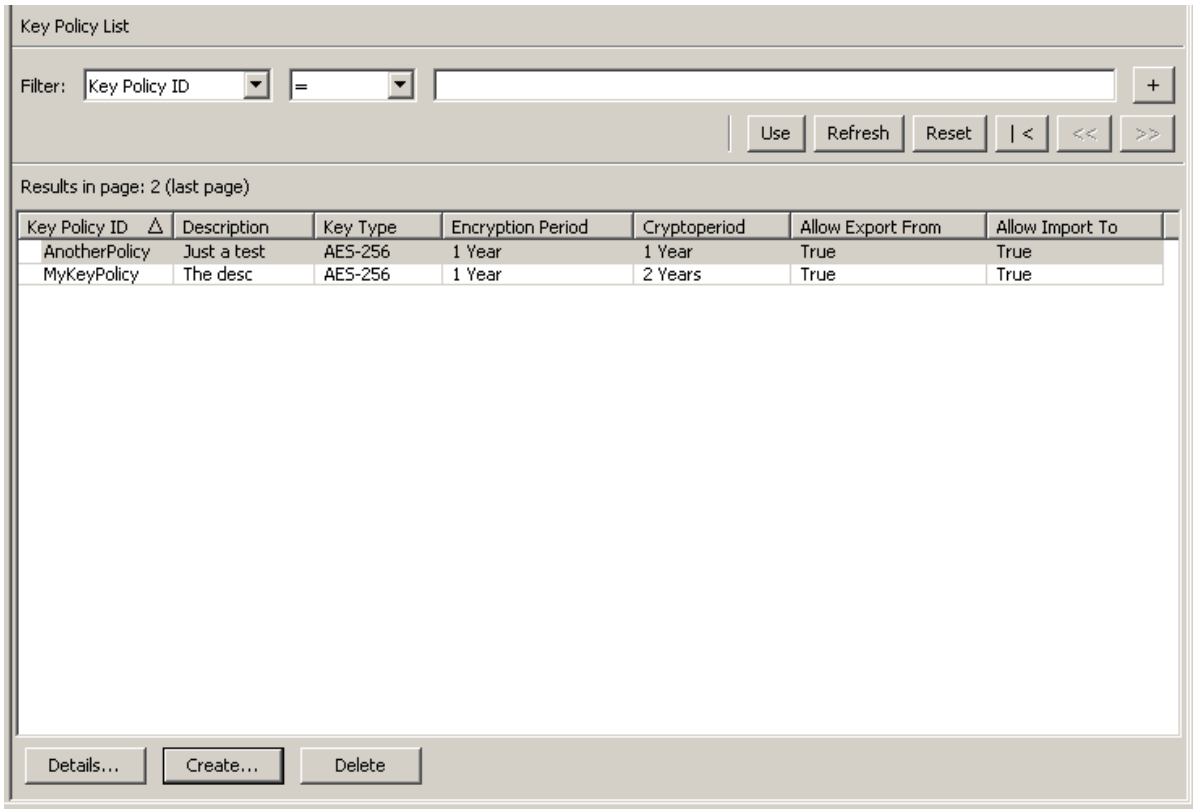
Allow Export From

この鍵ポリシーに関連付けられているデータユニットをエクスポートできるかどうかが示されます。True または False の値を取ります。

Allow Import To

この鍵ポリシーに関連付けられているデータユニットをエクスポートできるかどうかが示されます。True または False の値を取ります。

3. 「Save」ボタンを選択して、鍵ポリシーを保存します。「Key Policy List」画面に、新しい鍵ポリシーが表示されます。これで、この鍵ポリシーを鍵グループで使用できるようになります。

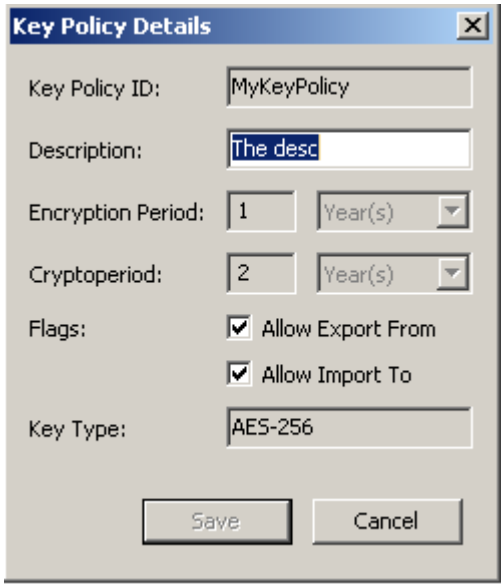


鍵ポリシーの表示および変更

注 – 鍵ポリシーの詳細情報を表示できるのは、コンプライアンス責任者のみです。

鍵ポリシーの詳細を変更するには、次の手順を実行します。

1. 「Key Policy List」画面で、詳細情報を表示する鍵ポリシーをダブルクリックするか、または鍵ポリシーを強調表示して「Details」ボタンを選択します。「Key Policy Details」画面が表示されます。



2. 必要に応じて、「`Description`」、「`Allow Export From`」、および「`Allow Import To`」フィールドを変更できます。終了したら、「Save」ボタンを選択して変更内容を保存します。システムによって新しい鍵ポリシーの評価と妥当性検査が行なわれたあと、新しい鍵ポリシーに鍵グループが関連付けられます。

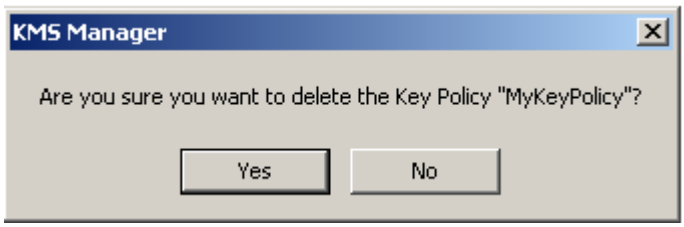
3. 「Cancel」ボタンを選択すると、変更内容を保存せずにダイアログボックスが閉じます。

鍵ポリシーの削除

鍵ポリシーは、鍵グループまたは鍵で使用されていない場合にのみ削除できます。

鍵ポリシーを削除するには、次の手順を実行します。

1. 「Key Policy List」画面で、削除する鍵ポリシーを強調表示して「Delete」ボタンを選択します。次のように、指定した鍵ポリシーの削除を確認するダイアログボックスが表示されます。



2. 「Yes」ボタンを選択して、鍵ポリシーを削除します。鍵ポリシーがデータベースから削除されます。「Key Policy List」画面に戻ります。リストから鍵ポリシーが削除されています。

鍵グループ

鍵グループとは、適用される鍵ポリシーとアクセスできるエージェントを決定するデータコンテキストです。鍵がエージェントに割り当てられ、データユニットに対してはじめて使用されるときに、鍵は鍵グループに関連付けられます。鍵グループを作成するときには、鍵ポリシーを選択する必要があります。選択した鍵ポリシーが、その鍵グループ内の鍵に適用されます。

エージェントは鍵グループに関連付けられます。エージェントは、アクセスを許可された 1 つ以上の鍵グループを持ちます。エージェントは、アクセスを許可された鍵グループに属する鍵のみを取得できます。エージェントがデフォルトの鍵グループを持つ場合もあります。エージェントによって新しい鍵が割り当てられると、その鍵はエージェントのデフォルトの鍵グループ内に配置されます。エージェントは、デフォルトの鍵グループが存在する場合にのみ、新しい鍵を割り当てることができます。

178 ページの図 6-1 に、鍵グループ、鍵ポリシー、エージェント、およびデータユニットの関係を示します。

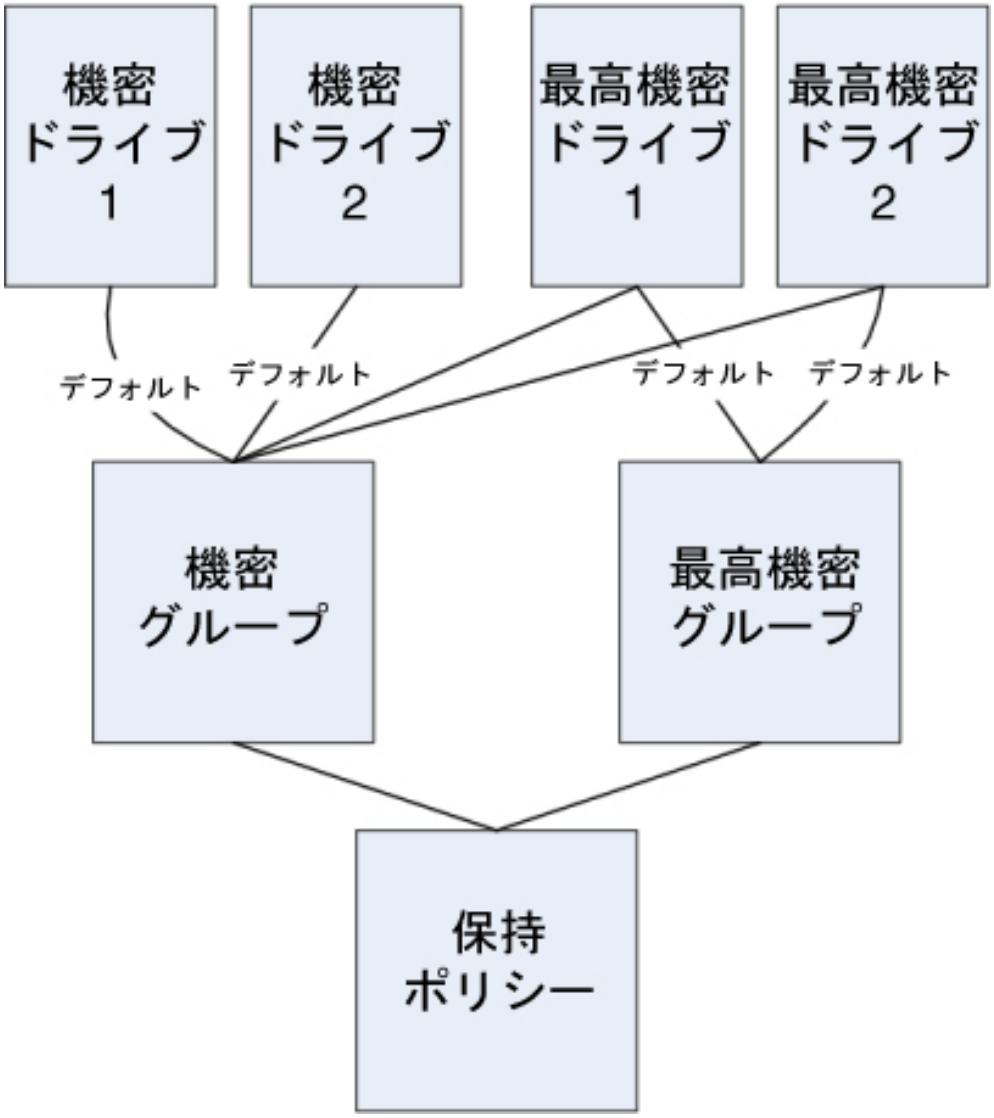
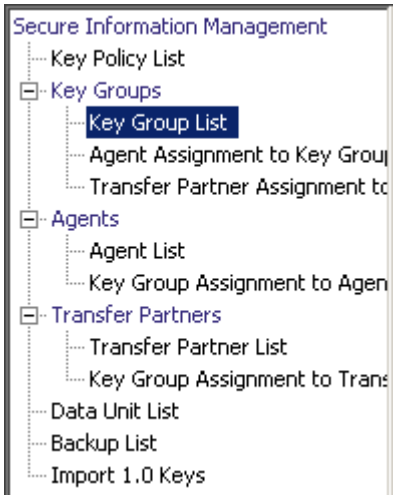


図 6-1　　鍵グループと鍵ポリシー、エージェント、データユニットとの関係

「Key Groups」メニュー

「Key Groups」メニューに含まれている「Key Group List」メニューオプションを使用すると、コンプライアンス責任者は、鍵グループを管理できます。



「Key Group List」メニュー

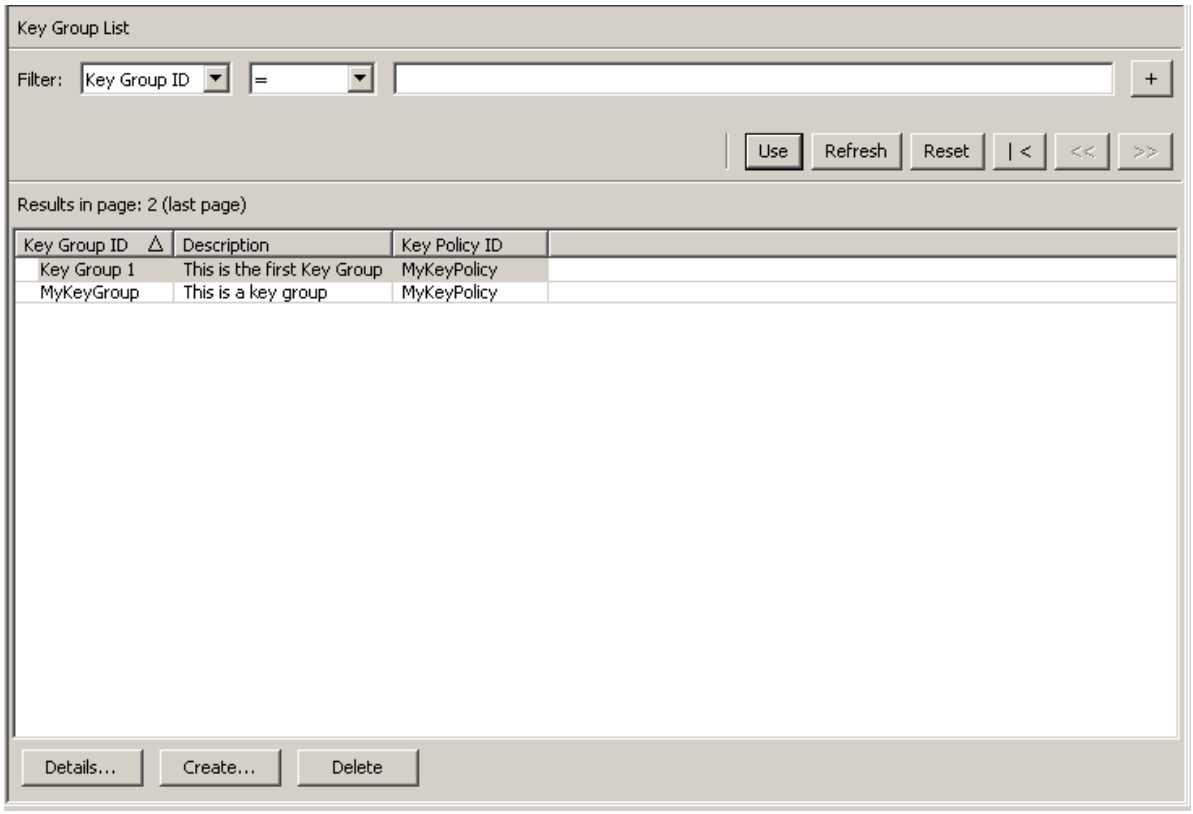
「Key Group List」メニューオプションを使用すると、ユーザーは次の操作を行うことができます。

- 鍵グループの表示
- 鍵グループの作成
- 既存の鍵グループの変更
- 既存の鍵グループの削除

鍵グループの表示

すべての鍵グループを表示するには、次の手順を実行します。

1. 「Key Groups」メニューから、「Key Group List」を選択します。「Key Group List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで鍵グループリストにフィルタを適用することもできます。

- Key Group ID
- Description
- Key Policy ID

表示されている鍵グループリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

表示されている鍵グループのリストにフィルタを適用するためのフィルタオプションを選択します。すべてのフィルタの条件を満たす鍵グループのみが表示されます。

フィルタ属性コンボボックス:

下矢印ボタンをクリックし、フィルタ条件として使用する属性を選択します。次に示す値を取ります。

- Key Group ID
- Description
- Key Policy ID

フィルタ演算子ボックス:

下矢印ボタンをクリックし、選択した属性に適用するフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス:

選択した属性のフィルタ条件として使用する値を入力します。

フィルタ値コンボボックス:

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

Use:

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

Refresh:

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、項目数に「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

Key Group ID

各鍵グループを識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。鍵グループ ID は、いったん定義すると変更できません。

Description

鍵グループの説明が示されます。この値は、1 ～ 64 文字で指定できます。

Key Policy ID

鍵グループ内の各データユニットに適用される既存の鍵ポリシーを識別する一意の識別子が表示されます。

既存の鍵グループの鍵ポリシー ID は変更できません。これは、変更が多数の鍵に影響することを回避するためです。

鍵グループを作成する場合は、「Create」ボタンを選択します。詳細は、183 ページの「鍵グループの作成」を参照してください。

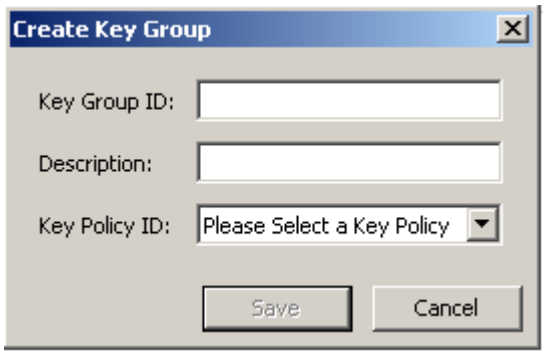
鍵グループを表示または変更する場合は、その鍵グループを強調表示して「Details」ボタンを選択します。詳細は、185 ページの「鍵グループの詳細の表示および変更」を参照してください。

鍵グループを削除する場合は、「Delete」ボタンを選択します。詳細は、186 ページの「鍵グループの削除」を参照してください。

鍵グループの作成

新しい鍵グループを作成するには、次の手順を実行します。

1. 「Key Group List」画面で、「Create」ボタンを選択します。「Create Key Group」画面が表示されます。



2. 次のパラメータを設定します。

Key Group ID

鍵グループを識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

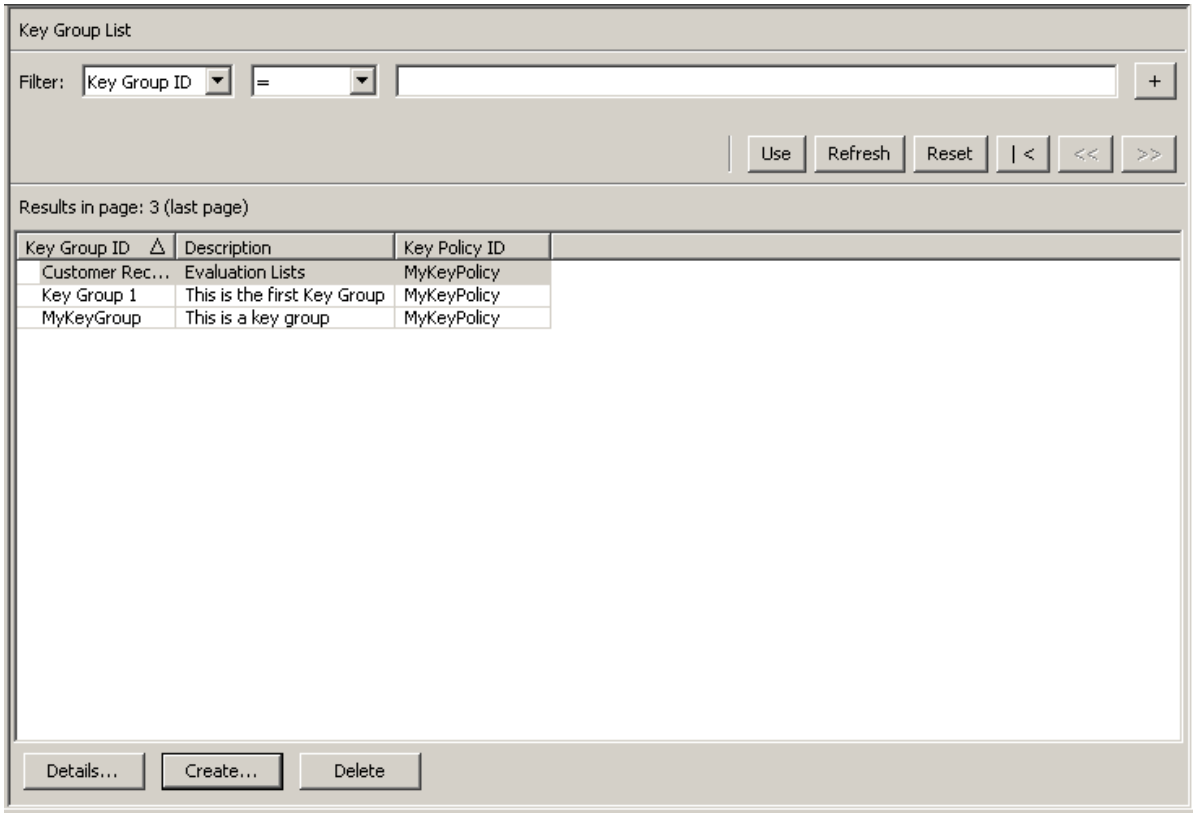
Description

鍵グループを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Key Policy ID

下矢印ボタンをクリックし、この鍵グループに関連付ける鍵ポリシーを選択します。新しい鍵グループを作成する場合は、既存の鍵ポリシーが表示されます。

3. 「Save」ボタンを選択します。新しい鍵グループが作成されてデータベースに保存され、「Key Group List」画面に表示されます。これで、データユニット、エージェントなどで鍵グループを使用できるようになります。

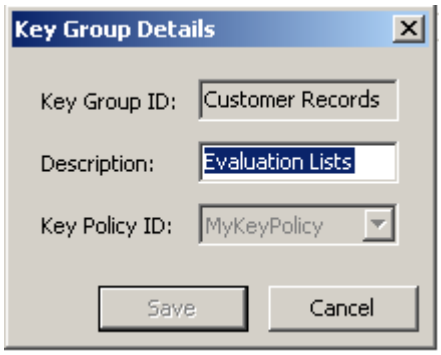

Key Group List
Filter:
Key Group ID
=
+
Use
Refresh
Reset
| <
<<
>>
Results in page: 3 (last page)
Key Group ID
Description
Key Policy ID
Customer Rec...
Evaluation Lists
MyKeyPolicy
Key Group 1
This is the first Key Group
MyKeyPolicy
MyKeyGroup
This is a key group
MyKeyPolicy
Details...
Create...
Delete

鍵グループの詳細の表示および変更

注 – コンプライアンス責任者以外のユーザーが鍵グループの詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。

鍵グループを変更するには、次の手順を実行します。

1. 「Key Group List」画面で、詳細情報を表示する鍵グループエントリをダブルクリックするか、または鍵グループエントリを強調表示して「Details」ボタンを選択します。「Key Group Details」画面が表示されます。



次のパラメータが表示されます。

Key Group ID:

鍵グループを一意に識別します。このフィールドは読み取り専用です。

Description:

鍵グループを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。このフィールドは、空白のままにすることができます。

Key Policy ID:

鍵グループおよび鍵グループ内のすべての鍵に関連付けられている既存の鍵ポリシーを識別する一意の識別子が表示されます。このフィールドは読み取り専用です。

2. 変更できるのは「Description」フィールドのみです。終了したら、「Save」ボタンを選択して変更内容を保存します。「Key Group List」画面に戻ります。

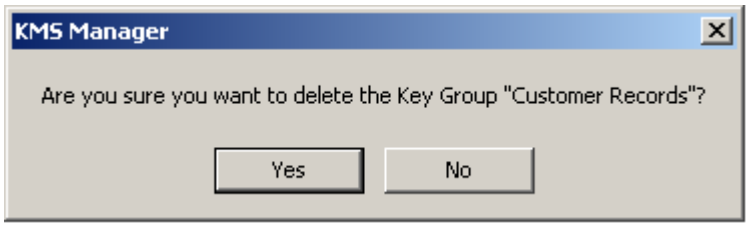
鍵グループの削除

注 – アクティブな鍵グループ、つまりエージェントまたはデータユニットが割り当てられている鍵グループは削除できません。

鍵グループを削除するには、次の手順を実行します。

1. 「Key Groups List」画面で、削除する鍵グループを強調表示して「Delete」ボタンを選択します。次のように、選択した鍵グループの削除を確認するダイアログボックスが表示されます。

   鍵グループは、鍵で使用されておらず、エージェントにも関連付けられていない場合にのみ削除できます。

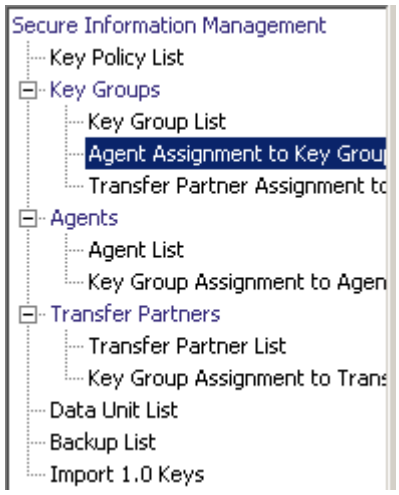


2. 「Yes」ボタンを選択して、鍵グループを削除します。鍵グループと、それに関連付けられたエントリが、データベースから削除されます。「Key Group List」画面に戻ります。リストから鍵グループが削除されています。

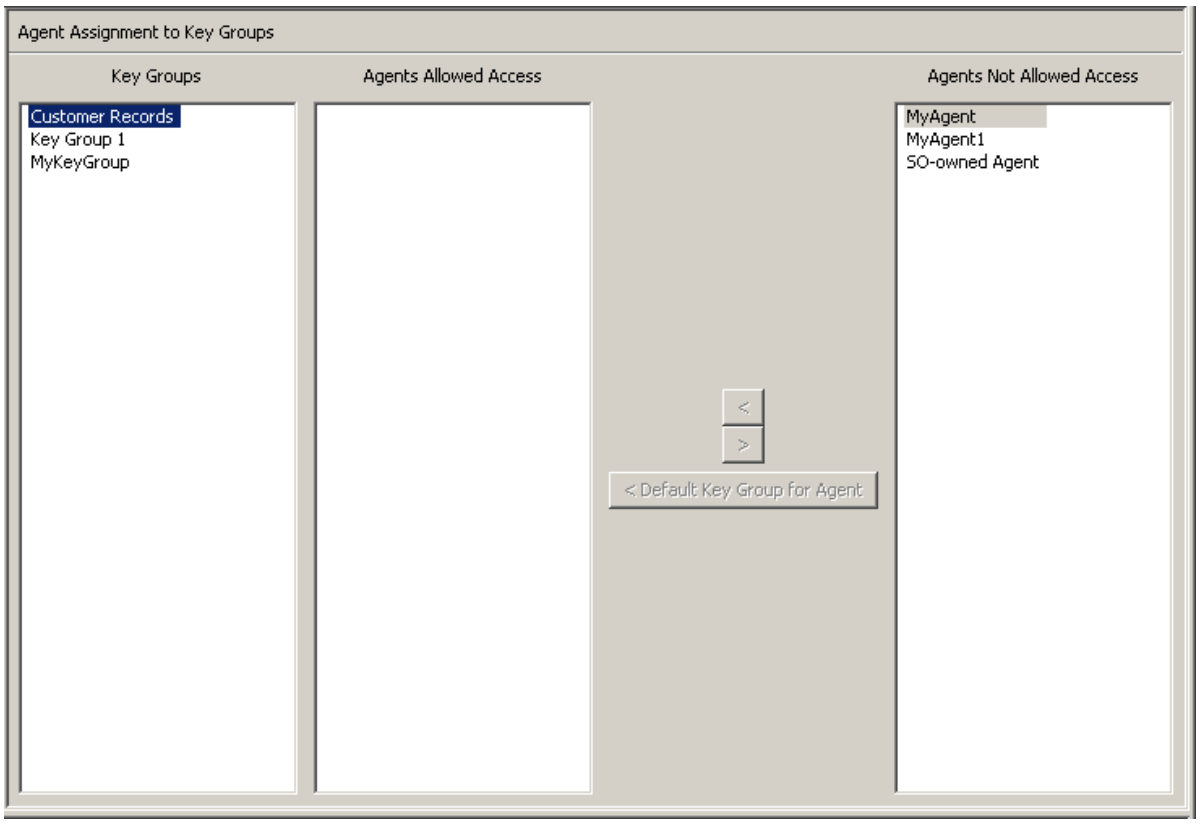
「Agent Assignment to Key Groups」メニュー

「Agent Assignment to Key Groups」メニューオプションを使用すると、ユーザーは、エージェントを鍵グループに割り当てることができます。エージェントを鍵グループに割り当てることで、そのエージェントがアクセスできるストレージデバイスが決定されます。これは「Agents」メニューの「Key Group Assignment」メニューオプションの逆の操作ですが、どちらも結果は同じになります。

重要 – エージェントによる鍵の割り当てを可能にするには、あらかじめエージェントにデフォルトの鍵グループを設定しておく必要があります。



エージェント割り当てを表示するには、「Key Groups」メニューから「Agent Assignment to Key Groups」を選択します。「Agent Assignment to Key Groups」画面が表示されます。

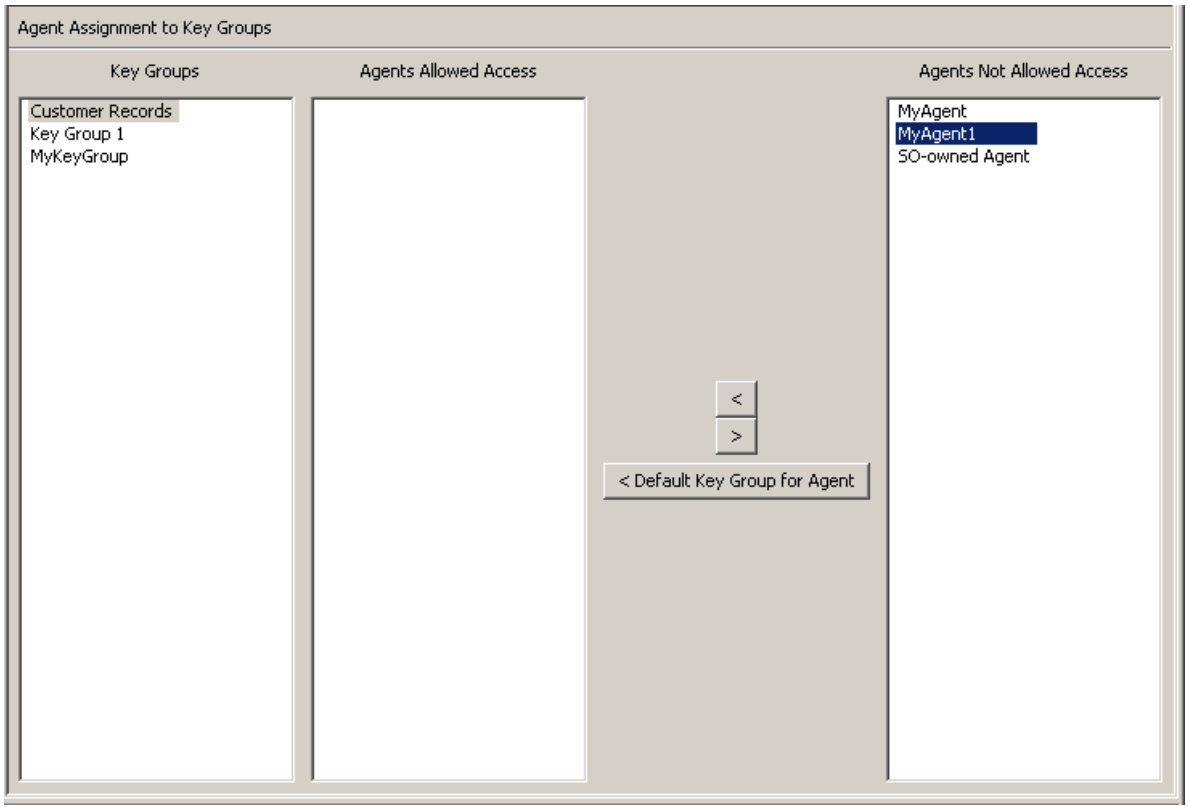


「Key Groups」列に、鍵グループが一覧表示されます。「Agents Allowed Access」列に、選択した鍵グループに割り当てられているエージェントが一覧表示されます。「Agents Not Allowed Access」列に、選択した鍵グループに割り当てられていないエージェントが一覧表示されます。

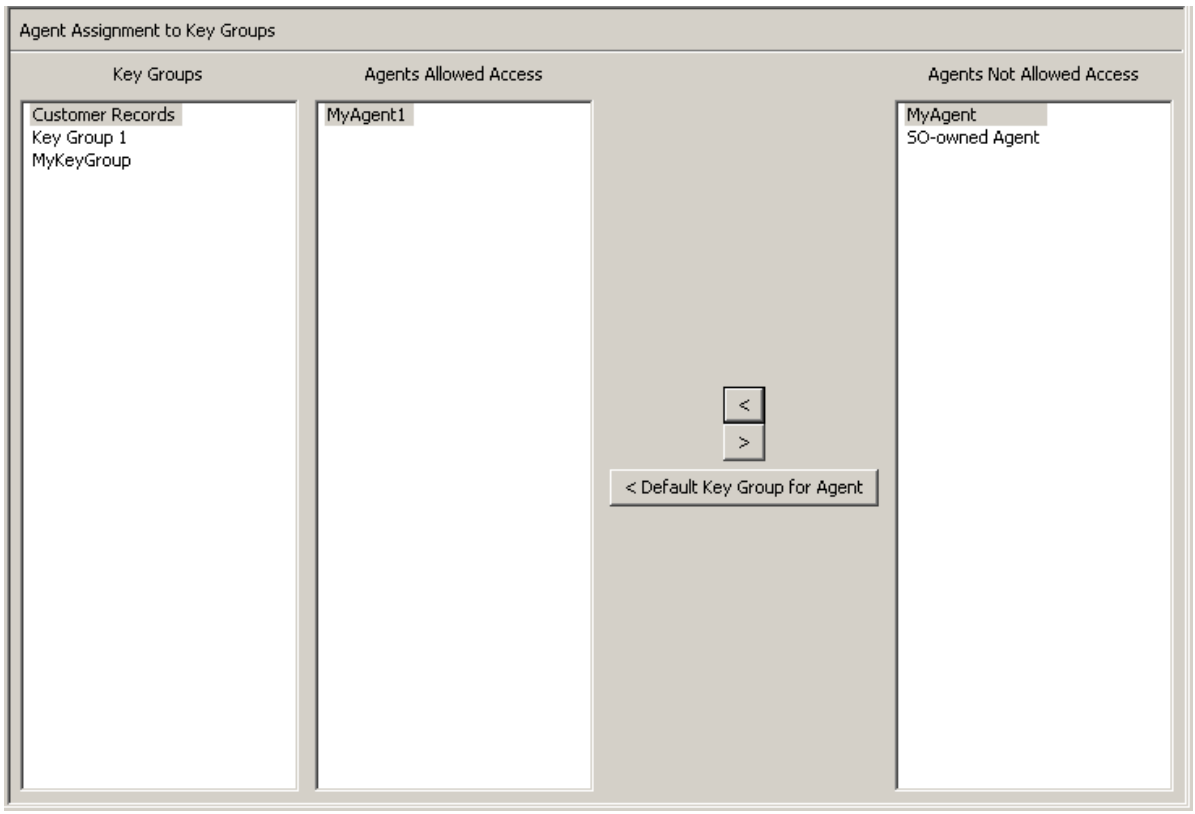
鍵グループへのエージェントの割り当て

鍵グループにエージェントを割り当てるには、次の手順を実行します。

1. 「Key Groups」列で、必要な鍵グループを強調表示します。「Agents Not Allowed Access」列で、追加するエージェントを強調表示し、「Move to」 < ボタンを選択します。



2. 選択したエージェントが「Agents Allowed Access」列に移動して、選択した鍵グループのエージェントリストにエージェントが正常に追加されたことを示します。



エージェントを鍵グループに割り当て、デフォルトの鍵グループを設定するには、次の手順を実行します。

1. 「Agent Assignment to Key Groups」画面で、「Key Groups」リストから必要な鍵グループを選択します。
2. 「Agents Not Allowed Access」リストで、追加してデフォルトの鍵グループを設定するエージェントを 1 つ以上選択します。
3. 「Default Key Group for Agent」ボタンをクリックします。選択したエージェントが「Agents Allowed Access」リストに移動して、その鍵グループにデフォルトの鍵グループが設定されます。これにより、エージェントは鍵グループにアクセスできるようになります。

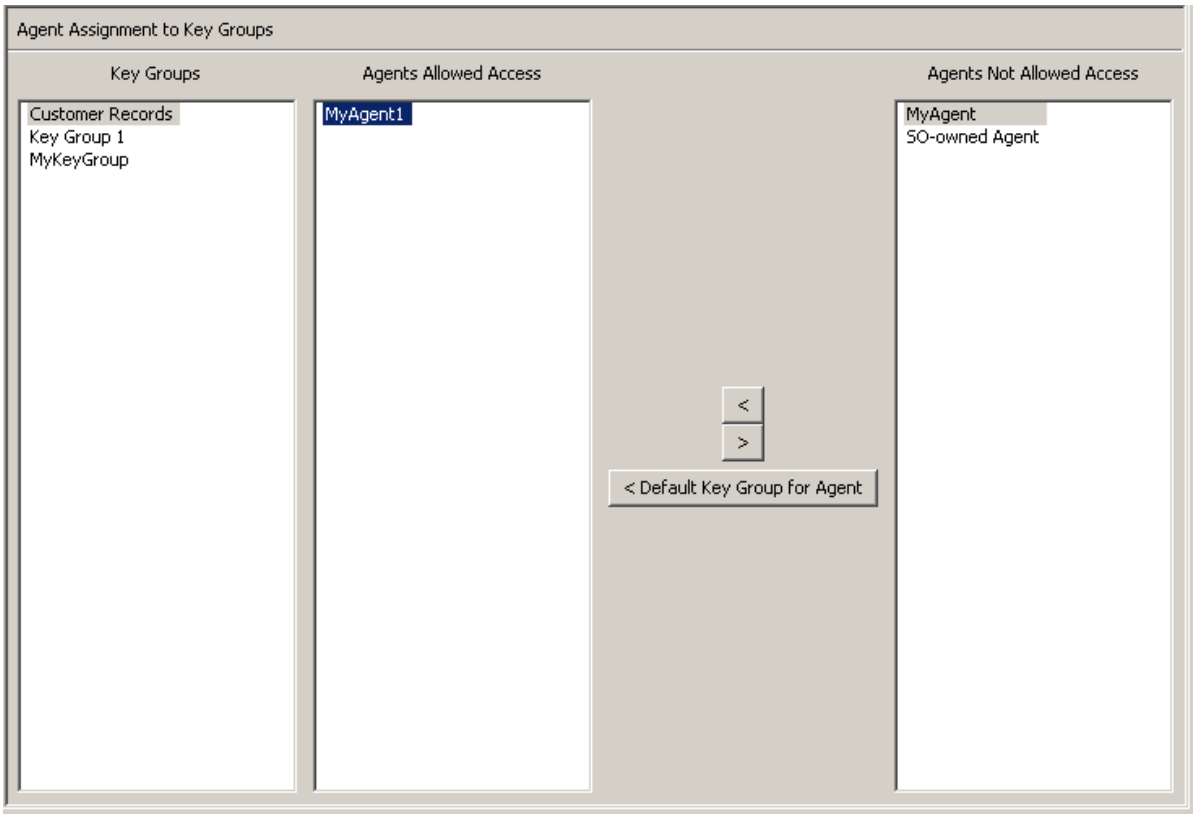
すでに割り当てられているエージェントに対してデフォルトの鍵グループを設定するには、次の手順を実行します。

1. 「Agent Assignment to Key Groups」画面で、「Key Groups」リストから必要な鍵グループを選択します。
2. 「Agents Allowed Access」リストで、デフォルトの鍵グループとして選択した鍵グループを持たない 1 つ以上のエージェントを選択します。
3. 「Default Key Group for Agent」ボタンをクリックします。選択したエージェントのデフォルトの鍵グループがその鍵グループに設定されます。

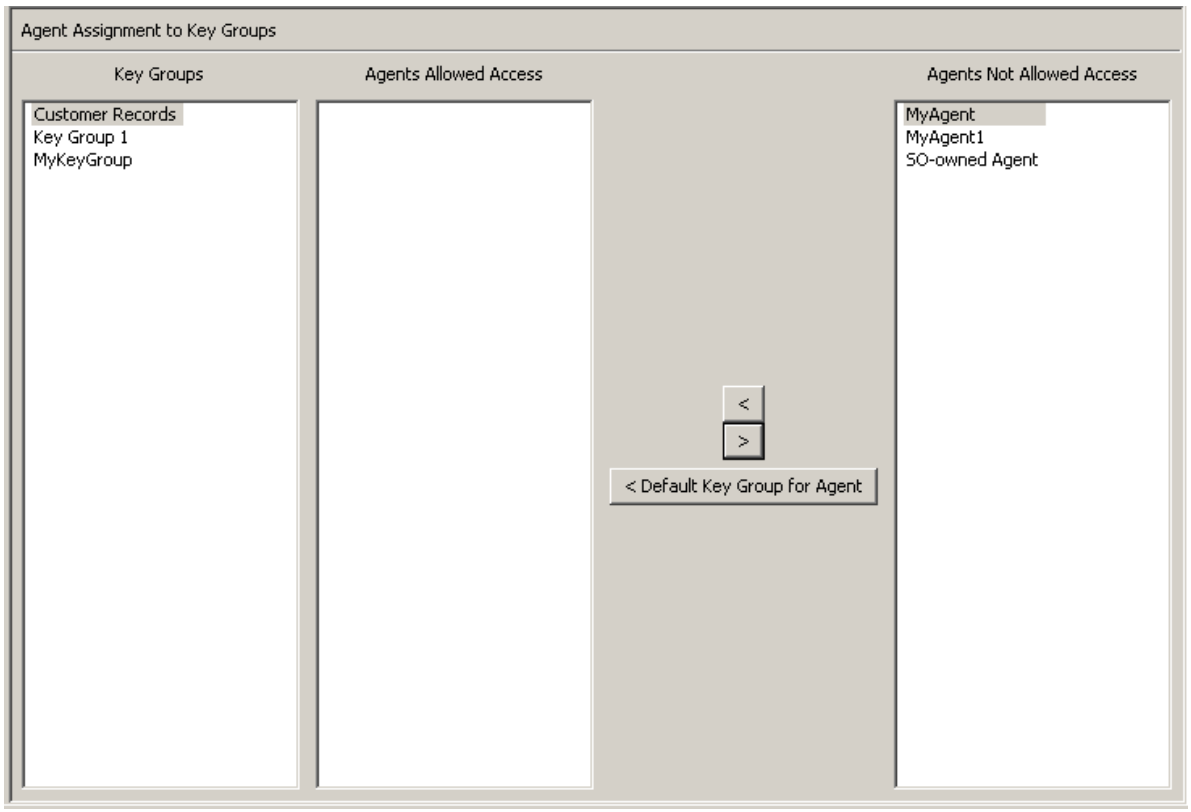
鍵グループからのエージェントの削除

鍵グループのエージェントリストからエージェントを削除するには、次の手順を実行します。

1. 「Key Groups」列で、必要な鍵グループを強調表示します。「Agents Allowed Access」列で、削除するエージェントを強調表示し、「Move from」 > ボタンを選択します。

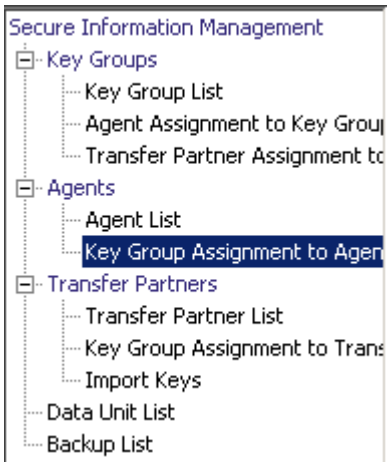


2. 選択したエントリが「Agents Allowed Access」列から削除され、「Agents Not Allowed Access」列に表示されます。選択した鍵グループへの割り当ては解除されています。


Agent Assignment to Key Groups
Key Groups
Agents Allowed Access
Agents Not Allowed Access
Customer Records
Key Group 1
MyKeyGroup
MyAgent
MyAgent1
SO-owned Agent
<
>
< Default Key Group for Agent

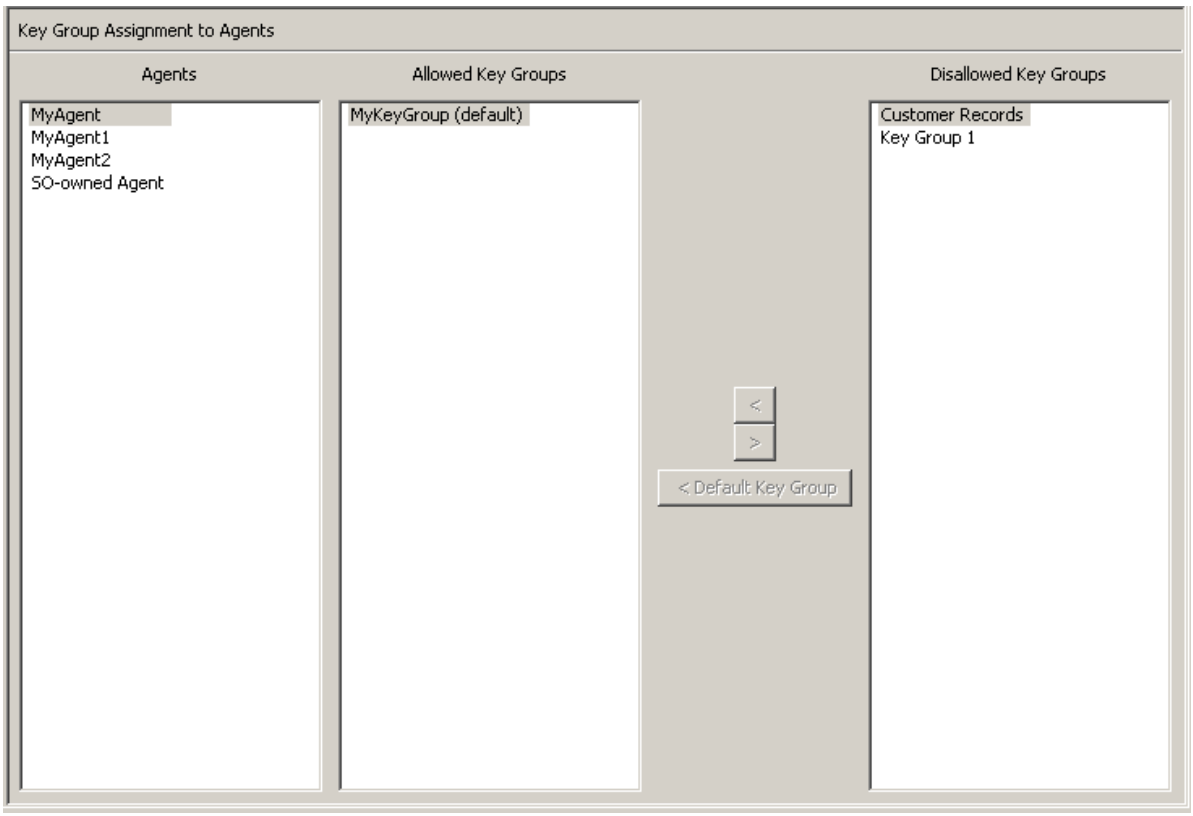
「Key Group Assignment to Agents」メニュー

「Key Group Assignment to Agents」メニューオプションを使用すると、鍵グループをエージェントに割り当てることができます。これは「Agent Assignment to Key Groups」メニューオプションの逆の操作ですが、どちらも結果は同じになります。



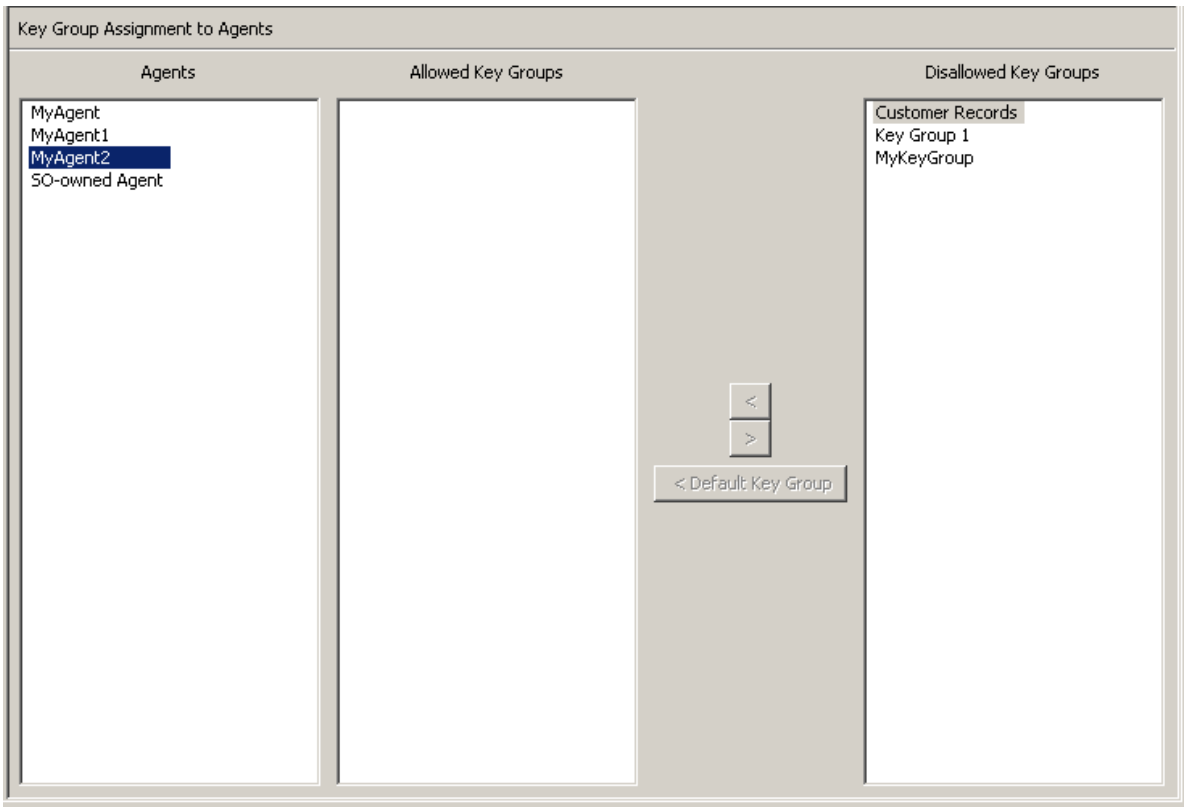
鍵グループを表示するには、次の手順を実行します。

1. 「Agents」メニューから、「Key Group Assignment」を選択します。「Key Group Assignment to Agents」画面が表示されます。



「Agents」列に、データベース内のエージェントが一覧表示されます。「Allowed Key Groups」列に、エージェントがアクセスできる鍵グループが一覧表示されます。「Disallowed Key Groups」列に、エージェントがアクセスできない鍵グループが一覧表示されます。

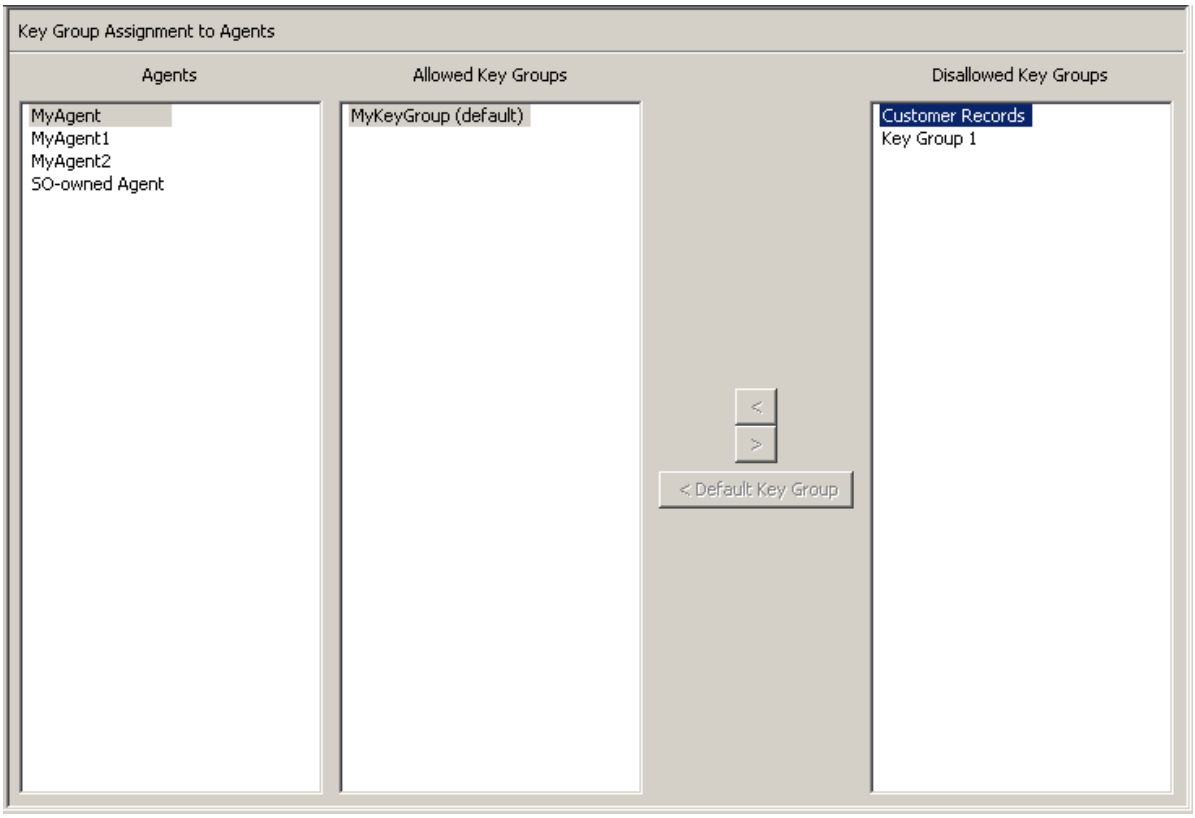
2. エージェントエントリをクリックすると、選択したエージェントのメンバーの鍵グループまたはメンバーでない鍵グループが表示されます。


Key Group Assignment to Agents
Agents
Allowed Key Groups
Disallowed Key Groups
MyAgent
MyAgent1
MyAgent2
SO-owned Agent
Customer Records
Key Group 1
MyKeyGroup
<
>
< Default Key Group

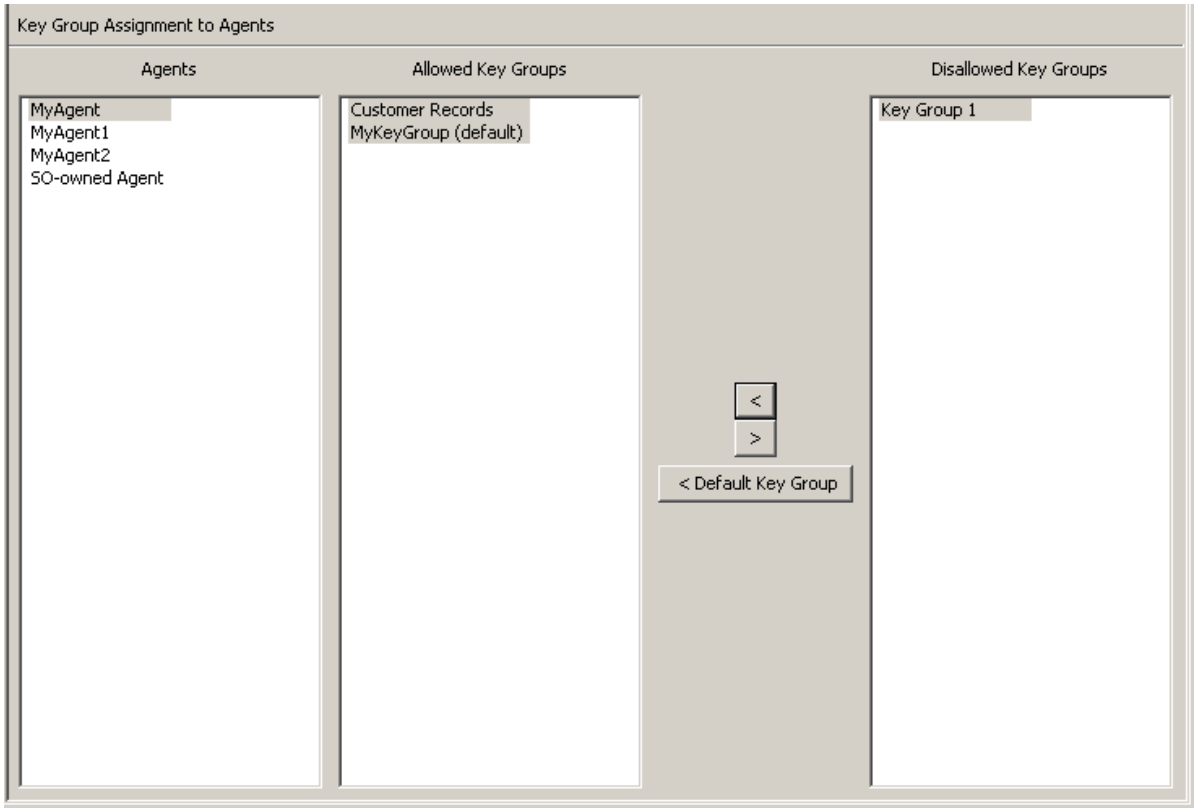
エージェントへの鍵グループの割り当て

エージェントに鍵グループを割り当てるには、次の手順を実行します。

1. 「Key Group Assignment to Agents」画面の「Agents」列で、必要なエージェントを強調表示します。「Disallowed Key Groups」列で、追加する鍵グループを強調表示し、「Move to」 < ボタンを選択します。



2. 選択したエントリが「Allowed Key Groups」列に移動し、選択したエージェントに鍵グループが正常に追加されます。



鍵グループをデフォルトの鍵グループとしてエージェントに割り当てるには、次の手順を実行します。

1. 「Key Group Assignment to Agents」画面の「Agents」リストで、必要なエージェントを選択します。
2. 「Disallowed Key Groups」リストで、追加してデフォルトの鍵グループとして設定する鍵グループを 1 つ選択します。
3. 「Default Key Group」ボタンをクリックします。選択した鍵グループが「Allowed Key Groups」リストに移動し、エージェントのデフォルトの鍵グループとして設定されます。これにより、エージェントは鍵グループにアクセスできるようになります。

すでに割り当てられている鍵グループをデフォルトの鍵グループに設定するには、次の手順を実行します。

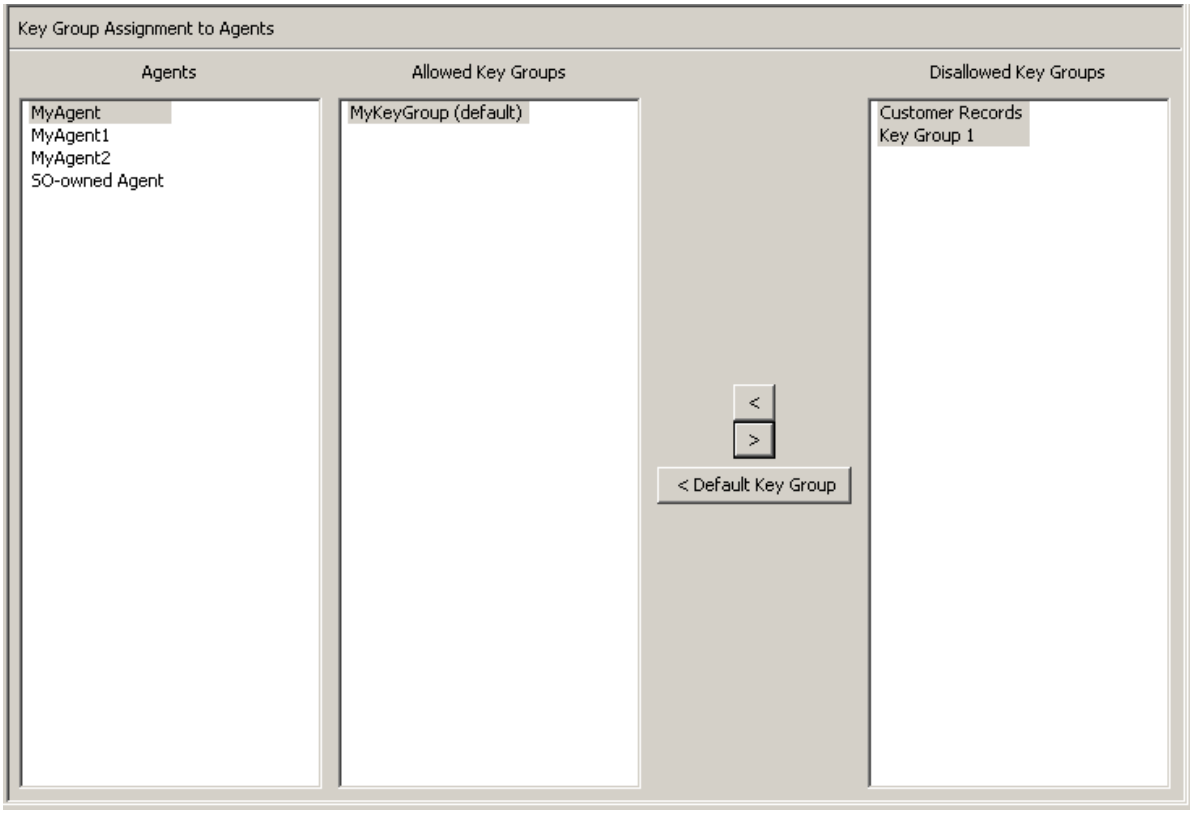
1. 「Key Group Assignment to Agents」画面の「Agents」リストで、必要なエージェントを選択します。
2. 「Allowed Key Groups」リストで、エージェントのデフォルトの鍵グループになっていない鍵グループを 1 つ選択します。

「Default Key Group」ボタンをクリックします。エージェントのデフォルトの鍵グループに、選択した鍵グループが設定されます。

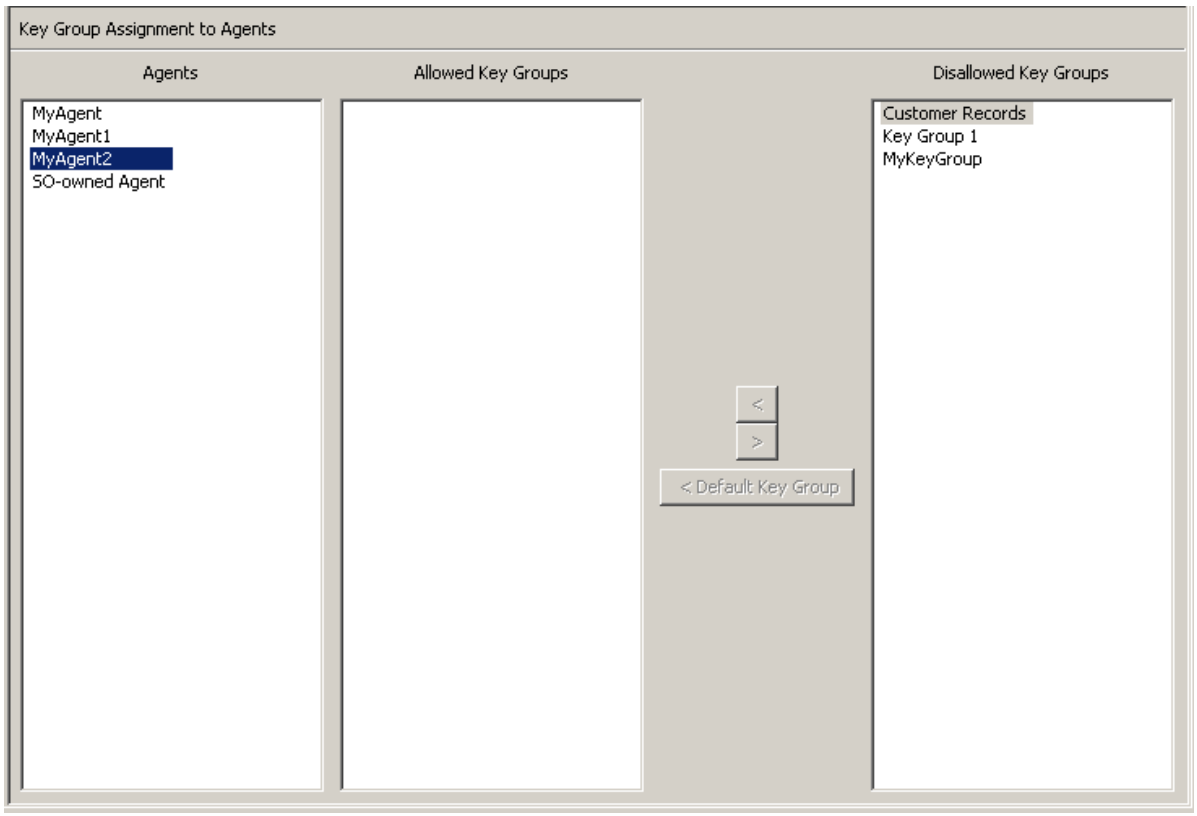
エージェントからの鍵グループの削除

エージェントから鍵グループを削除するには、次の手順を実行します。

1. 「Key Group Assignment to Agents」画面の「Agents」列で、必要なエージェントを強調表示します。「Allowed Key Groups」列で、削除する鍵グループを強調表示し、「Move from」 > ボタンを選択します。



2. 選択したエントリが「Allowed Key Groups」列から「Non-member of Info. Groups」列に移動し、エージェントへの割り当てが解除されます。

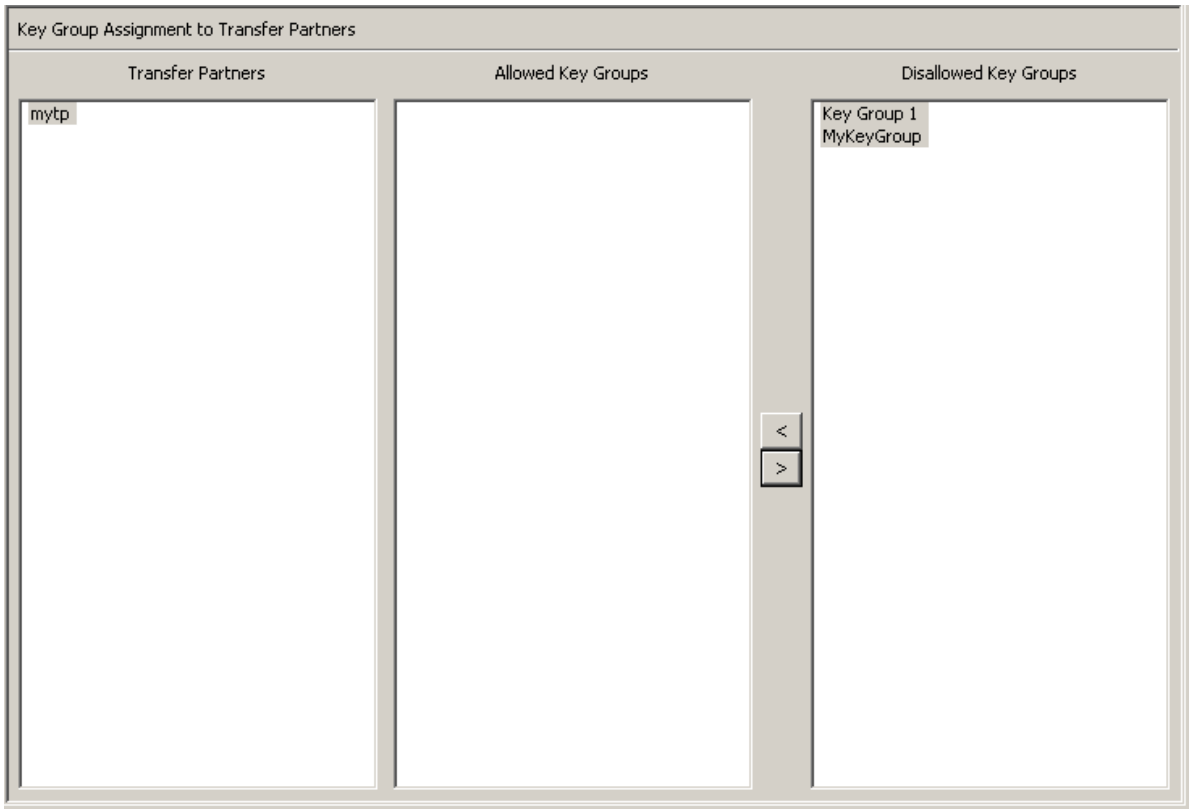

Key Group Assignment to Agents
Agents
Allowed Key Groups
Disallowed Key Groups
MyAgent
MyAgent1
MyAgent2
SO-owned Agent
Customer Records
Key Group 1
MyKeyGroup
<
>
< Default Key Group

「Key Group Assignment to Transfer Partners」メニュー

「Key Group Assignment to Transfer Partners」メニューオプションを使用すると、鍵グループを転送パートナーに割り当てることができます。

鍵グループ割り当ての表示

鍵グループ割り当てを表示するには、「Transfer Partners」メニューから「Key Group Assignment to Transfer Partners」を選択します。次の画面が表示されます。

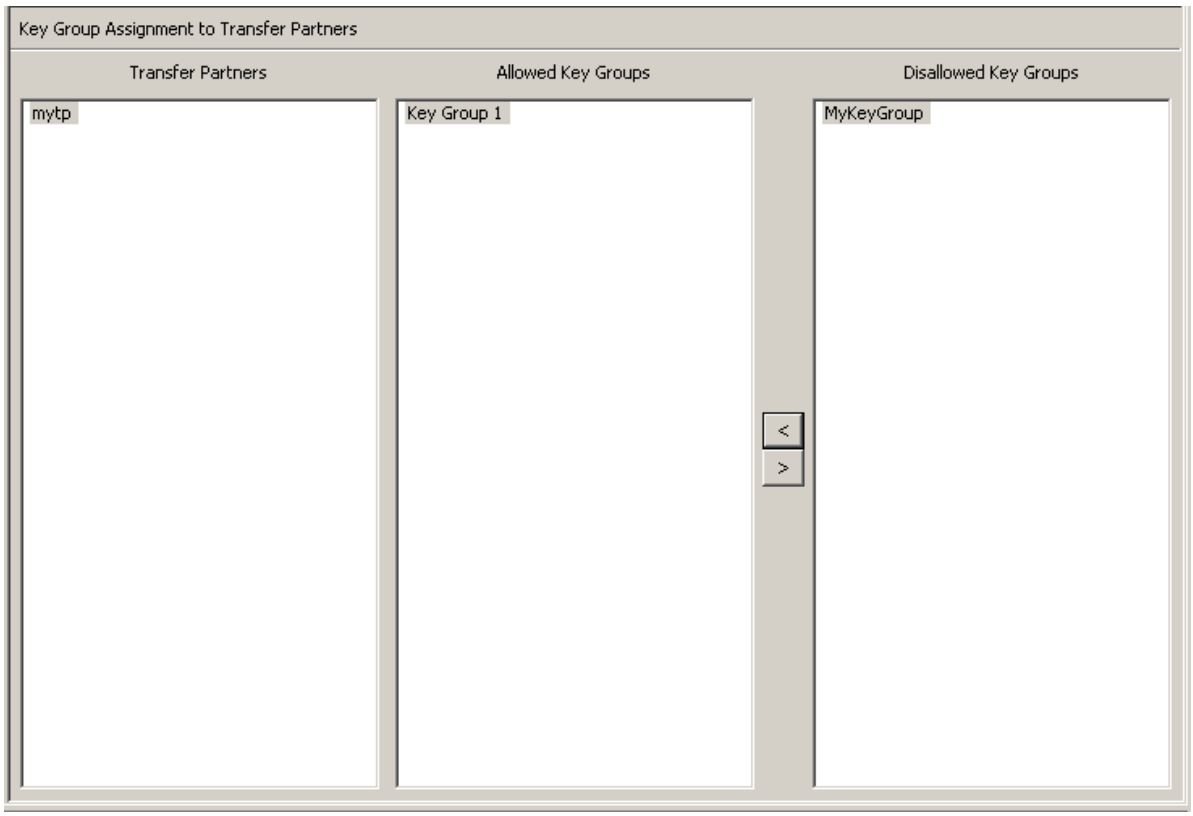


画面に、転送パートナーにアクセスできる鍵グループが表示されます。「Allowed Key Groups」列に、選択した転送パートナーに割り当てられた鍵グループが一覧表示されます。「Disallowed Key Groups」列に、転送パートナーに割り当てられていない鍵グループが表示されます。

転送パートナーへの鍵グループの追加

転送パートナーリストに鍵グループを追加するには、次の手順を実行します。

1. 「Transfer Partners」列で、対象とする転送パートナーを強調表示します。「Disallowed Key Groups」列で、追加する鍵グループを強調表示し、「Move to」 < ボタンを選択します。

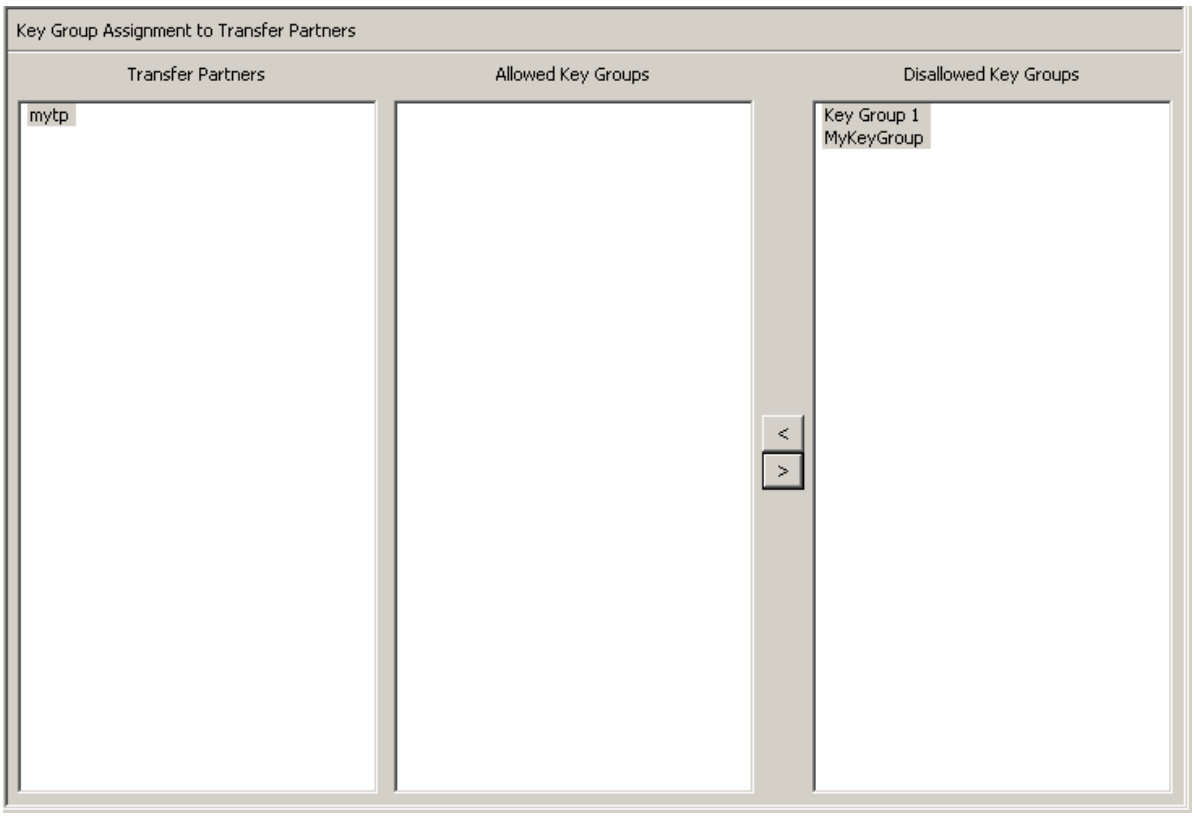


2. 選択した鍵グループが「Allowed Key Groups」列に移動して、転送パートナーがその鍵グループにアクセスできるようになったことを示します。

転送パートナーからの鍵グループの削除

転送パートナーから鍵グループリストを削除するには、次の手順を実行します。

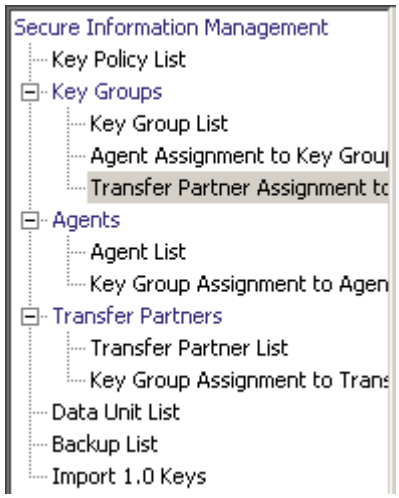
1. 「Transfer Partners」列で、対象とする転送パートナーを強調表示します。「Allowed Key Groups」列で、削除する鍵グループを強調表示し、「Move from」 > ボタンを選択します。



2. 選択した鍵グループが「Disallowed Key Groups」列に移動して、転送パートナーがその鍵グループにアクセスできなくなったことを示します。

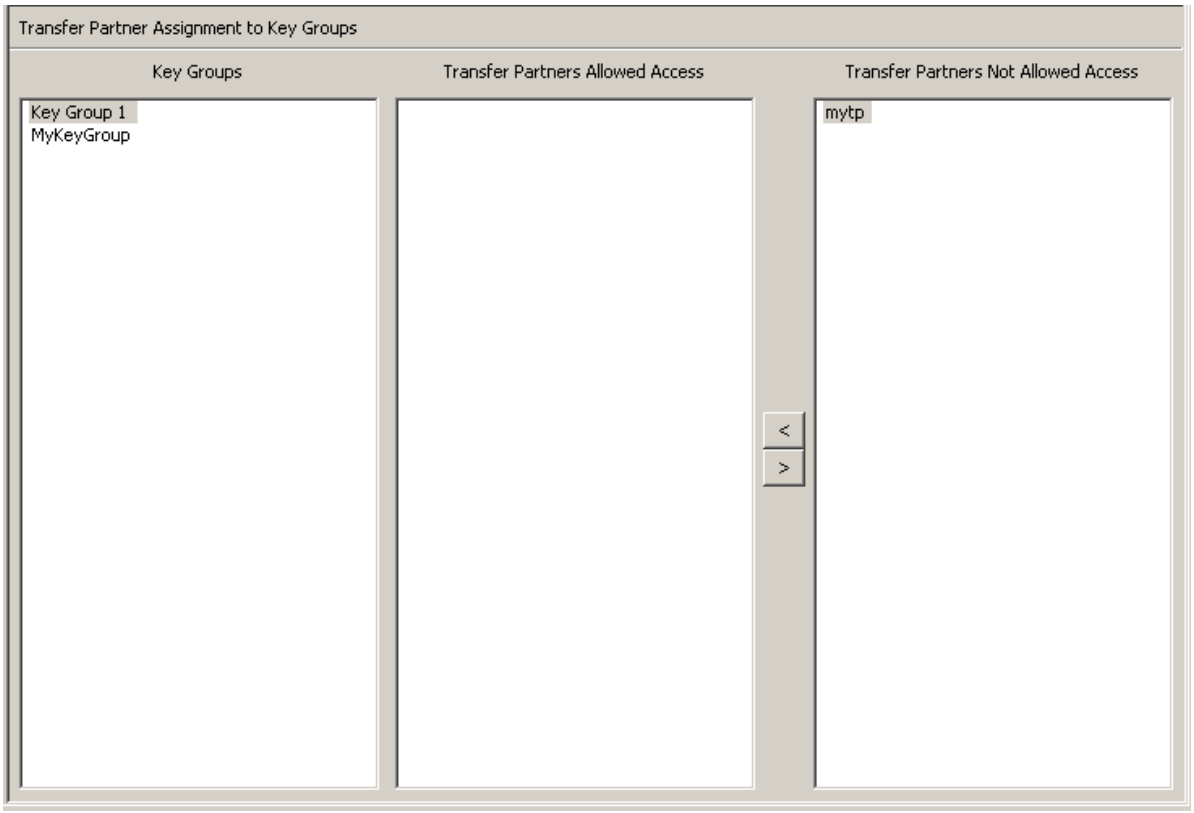
「Transfer Partner Assignment to Key Groups」メニュー

「Transfer Partner Assignment to Key Groups」メニューを使用すると、特定の鍵グループへのアクセスを許可されている一連の鍵転送パートナーに、鍵転送パートナーを追加できます。



転送グループ割り当ての表示

転送グループ割り当てを表示するには、「Key Groups」メニューから「Transfer Partner Assignment to Key Groups」を選択します。次の画面が表示されます。

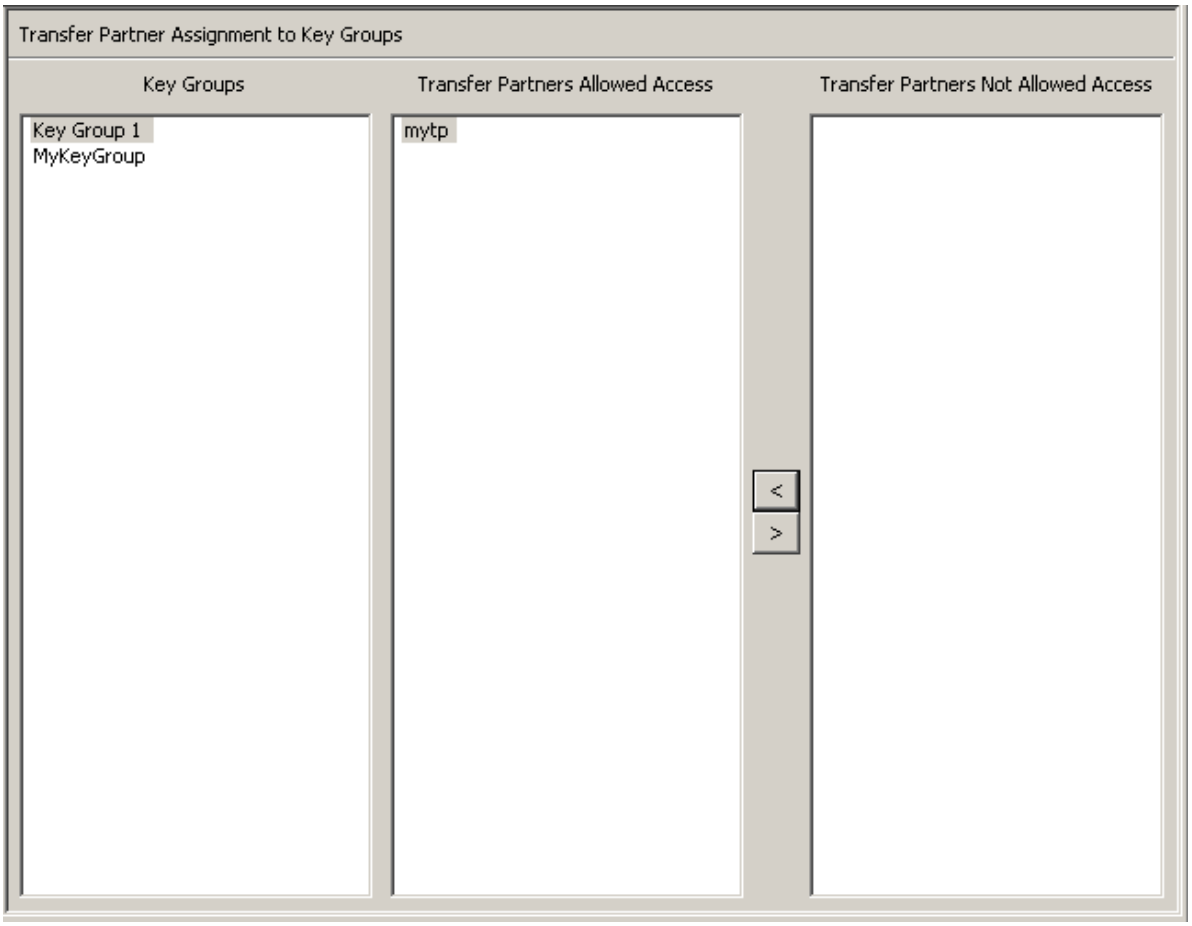


画面には、鍵グループにアクセスできる転送パートナーが表示されます。「Transfer Partners Allowed Access」列に、鍵グループに割り当てられている転送パートナーが一覧表示されます。「Transfer Partners Not Allowed Access」列に、鍵グループに割り当てられていない転送パートナーが表示されます。

鍵グループへの転送パートナーの追加

鍵グループに転送パートナーを追加するには、次の手順を実行します。

1. 「Key Groups」列で、対象とする鍵グループを強調表示します。「Transfer Partners Allowed Access」列で、追加する鍵グループを強調表示し、「Move to」 < ボタンを選択します。

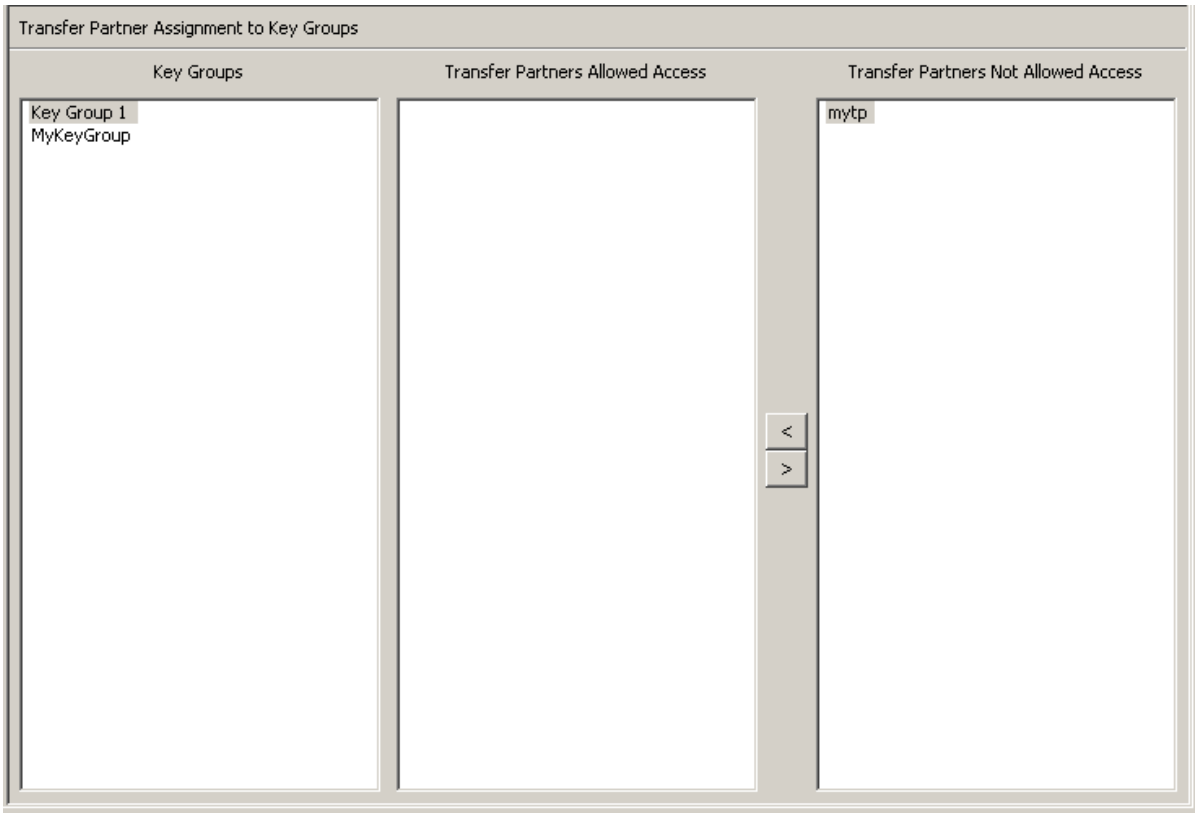


2. 選択した転送パートナーが「Transfer Partners Allowed Access」列に移動して、鍵グループがその転送パートナーにアクセスできるようになったことを示します。

鍵グループからの転送パートナーの削除

鍵グループから転送パートナーを削除するには、次の手順を実行します。

1. 「Key Groups」列で、対象とする鍵グループを強調表示します。「Transfer Partners Allowed Access」列で、削除する転送パートナーを強調表示し、「Move from」 > ボタンを選択します。

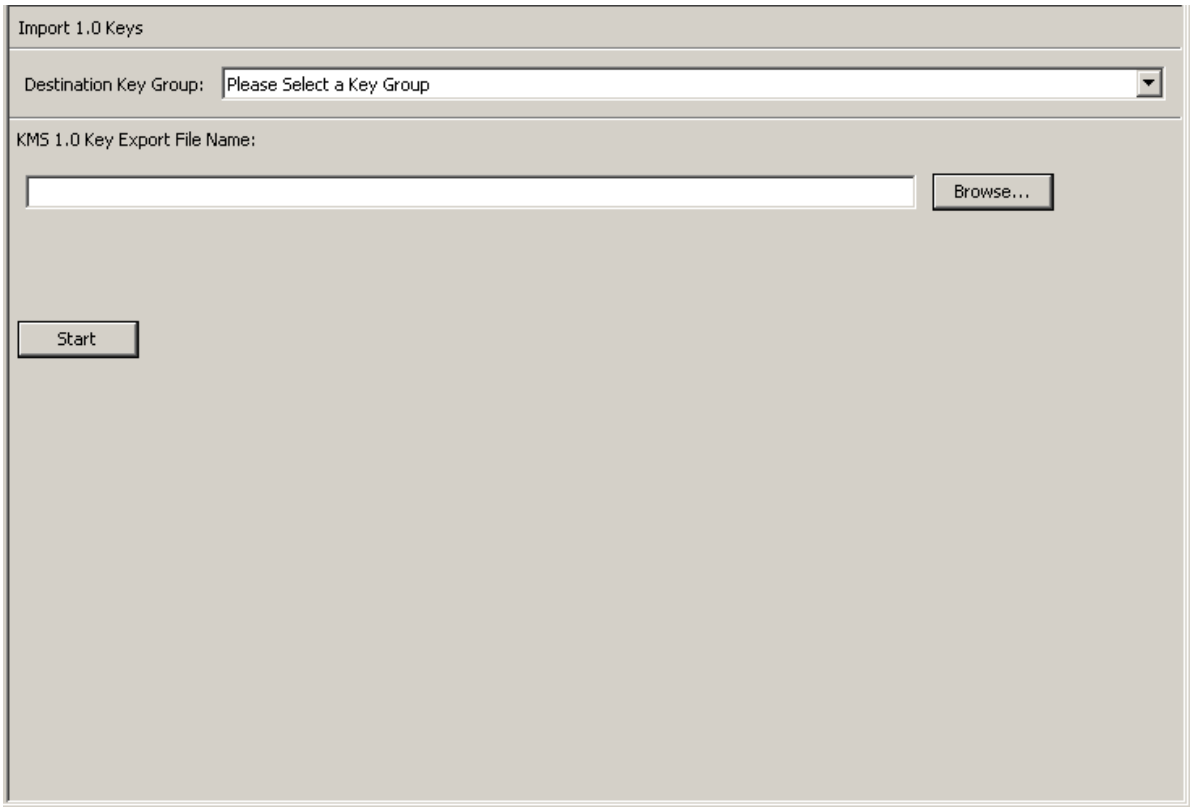


2. 選択した転送パートナーが「Transfer Partners Not Allowed Access」列に移動して、鍵グループがその転送パートナーにアクセスできなくなったことを示します。

KMS 1.0 の鍵エクスポートファイルのインポート

KMS 1.0 の鍵エクスポートファイルを KMA にインポートし、このファイル内の各鍵に対して新しい鍵を作成するには、次の手順を実行します。

1. KMS 1.2 システムに移動し、鍵をファイルにエクスポートします。インポートできるのは、KMS 1.2 システムからエクスポートされた鍵のみです。KMS 1.0 および 1.1 のシステムは、鍵をエクスポートする前に KMS 1.2 にアップグレードする必要があります。
2. 「Secure Information Management」メニューから、「Import 1.0 Keys」を選択します。



3. 次のパラメータを設定します。

Destination Key Group

これらの鍵のインポート先となる鍵グループを選択します。

KMS 1.0 Key Export File Name

KMS 1.0 の鍵エクスポートファイルの名前を入力します。

Browse

このボタンをクリックすると、ファイルの場所を指定できます。

Start

このボタンをクリックすると、KMS 1.0 の鍵ファイルの KMA へのアップロードが開始されます。ファイルに含まれる鍵ごとに、新しい鍵が作成されます。新しい鍵はそれぞれ、選択した鍵グループに関連付けられます。ファイルがアップロードされ適用された時間を示すメッセージが表示されます。

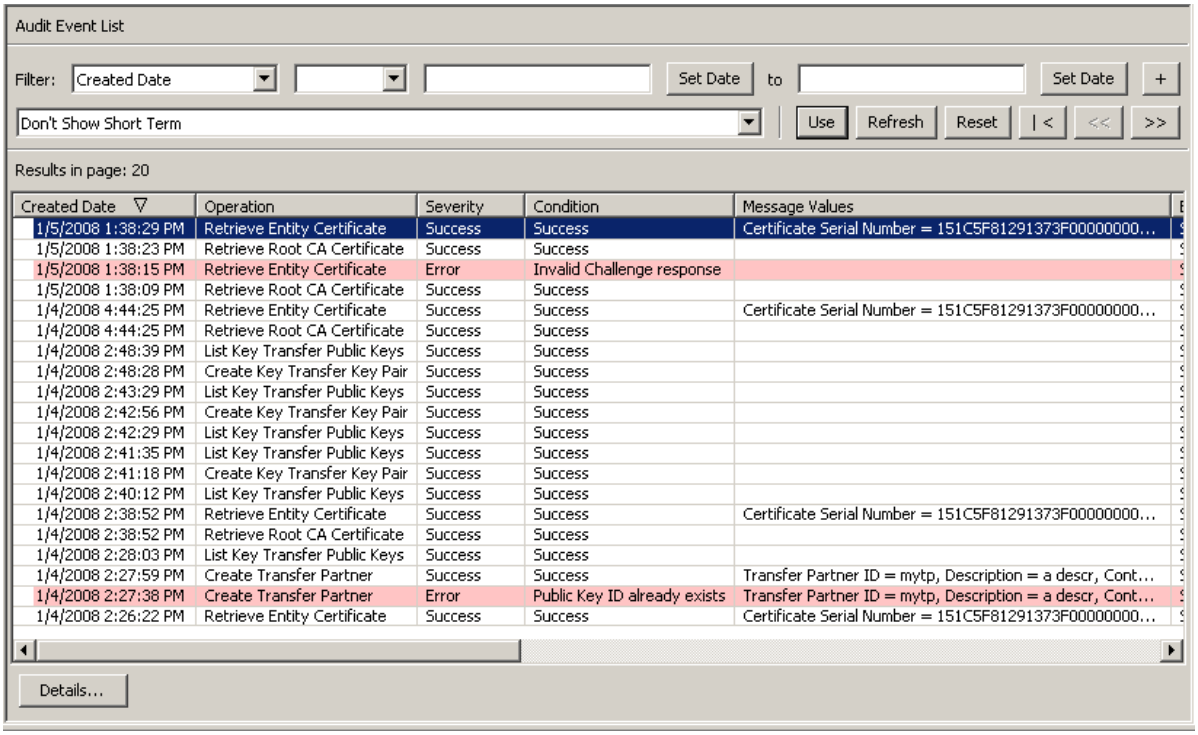
「Audit Event List」メニュー

「Audit Event List」メニューを使用すると、監査ログイベントを表示できます。

監査ログの表示

監査ログイベントを表示するには、次の手順を実行します。

「System Management」メニューから、「Audit Event List」を選択します。「Audit Event List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで監査イベントリストにフィルタを適用することもできます。

- Created Date
- Operation
- Severity
- Condition
- Entity ID
- Entity Network Address
- KMA ID
- KMA Name
- Class
- Retention Term
- Audit Log ID

表示されている監査ログのリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Created Date
- Operation
- Severity
- Condition
- Entity ID
- Entity Network Address
- KMA Name
- Class
- Retention Term
- Audit Log ID

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 空白
- 空白以外

フィルタ値 1 ボックス:

日付フィルタを選択した場合は、「Set Date」をクリックして開始日時を指定します。値は、フィルタキーの範囲の開始値として表示されます。ほかのフィルタを選択した場合は、このフィールドに値を入力します。

フィルタ値 2 ボックス:

日付フィルタを選択した場合は、「Set Date」をクリックして終了日時を指定します。値は、フィルタキーの範囲の終了値として表示されます。

フィルタ値 3 ボックス:

下矢印ボタンをクリックし、次のいずれかのフィルタを選択します。

- Don't Show Short Term
- Show All Retentions

Created Date

監査イベントが作成された日時が表示されます。

Operation

監査イベントレコードが作成される原因となった操作が表示されます。

Severity

操作が失敗した場合の状況の重大度が示されます。「Success」(エラーなし)、「Warning」、または「Error」の値を取ります。

Condition

操作が正常に完了したかどうかが示されます。

注 – エラーは赤色で強調表示され、警告は黄色で強調表示されます。エラーメッセージの上にカーソルを置くと、エラーの詳細な説明が表示されます。

Event Message

監査イベントエントリの詳細情報が表示されます。

Entity ID

操作を実行したユーザーが表示されます。

Entity Network Address

監査イベントを生成した実体のネットワークアドレスが表示されます。

KMA ID

監査イベントエントリの作成元のアプライアンスが表示されます。

KMA Name

クラスタ内の各アプライアンスを識別するユーザー指定の識別子が表示されます。

Class

監査イベントエントリが属する操作のクラスが示されます。次に示す値を取ります。

- Agent Access Control Management Operations
- Agent Client Generated Audits
- Agent Management Operations
- Appliance Management Operations
- Audit Log Agent Operations
- Audit Log Management Operations
- Audit Log Operations
- Backup Management Operations
- CA Operations

- Cluster Client Communication
- Cluster Operations
- Communication and Authentication
- Console Security Management Operations
- Data Unit Agent Operations
- Data Unit Management Operations
- Discovery Operations
- Key Group Agent Operations
- Key Group Management Operations
- Key Policy Management Operations
- License Key Management Operations
- Local Management Operations
- Management Client Generated Audits
- Passphrase Agent Operations
- Replication Operations
- Retrieve Certificate Operations
- Role Management operations
- SNMP Management Operations
- Security Management Operations
- Security Parameter Management Operations
- Security Violation
- Site Management Operations
- System Messages
- User Management Operations

Retention Term

監査イベントレコードの定義された保持期間が表示されます。次に、表示される可能性のある値とその説明を示します。

Long Term

長い期間格納する必要のあるイベントレコード。

Medium Term

中程度の期間格納する必要のあるイベントレコード。

Short Term

短い期間格納する必要のあるイベントレコード。

Audit Log Entry ID

監査イベントエントリの各タイプを識別する一意のシステム生成識別子が表示されます。

Audit Log ID

各監査イベントエントリを識別する一意のシステム生成識別子が表示されます。

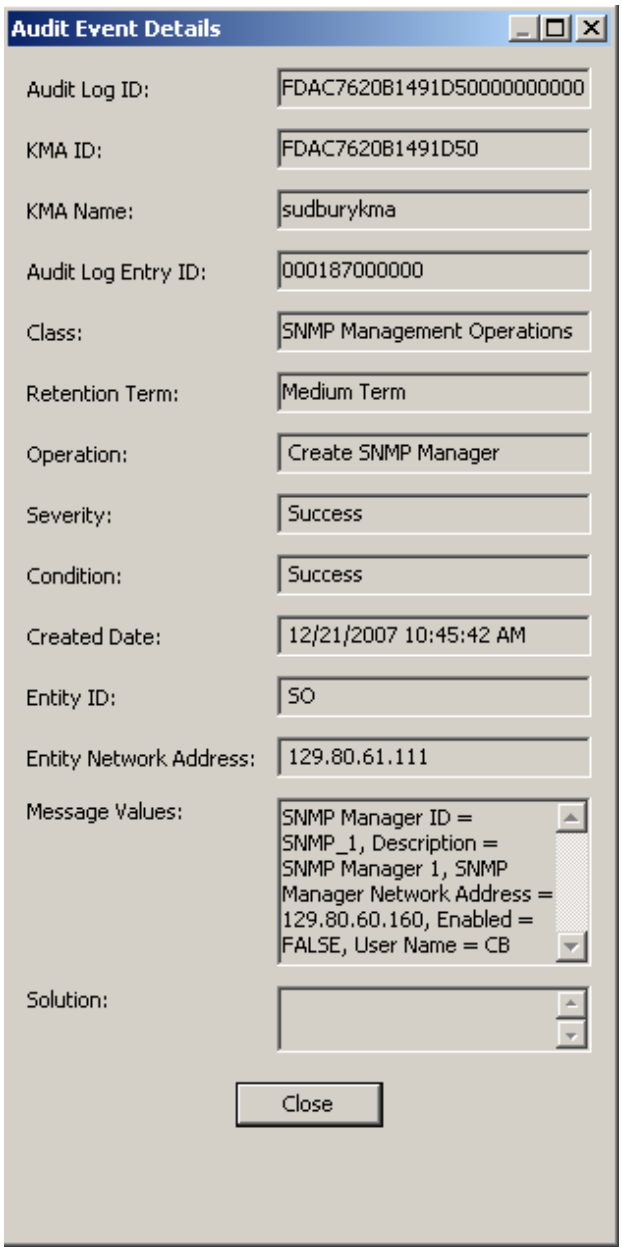
監査ログの詳細を表示する場合は、その監査ログを強調表示して「Details」ボタンを選択します。詳細は、214 ページの「監査ログの詳細の表示」を参照してください。

監査ログをエクスポートするには、「Export」ボタンを選択します。詳細は、215 ページの「監査ログのエクスポート」を参照してください。

監査ログの詳細の表示

監査ログの詳細を表示するには、次の手順を実行します。

1. 「Audit Event List」画面で、詳細情報を表示する監査ログエントリを選択して「Details」ボタンを選択するか、またはエントリをダブルクリックします。「Audit Event Details」画面が表示され、「Close」ボタンを除くすべてのフィールドが使用不可になっています。



2. 「Close」ボタンを選択して、「Audit Event List」画面に戻ります。

監査ログのエクスポート

エクスポート機能を使用すると、すべての監査ログエントリまたは指定した監査ログエントリを、ユーザーのワークステーションのテキストファイルにエクスポートできます。ユーザーは、このファイルをスプレッドシートアプリケーションで表示できます。

監査ログをエクスポートするには、次の手順を実行します。

1. 「Audit Event List」画面で、「View」メニューから「Save Report...」を選択するか、または Ctrl-S を押します。
2. 終了したら、「Start」ボタンを選択してエクスポート処理を開始します。「Audit Event List」画面でエントリにフィルタを適用した場合は、該当するエントリのみがエクスポートされます。フィルタを適用していない場合は、すべての監査イベントがエクスポートされます。
3. エクスポート処理が完了すると、エクスポートされた監査ログの数が、ダイアログボックスの下部に表示されます。
4. 「Close」ボタンを選択してこのダイアログボックスを閉じ、「Audit Event List」画面に戻ります。

「Data Units」メニュー

「Data Units」メニューの使用法については、232 ページの「「Data Unit List」メニュー」を参照してください。

その他の機能

コンプライアンス責任者は、次の操作を行うこともできます。

- 監査イベントリストの表示
- システム時刻の表示
- KMA 状態のロックおよびロック解除

これらの機能の手順については、第 5 章「セキュリティー責任者の操作」を参照してください。

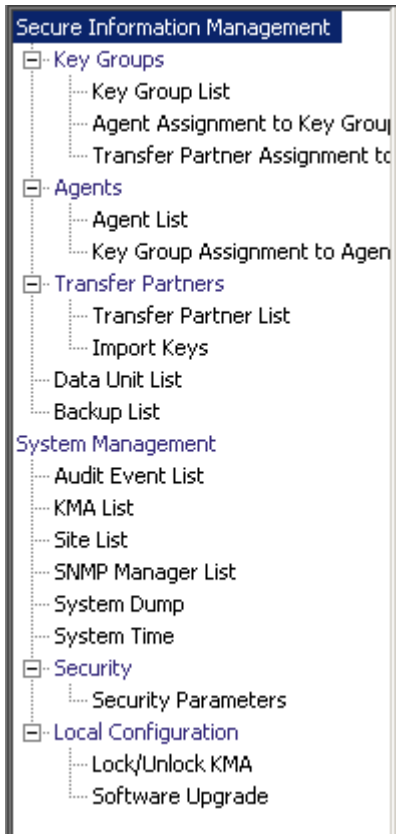
第7章

オペレータの操作

この章では、オペレータロールが付与されたユーザーが実行できる操作について説明します。複数のロールが割り当てられている場合は、そのロールを実行する手順について、該当する章を参照してください。

オペレータロール

オペレータは、システムの日常業務を管理します。



「Key Groups」メニュー

「Key Groups」メニューには、次のメニューオプションがあります。

このメニューを使用すると、次の操作を行うことができます。

- 鍵グループのリストの表示
- 鍵グループへのエージェントの割り当ての表示
- 鍵グループへの転送パートナーの割り当ての表示

Key Group List

「Key Group List」メニューオプションを使用すると、ユーザーは鍵グループを管理できます。手順については、179 ページの「「Key Group List」メニュー」を参照してください。

Agent Assignment to Key Groups

「Agent Assignment to Key Groups」メニューオプションを使用すると、ユーザーは、鍵グループに割り当てられているエージェントを表示できます。手順については、187 ページの「「Agent Assignment to Key Groups」メニュー」を参照してください。

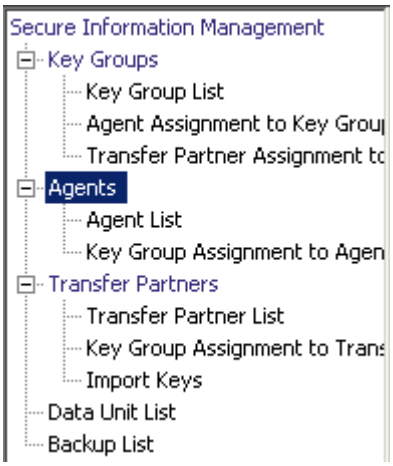
Transfer Partner Assignment to Key Groups

「Transfer Partner Assignment to Key Groups」オプションを使用すると、ユーザーは、特定の鍵グループへのアクセスを許可されている一連の鍵転送パートナーを表示できます。手順については、204 ページの「「Transfer Partner Assignment to Key Groups」メニュー」を参照してください。

「Agent List」メニュー

「Agent List」メニューオプションを使用すると、次の操作を行うことができます。

- エージェントの表示
- エージェントの作成
- エージェントの表示および変更
- 既存のエージェントの削除

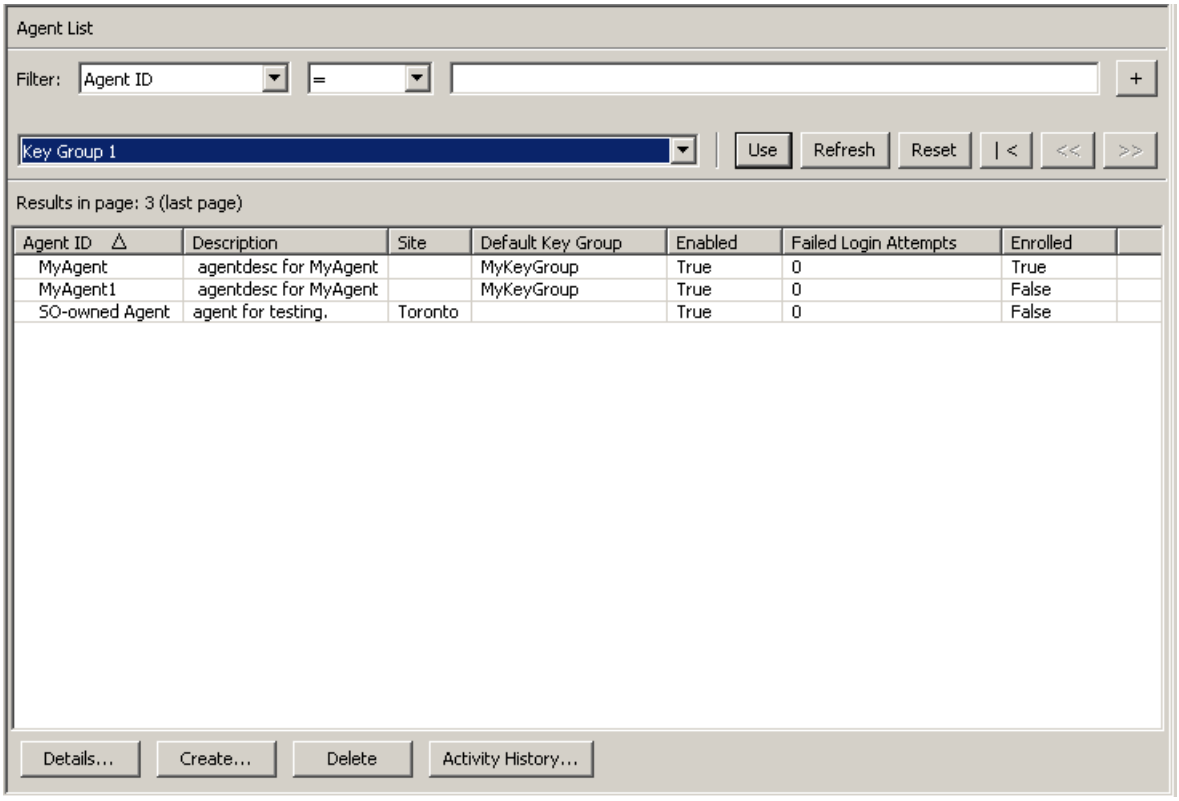


エージェントリストの表示

「Agent List」メニューオプションを使用すると、ユーザーは、特定の鍵グループに関連付けられているすべてのエージェントを表示できます。

この画面を表示するには、次の手順を実行します。

1. 「Agents」メニューから、「Agent List」を選択します。「Agent List」画面が表示されます。
2. 鍵グループのフィールドの横にある下矢印ボタンをクリックし、鍵グループを選択します。鍵グループに関連付けられているエージェントが表示されます。



リスト全体をスクロールするか、次のいずれかのキーでエージェントにフィルタを適用することもできます。

- Agent ID
- Description
- Site
- Default Key Group
- Enabled
- Failed Login Attempts
- Enrolled

表示されているエージェントリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Agent ID
- Description
- Site
- Default Key Group
- Enabled
- Failed Login Attempts
- Enrolled

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス:

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス:

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

Show Agents in any Key Group:

提供されているフィルタで、鍵グループへの関連付けによってエージェントにフィルタを適用できます。選択した鍵グループに関連付けられているエージェントのみが表示されます。下矢印ボタンをクリックし、フィルタ条件として使用する鍵グループを選択します。

Use:

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Agent ID

各エージェントを識別するユーザー指定の一意の識別子が表示されます。

Description

エージェントの説明が示されます。

Site

エージェントが属しているサイトを示す一意の識別子が表示されます。

Default Key Group

エージェントで別の鍵グループが明示的に指定されていない場合に、このエージェントによって作成されたすべての鍵に関連付けられる鍵グループ。

Enabled

エージェントの状態を示します。True または False の値を取ります。このフィールドが False の場合、エージェントは KMA とのセッションを確立できません。

Failed Login Attempts

ログオンに失敗した回数が表示されます。

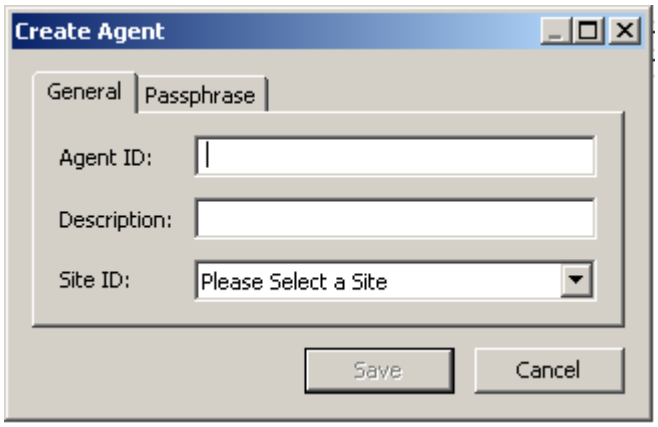
Enrolled

エージェントが KMS クラスタに正常に登録されたかどうかが示されます。True または False の値を取ります。エージェントがはじめて作成されたか、またはエージェントのパスフレーズが変更された場合、このフィールドは False になります。

エージェントの作成

エージェントを作成するには、次の手順を実行します。

1. 「Agents List」画面で、「Create」ボタンを選択します。「Create Agent」画面が開き、「General」タブが表示されます。



2. 次のパラメータを設定します。

Agent ID

エージェントを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

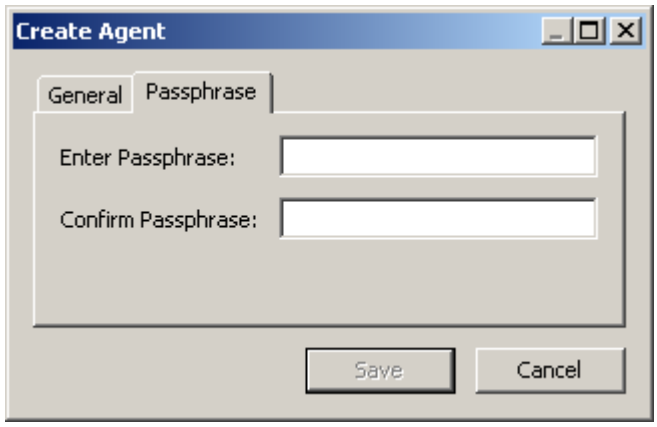
Description

エージェントを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Site ID

下矢印ボタンをクリックし、エージェントが属するサイトを強調表示します。このフィールドは省略可能です。

3. 「Passphrase」タブを開きます。



4. 次のパラメータを設定します。

Enter Passphrase

このユーザーのパスフレーズを入力します。最小文字数は 8 文字、最大文字数は 64 文字です。デフォルト値は 8 です。

パスフレーズの要件は、次のとおりです。

- パスフレーズに、ユーザーのエージェント ID を含めないでください。
- パスフレーズには、大文字、小文字、数値、または特殊文字の 4 つの文字クラスのうち 3 つを使用する必要があります。

  使用可能な特殊文字は、次のとおりです。

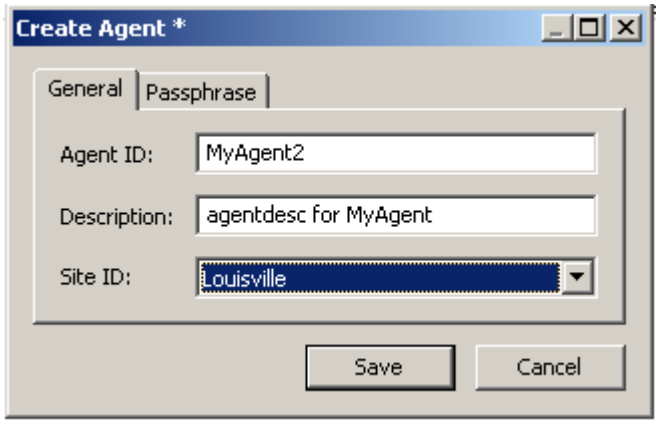
  ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ ” < > , . / ?
- タブ、改行などの制御文字は使用できません。

注 – パスフレーズの最小文字数の要件を変更する方法については、148 ページの「セキュリティーパラメータの変更」を参照してください。

Confirm Passphrase

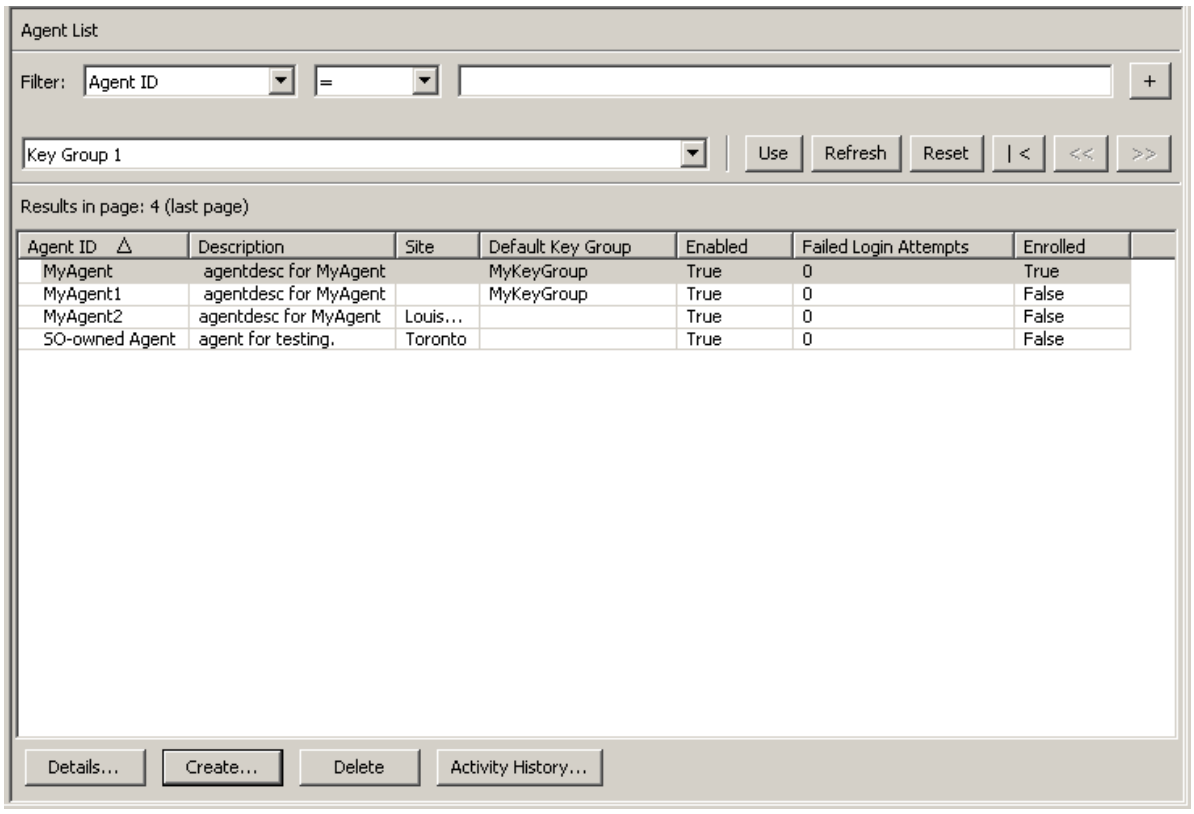
「Enter Passphrase」フィールドに入力した値と同じ値を入力します。

次に、値を入力した「Create Agent」画面の例を示します。



5. 「Save」ボタンを選択します。エージェントレコードがデータベースに追加され、「Agent List」画面に表示されます。

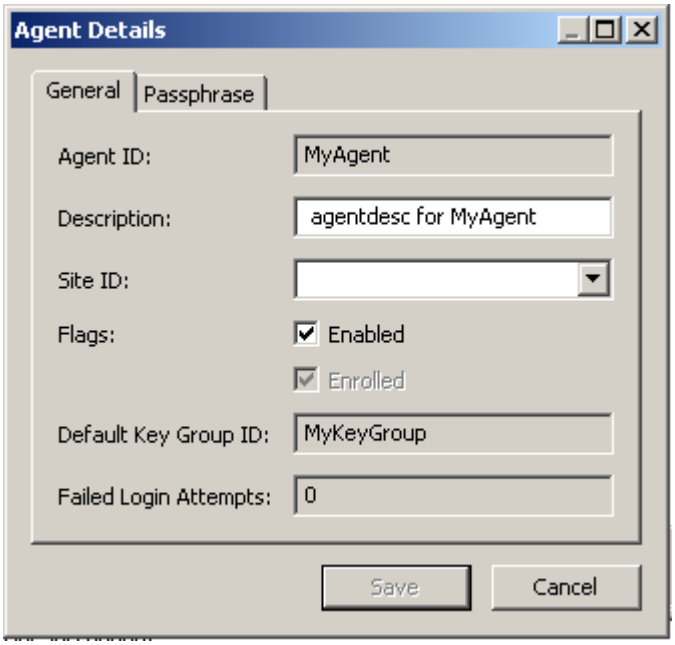
6. エージェント固有のインタフェースを使用して、エージェント固有の登録手順を完了します。たとえば、Sun のドライブの場合、登録手順を完了するには VOP (Virtual Operator Panel) を使用する必要があります。


Agent List
Filter:
Agent ID
=
+
Key Group 1
Use
Refresh
Reset
| <
<<
>>
Results in page: 4 (last page)
Agent ID △
Description
Site
Default Key Group
Enabled
Failed Login Attempts
Enrolled
MyAgent
agentdesc for MyAgent
MyKeyGroup
True
0
True
MyAgent1
agentdesc for MyAgent
MyKeyGroup
True
0
False
MyAgent2
agentdesc for MyAgent
Louis...
True
0
False
SO-owned Agent
agent for testing.
Toronto
True
0
False
Details...
Create...
Delete
Activity History...

エージェントの表示および変更

エージェントの詳細を変更するには、次の手順を実行します。

1. 「Agents List」画面で、詳細情報を表示するエージェントエントリをダブルクリックするか、またはエージェントエントリを強調表示して「Details」ボタンを選択します。「Agents Details」画面が表示されます。



2. 「General」タブを開き、必要に応じて次のフィールドを変更します。

- Description
- Site ID
- Flags - Enabled

注 – エージェントのパスフレーズは、パスフレーズが危殆化されていることが確かな場合にのみ変更してください。手順については、227 ページの「エージェントのパスフレーズの設定」を参照してください。

---

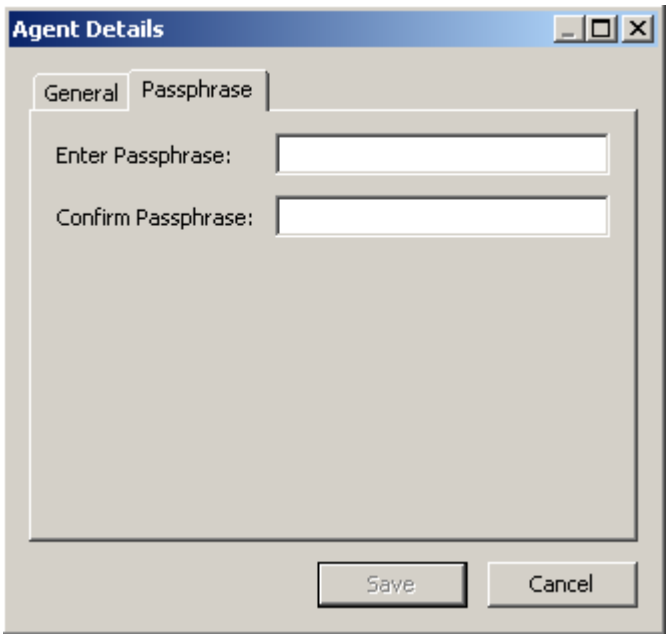
3. 終了したら、「Save」ボタンを選択します。KMS Manager データベースが変更され、「Agents List」画面に戻ります。

エージェントのパスフレーズの設定

エージェントのパスフレーズを設定すると、エージェントが KMA で認証を受けるためのエージェント証明書を失効させることができます。エージェント証明書またはパスフレーズ、あるいはその両方が危殆化されていると思われる場合、オペレータは、エージェントのパスフレーズ証明書を設定できます。

エージェントのパスフレーズを設定するには、次の手順を実行します。

1. 「Agents List」画面で、パスフレーズを設定するエージェントエントリをダブルクリックするか、またはエージェントエントリを強調表示して「Details」ボタンを選択します。「Agent Details」画面が表示されます。「Passphrase」タブを開きます。

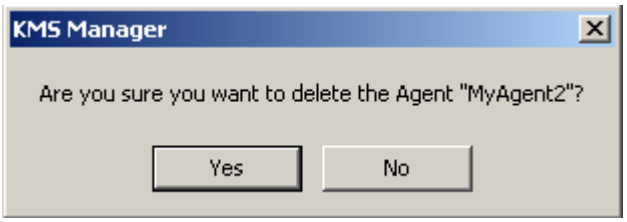


2. 次のフィールドを変更し、「Save」ボタンを選択します。
   - Enter Passphrase
   - Confirm Passphrase
3. データベースが変更され、「Agents List」画面に戻ります。
4. エージェント固有の手順で、エージェントを再登録します。たとえば、Sun のテープドライブの場合、エージェントを KMS Cluster に再登録するには VOP (Virtual Operator Panel) を使用する必要があります。エージェントのパスフレーズを変更したあと、エージェントを再登録するまでは、KMS クラスタに要求を送信できません。

エージェントの削除

エージェントを削除するには、次の手順を実行します。

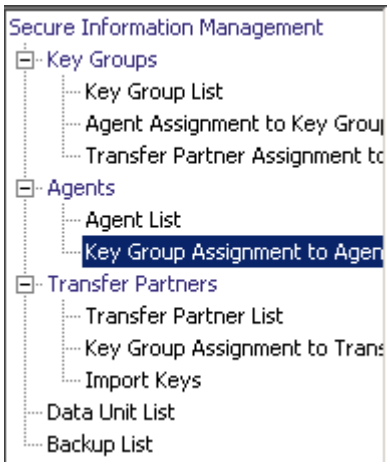
1. 「Agents List」画面で、削除するエージェントを強調表示します。次のように、選択したエージェントの削除を確認するダイアログボックスが表示されます。



2. 「Yes」ボタンを選択して、エージェントを削除します。エージェントがデータベースから削除され、「Agents List」画面に戻ります。削除したエージェントは表示されなくなります。

「Key Group Assignment to Agents」メニュー

「Key Group Assignment to Agents」メニューオプションを使用すると、エージェントに割り当てられている鍵グループを表示できます。手順については、193 ページの「「Key Group Assignment to Agents」メニュー」を参照してください。



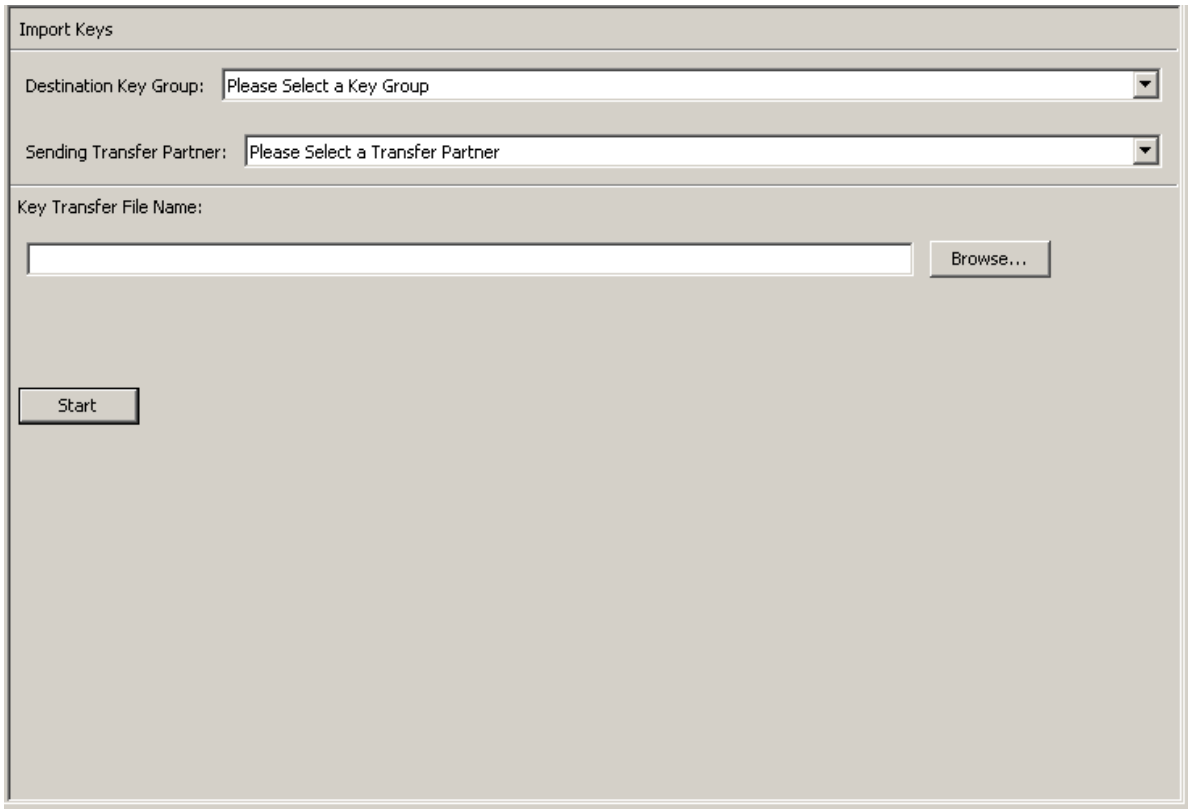
「Import Keys」メニュー

このメニューオプションを使用すると、鍵およびデータユニットを KMS クラスタにインポートできます。鍵およびデータユニットの情報は、鍵転送パートナーから受け取った鍵転送ファイルに含まれています。

注 – KMS クラスタに鍵をアップロードしてインポートするには、この画面を使用します。これらの鍵は、別の KMS クラスタからエクスポートされたものです。

鍵をインポートするには、次の手順を実行します。

1. 「Transfer Partners」メニューから、「Import Keys」を選択します。「Import Keys」画面が表示されます。



2. 次のパラメータを設定します。

Destination Key Group:

これらの鍵のインポート先となる鍵グループを選択します。

この鍵グループの鍵ポリシーの「Allow Imports」フラグがオンになっている必要があります。この鍵グループは、選択した送信側転送パートナーに対して許可された鍵グループである必要があります。

Sending Transfer Partner:

これらの鍵をエクスポートした送信側転送パートナーを選択します。

Key Transfer File:

鍵転送ファイルの名前を入力します。また、「Browse」をクリックして出力先のパスを選択することもできます。

3. 「Start」ボタンをクリックして、アップロードと鍵のインポートの処理を開始します。ファイルがアップロードされて適用されたことを示すメッセージが表示されます。

データユニット

データユニットは、ディスク、テープ、オブジェクトなどの論理ストレージデバイスです。データユニットは、鍵グループに関連付けられている有効な鍵ポリシーによってセキュリティー保護されます。エージェントは、選択したデータユニットにアクセス可能である必要があります。

注 – オペレータは、データユニットの鍵グループの変更を除くすべての機能を実行できます。データユニットの鍵グループを変更できるのは、コンプライアンス責任者のみです。

「Data Unit List」メニュー

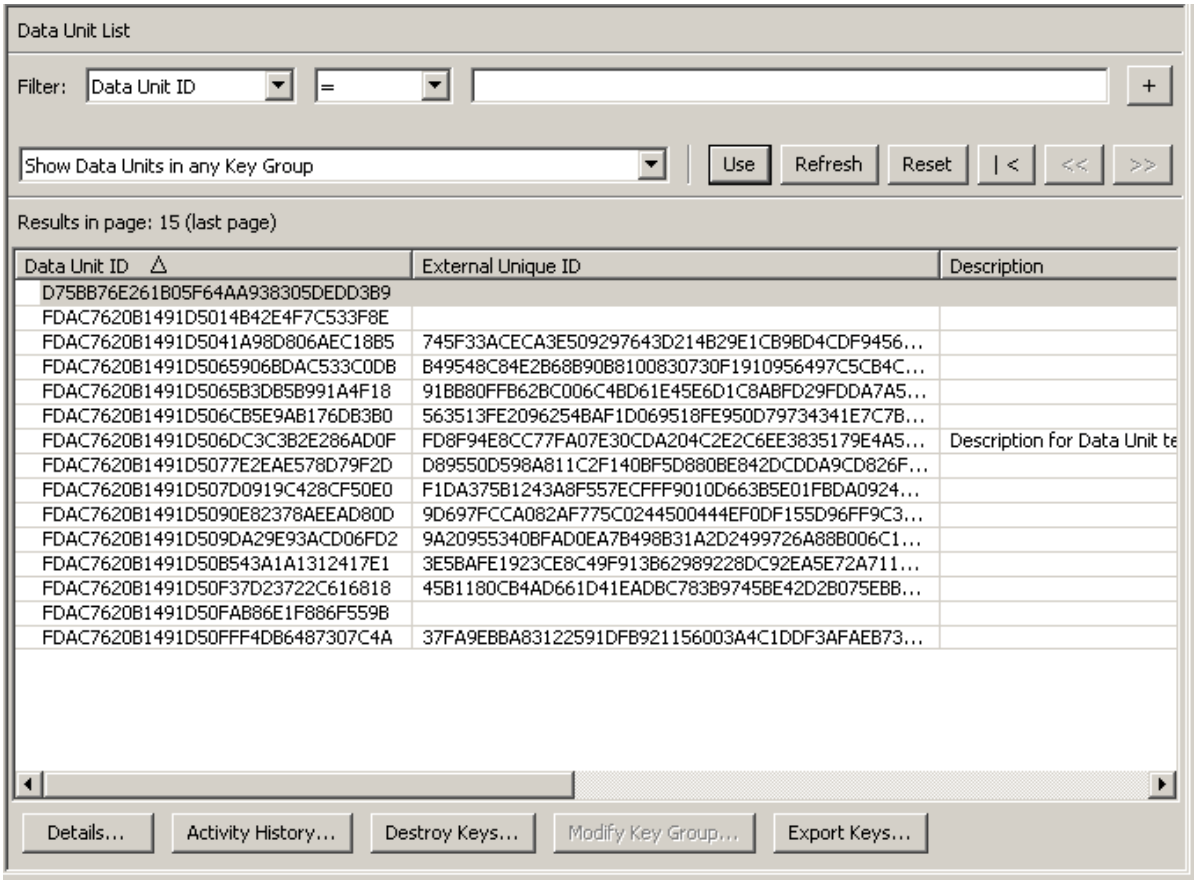
「Data Unit List」メニューには、次のメニューオプションがあります。

このメニューを使用すると、次の操作を行うことができます。

- データユニットの表示
- データユニットの詳細の表示および変更
- データユニットの活動履歴の表示
- データユニットの運用後鍵の破棄

データユニットの表示

データユニットを表示するには、「Data Units」メニューから「Data Unit List」を選択します。「Data Unit List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでデータユニットリストにフィルタを適用することもできます。

- Data Unit ID
- External Unique ID
- Description
- External Tag
- Created Date
- Imported
- Exported
- State

表示されているデータユニットリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

Filter:

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。次に示す値を取ります。

- Data Unit ID
- External Unique ID
- Description
- External Tag
- Created Date
- Imported
- Exported
- State

フィルタ演算子ボックス:

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。次に示す値を取ります。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

Show Data Units in Any Key Group. Use:

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

Refresh:

このボタンをクリックすると、リストが再表示されます。

Reset:

このボタンをクリックすると、すべてのフィルタが削除され、最初のページに戻ってリストが表示されます。

このボタンをクリックすると、リストの最初のページが表示されます。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Data Unit ID

各データユニットを識別する一意のシステム生成識別子が表示されます。

External Unique ID

データユニットの一意の外部識別子が表示されます。

この値は、エージェントによって KMS に送信されるため、外部のエンドユーザーには見えないことがあります。LTO-4 テープの場合、この値は、製造時にカートリッジに焼き付けられたカートリッジのシリアル番号です。この値を、光学式バーコードや ANSI テープラベルのボリュームシリアル番号 (VOLSER) と混同しないでください。この値は、Sun のテープドライブでは使用されません。

Description

データユニットの説明が示されます。

External Tag

データユニットの一意の外部タグの説明が示されます。

Sun のテープライブラリ内のテープ、または ANSI 標準ラベルの付いたテープの場合、このフィールドは VOLSER になります。ライブラリ内のテープに ANSI ラベルが付いており、ライブラリの VOLSER (光学式バーコード) が ANSI ラベルの VOLSER と異なる場合は、ライブラリの VOLSER が使用されます。ANSI ラベルを付けずにスタンドアロンドライブで書き込まれたテープの場合、このフィールドは空白になります。

Created Date

データユニットが作成または登録された日時を示します。

Imported

データユニットがインポートされたかどうかが示されます。

Exported

データユニットがエクスポートされたかどうかが示されます。

State

データユニットの状態を示します。次に示す値を取ります。

- No Key: データユニットは作成されたが、まだ鍵が作成されていない場合は、この値に設定されます。
- Readable: データユニットの少なくとも一部分を復号化 (読み取り) できる鍵がデータユニット内に存在する場合は、この値に設定されます。
- Normal: データユニットの少なくとも一部分を復号化 (読み取り) できる鍵がデータユニット内に存在する場合は、この値に設定されます。さらに、データの暗号化に使用できる「Protect-and-Process」状態の鍵が、データユニット内に 1 つ以上存在します。したがって、データユニットは書き込み可能になります。
- Needs ReKey: データユニットの少なくとも一部分を復号化 (読み取り) できる鍵がデータユニット内に存在する場合は、この値に設定されます。ただし、「Protect-and-Process」状態の鍵は、データユニット内に 1 つもありません。

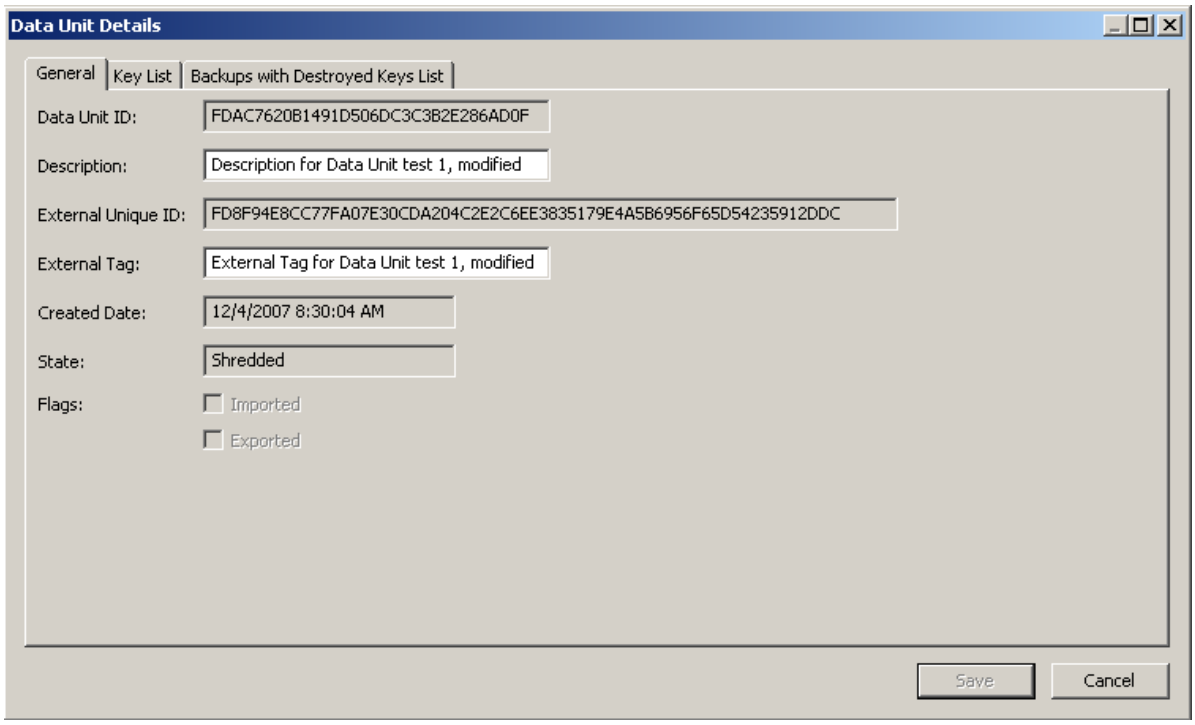
  データがこのテープに書き込まれると、新しい「Protect-and-Process」状態の鍵がデータユニットに自動的に付与されます。
- Shredded: このデータユニットのすべての鍵が破棄された場合は、この値に設定されます。データユニットの読み取りまたは書き込みを行うことはできません。ただし、このデータユニットに対して新しい鍵を作成することができ、作成するとデータユニットの状態は「Normal」に戻ります。

データユニットの詳細の表示および変更

注 – オペレータ以外のユーザーがデータユニットの詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。コンプライアンス責任者に対しては、「Key Group」フィールドが使用可能になります。

データユニットの情報を変更するには、次の手順を実行します。

1. 「Data Unit List」画面で、変更するデータユニットを選択して「Details」ボタンを選択します。「Data Unit Details」画面が表示されます。



2. 次のパラメータを変更できます。

Description

新しい値を入力します。元の情報は、登録時にソフトウェア暗号化ドライバによって提供されたものです。この値は 1 ～ 64 文字、または空白で指定できます。

External Tag

データユニットの一意の外部識別子を入力します。この値は 1 ～ 64 文字、または空白で指定できます。このフィールドには、通常、テープカートリッジのラベルまたはバーコードが表示されます。

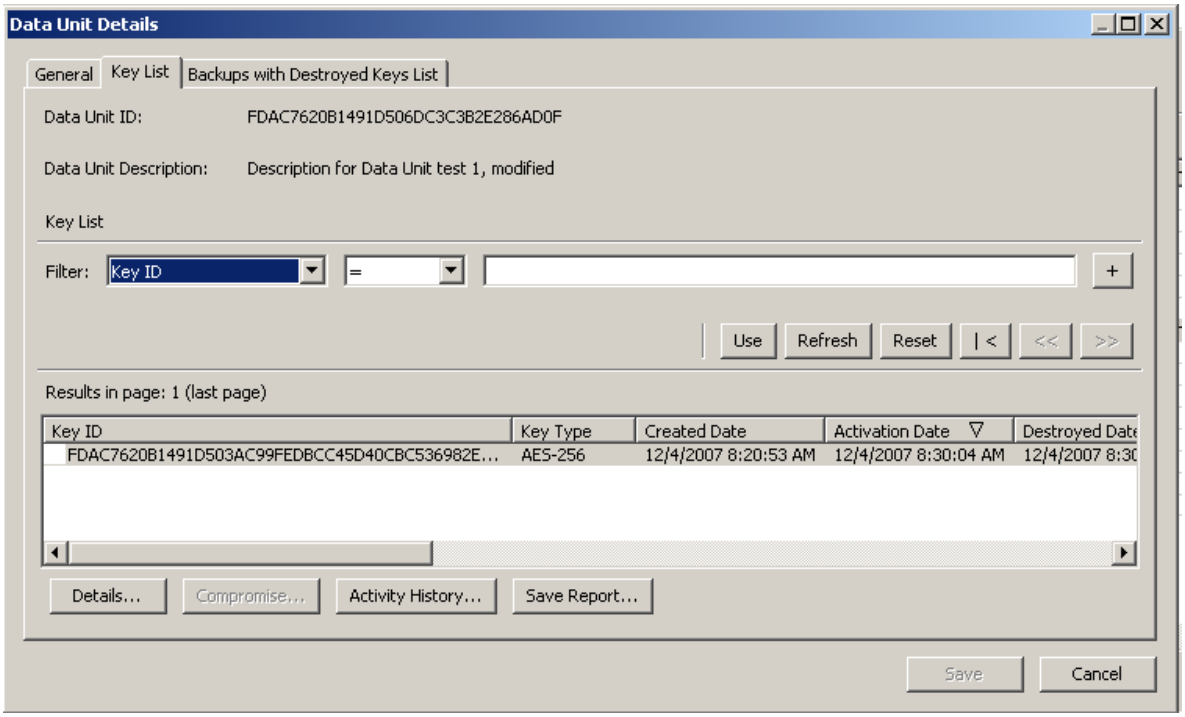
3. 「Save」ボタンを選択して、変更内容を保存します。

次のフィールドは編集できません。

「General」タブ

- Data Unit ID
- External Unique ID
- Created Date
- State
- Flags Imported/Exported

「Key List」タブ



Data Unit ID

データユニットを一意に識別します。

Data Unit Description

データユニットの説明が示されます。

Key ID

データユニットの鍵情報が表示されます。

Key Type

この鍵が使用する暗号化アルゴリズムのタイプを示します。値は AES-256 になります。

Created Date

鍵が作成された日時が表示されます。

Activation Date

鍵が有効になった日時が表示されます。これは、鍵が最初にエージェントに付与された日時です。また、鍵の暗号化期間および暗号有効期間の開始日時でもあります。

Destroyed Date

鍵が破棄された日付が表示されます。このフィールドが空白である場合、鍵は破棄されていません。

Destruction Comment

鍵の破棄に関するユーザーが指定した情報が表示されます。このフィールドが空白である場合、鍵は破棄されていません。

Imported

データユニットがインポートされたかどうかが示されます。

Exported

データユニットがエクスポートされたかどうかが示されます。

Key Group

データユニットに関連付けられた鍵グループが表示されます。

Encryption End Date

鍵が使用されなくなった日時、またはデータの暗号化に使用されなくなった日時が表示されます。

Deactivation Date

鍵が無効になる日時、または無効になった日時が表示されます。

Compromised Date

鍵が危殆化された日付が表示されます。このフィールドが空白である場合、鍵は危殆化されていません。

Compromised Comment

鍵の危殆化に関するユーザーが指定した情報が表示されます。このフィールドが空白である場合、鍵は危殆化されていません。

Key State

データユニットの鍵の状態を示します。次に示す値を取ります。

Generated

鍵が KMS クラスタ内の 1 つの KMA に対して作成されている場合は、この値に設定されます。複数の KMA で構成されるクラスタ内の、別の 1 つ以上の KMS に複製されるまで、鍵は「Generated」状態のままになります。単一の KMA のみで構成されるクラスタでは、少なくとも 1 つのバックアップに記録されるまで、鍵は「Generated」状態のままになります。

Ready

複製またはバックアップによって鍵が損失しないように保護されている場合は、この値に設定されます。「Ready」状態の鍵は、割り当てに使用できます。

Protect and Process

暗号化エージェントが新しい鍵の作成を要求したときに、鍵がすでに割り当てられていると、この値に設定されます。この状態の鍵は、暗号化と復号化の両方に使用できます。

Process Only

鍵が割り当てられているが、鍵の暗号化期間を過ぎている場合には、この値に設定されます。この状態の鍵は、復号化には使用できますが、暗号化には使用できません。

Deactivated

鍵の暗号有効期間が過ぎているが、情報を処理 (復号化) するために鍵が必要となる可能性がある場合には、この値に設定されます。

Compromised

承認されていない実体に鍵が渡された場合、または承認されていない実体によって鍵が検出された場合には、この値に設定されます。この状態の鍵は、復号化には使用できますが、暗号化には使用できません。

Incompletely Destroyed

鍵が破棄されたが、1 つ以上のバックアップ内にまだ存在している場合には、この値に設定されます。

Completely Destroyed

破棄された鍵が存在していたすべてのバックアップが破棄された場合には、この値に設定されます。

Compromised and Incompletely Destroyed

危殆化された鍵が 1 つ以上のバックアップ内にまだ存在している場合には、この値に設定されます。

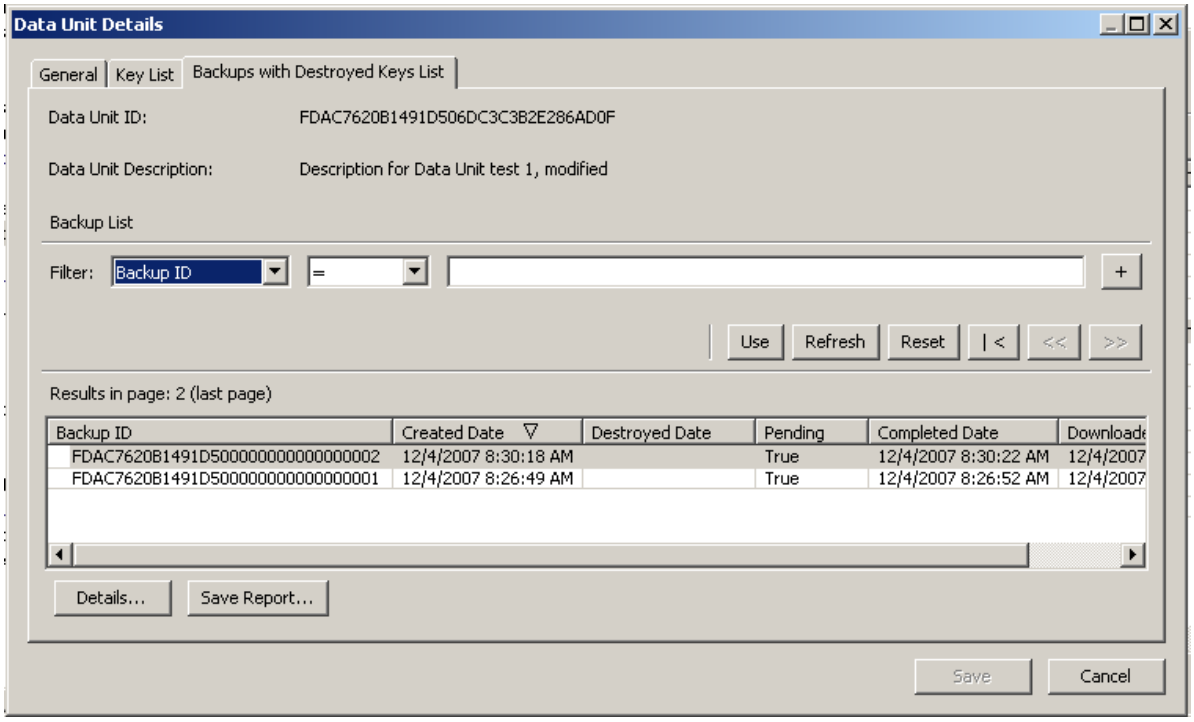
Compromised and Completely Destroyed

危殆化された鍵が存在していたすべてのバックアップが破棄された場合には、この値に設定されます。

Recovery Activated

復旧操作によって鍵がデータユニットにリンクされたかどうかを示します。この状況は、KMS クラスタ内の 1 つの KMA で鍵がデータユニットに対して使用されたあと、障害が発生したために、その鍵が別の KMA から同じデータユニットに対して要求された場合に発生します。ネットワーク機能停止などの障害などによって、データへの鍵の割り当てを 2 番めの KMA に伝播できなかった場合には、2 番めの KMA によってそのデータユニットへのリンクが作成されます。このような鍵は「Recovery Activated」状態になり、管理者が、システムで KMA またはネットワークの機能停止が発生しているかどうかを評価することになります。True または False の値を取ります。

「Backups with Destroyed Keys List」タブ



データユニットは、データユニット鍵が含まれるすべてのバックアップが破棄されるまで、「Completely Destroyed」とは見なされません。

「Data Unit Details」ダイアログの「Backups with Destroyed Keys List」タブは、選択したデータユニットのデータユニット鍵が含まれるバックアップと、それらのバックアップの破棄の状態を特定するために役立ちます。

バックアップに特定のデータユニット鍵が含まれているかどうかは、次のように判断します。

データユニット鍵の作成後にバックアップが作成され、**かつ**データユニット鍵がまだ破棄されていない場合、またはデータユニット鍵が破棄され、**かつ**バックアップの作成後にその破棄が行われた場合、バックアップにはデータユニット鍵が含まれています。

ただし、日時を比較する場合は、クラスタ内のさまざまな KMA の時刻が自動的に同期化されていない (NTP サーバーが指定されていない) ため異なる時刻が報告される可能性を考慮する必要があります。KMA 間で時刻が違う可能性を考慮して、比較にはバックアップ時間枠が使用されます。バックアップ時間枠は、5 分間に固定されています。比較チェックは、バックアップ時間枠を使用して、次のように行われます。

バックアップ作成以降の 5 分以内にバックアップが作成され、**かつ**バックアップ作成以降の 5 分以内にデータユニット鍵が破棄されている場合、そのバックアップにはデータユニット鍵が含まれています。

バックアップ時間枠は、特定のバックアップ内のデータユニットが実際には存在しているのに、存在していないと誤って報告される可能性を最小限に抑えるために使用されます。このような状況は「偽陰性」と呼ばれ、これによりデータ破棄の適合性要件が非常に損なわれます。ただし、バックアップ時間枠を使用した場合には、バックアップ内の

データユニットが実際は存在していないのに、存在していると誤って報告される可能性が高くなります。「偽陰性」とは異なり、「偽陽性」はデータ破棄の適合性要件を損なうことがありません。

Data Unit ID

データユニットを一意に識別します。

Data Unit Description

データユニットの説明が示されます。

Data Unit Destruction Status

データユニットの破棄の状態を示します。

Backup ID

バックアップを識別します。

Created Date

バックアップファイルが作成された日時、つまりバックアップが開始された日時が表示されます。

Destroyed Date

バックアップファイルが破棄された日時が表示されます。

Pending:

バックアップがまだ保留中であることを示します。True または False の値を取ります。

Completed Date:

バックアップファイルの作成が完了した日時が表示されます。

Downloaded Date:

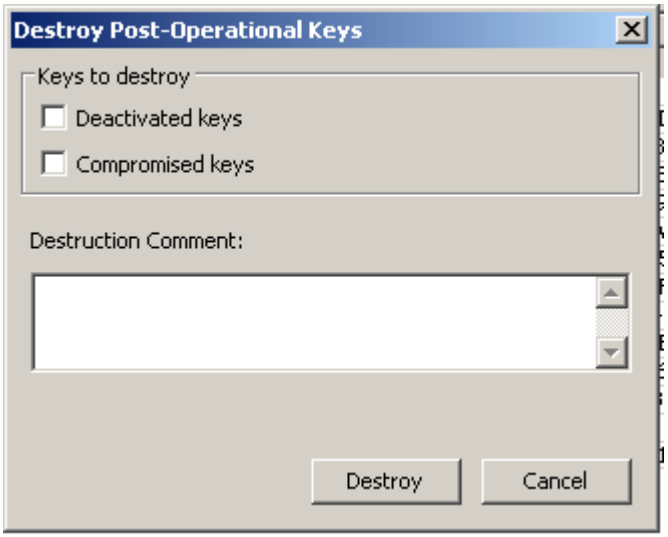
バックアップファイルがダウンロードされた日時が表示されます。

4. 「Save」ボタンを選択して、変更内容を保存します。

運用後鍵の破棄

データユニットに関連付けられている運用後鍵を破棄するには、次の手順を実行します。

1. 「Data Unit List」画面で、破棄するデータユニットを強調表示し、「Destroy Keys」ボタンを選択します。
2. 次のように、破棄する鍵の指定を求めるダイアログボックスが表示されます。



Deactivated keys

鍵の暗号有効期間が過ぎているが、情報を処理 (復号化) するために鍵が必要となる可能性がある場合には、このチェックボックスを選択します。

Compromised keys

承認されていない実体に鍵が渡された場合、または承認されていない実体によって鍵が検出された場合に鍵を破棄するには、このチェックボックスを選択します。

Destruction Comment

これらの鍵の破棄に関するコメントを入力します。

3. 「Destroy」ボタンを選択すると、これらの鍵の破棄を確認する別のダイアログボックスが表示されます。
4. 「Yes」ボタンを選択します。破棄した鍵の数を示す別のダイアログボックスが表示されます。

「Software Upgrade」メニュー

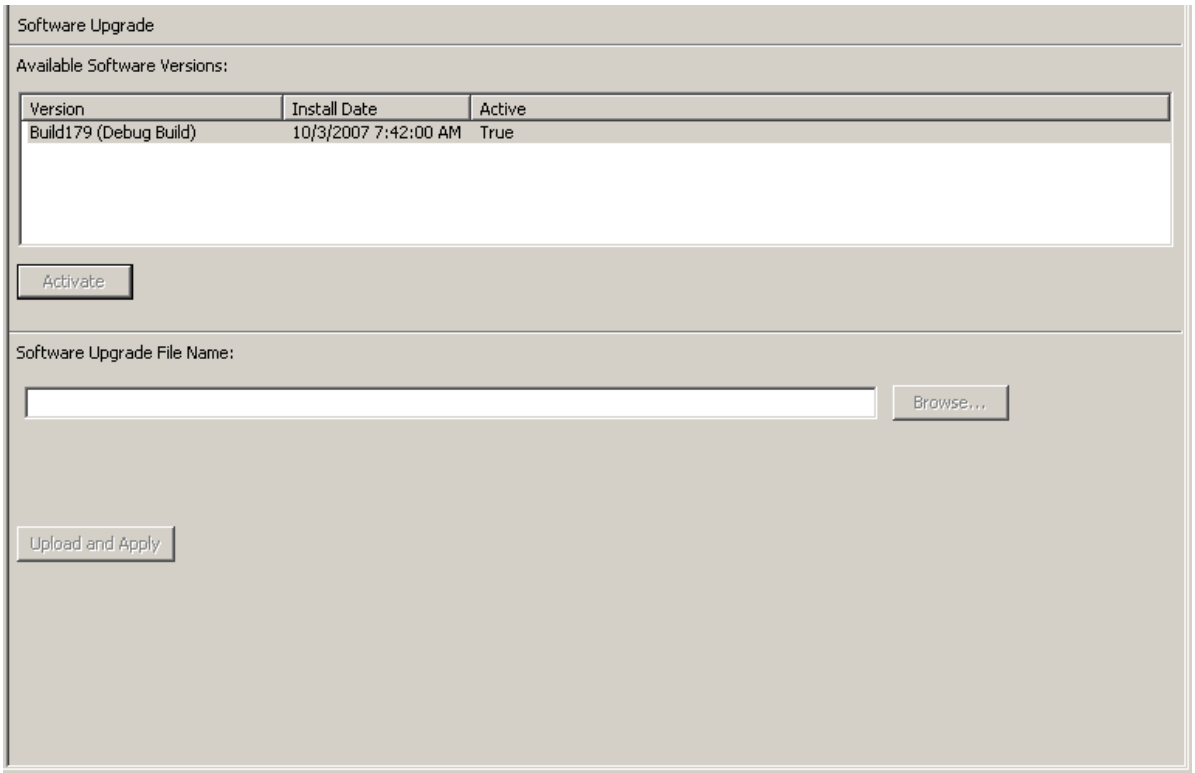
「Software Upgrade」メニューオプションを使用すると、オペレータは、ソフトウェアアップグレードファイルを KMA にアップロードし、ただちにアップグレードを適用できます。ソフトウェア更新は Sun によって署名されており、適用前に KMA によって確認されます。

注 – この機能を実行する前に、システムをバックアップする必要があります。手順については、251 ページの「バックアップの作成」を参照してください。

ソフトウェアアップグレードのアップロードおよび適用

KMA をアップグレードするには、次の手順を実行します。

1. 「Local Configuration」メニューから、「Software Upgrade」を選択します。
「Software Upgrade」画面が表示されます。



2. 「Software Upgrade File Name」フィールドに、ソフトウェアアップグレードファイルの名前を入力します。また、「Browse」ボタンを選択してファイルの場所を指定することもできます。「OK」ボタンを選択して、「Software Upgrade」画面に戻ります。「Upload and Apply」ボタンを選択します。
3. ファイルが正常にアップロードされたことを示すメッセージが表示されます。
4. アップグレードファイルを適用中であることを示すメッセージが表示されます。

5. アップグレードファイルを有効にするには、画面上部の使用可能なバージョンのリストから新しいバージョンを選択し、「Activate」ボタンをクリックします。有効にするまで、新しいバージョンは、システム上では無効な状態のままになります。

「Backup List」メニュー

バックアップファイルの詳細情報の表示手順については、247 ページの「「Backup List」メニュー」を参照してください。

「Audit Event List」メニュー

監査イベントリストの表示手順については、210 ページの「「Audit Event List」メニュー」を参照してください。

「KMA List」メニュー

KMA のリストの表示手順については、81 ページの「「KMA List」メニュー」を参照してください。

「Site List」メニュー

サイトのリストの表示手順については、103 ページの「「Site List」メニュー」を参照してください。

「SNMP Manager List」メニュー

SNMP Manager のリストの表示手順については、110 ページの「「SNMP Manager List」メニュー」を参照してください。

「System Time」メニュー

KMA の時刻を表示する手順については、164 ページの「「System Time」メニュー」を参照してください。

「Lock/Unlock KMA」メニュー

KMA のロック状態を表示する手順については、160 ページの「Lock/Unlock KMA」を参照してください。

第8章

バックアップオペレータの操作

この章では、バックアップオペレータロールを付与されたユーザーが実行できる操作について説明します。ほかのロールが割り当てられている場合は、そのロールの実行手順について、該当する章を参照してください。

バックアップオペレータロール

バックアップオペレータは、データおよびその鍵のセキュリティー保護および格納を担当します。

「Backup List」メニュー

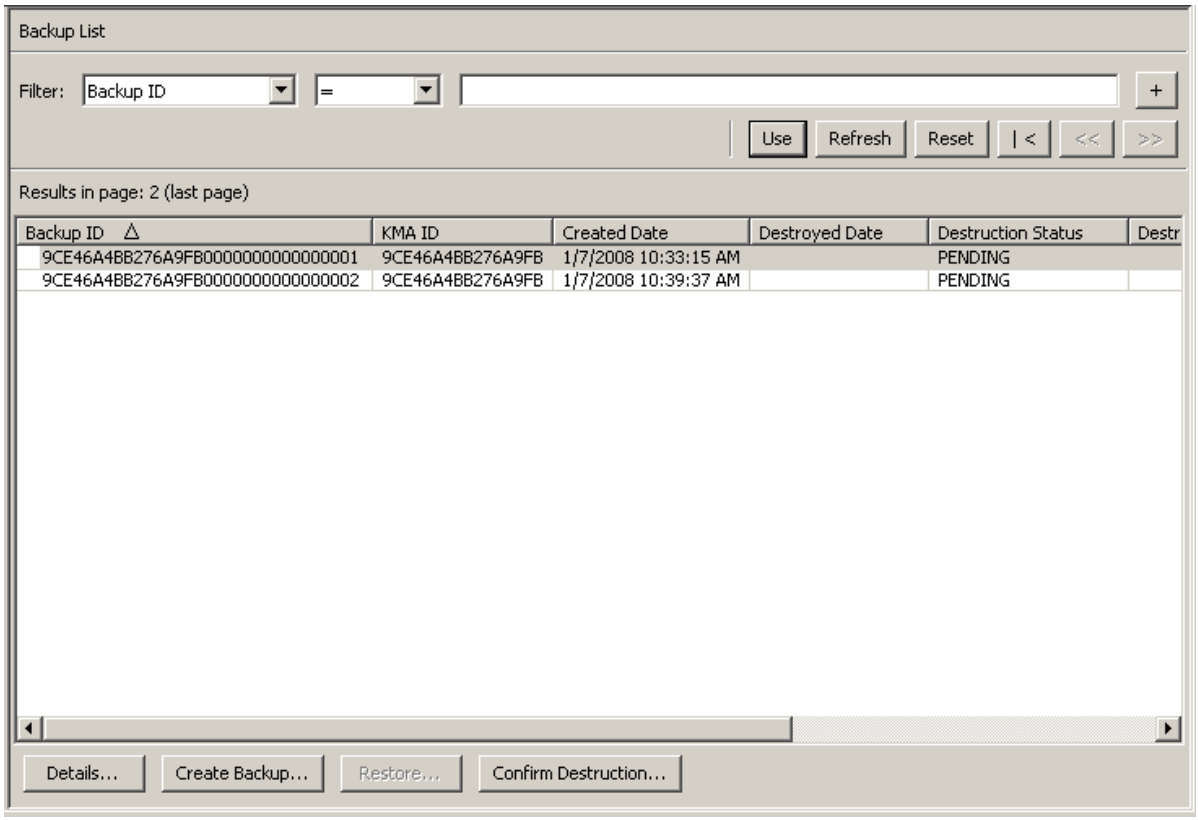
「Backups List」メニューオプションを使用すると、バックアップオペレータは次の操作を実行できます。

- バックアップ履歴の表示およびバックアップ破棄ステータスの確認
- バックアップの作成

バックアップファイルの履歴の表示

バックアップファイルの履歴を表示するには、次の手順に従います。

「Backups」メニューから「Backup List」を選択します。「Backup List」画面が表示されます。



バックアップの詳細情報を表示する場合は、バックアップを強調表示して「Details」ボタンを選択します。詳細は、249 ページの「バックアップの詳細の表示」を参照してください。

「Create Backup」ボタンを選択して、バックアップを作成します。詳細は、251 ページの「バックアップの作成」を参照してください。

「Confirm Destruction」ボタンを選択して、バックアップの破棄を確認します。詳細は、252 ページの「バックアップの破棄の確認」を参照してください。

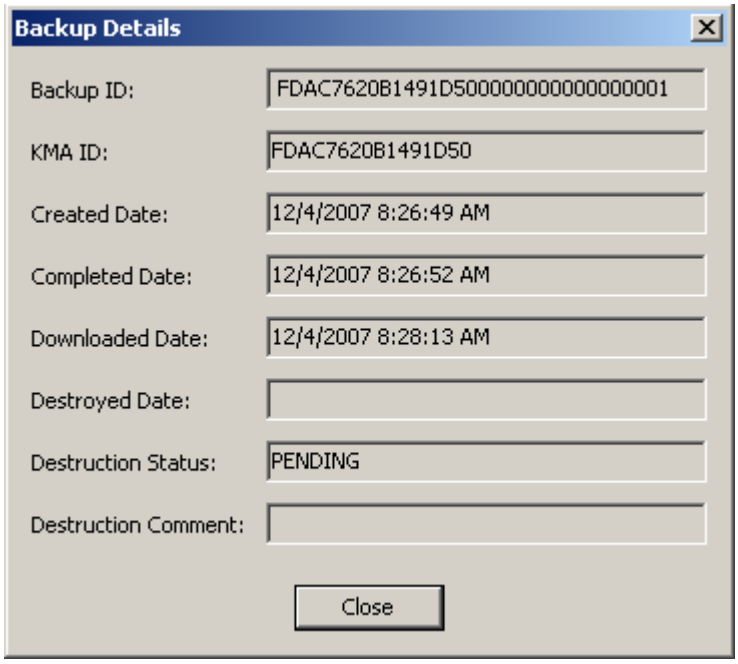
バックアップの詳細の表示

「Backup Details」ダイアログボックスは、バックアップファイルの詳細を表示する場合に使用します。

注 – バックアップを作成する場合、バックアップファイルは、KMS Manager が実行されているマシンにダウンロードされます。

バックアップファイルの詳細を表示するには、次の手順に従います。

1. 「Backups List」画面で、詳細情報を表示するバックアップエントリをダブルクリックするか、またはバックアップエントリを強調表示して「Details」ボタンを選択します。「Backup Details」ダイアログボックスが表示されます。すべてのフィールドが使用不可になっています。



2. 次に、フィールドとその説明を示します。

Backup ID

各バックアップファイルを識別する一意のシステム生成識別子が表示されます。

KMA ID

このバックアップファイルが生成された KMA が表示されます。

Created Date

バックアップファイルが作成された日時が表示されます。

Completed Date

バックアップファイルの作成が完了した日時が表示されます。

Downloaded Date

バックアップファイルがダウンロードされた日時が表示されます。

Destroyed Date

バックアップファイルが破棄された日付が表示されます。

Destruction Status

破棄に関するバックアップの状態が表示されます。

Destruction Comment

バックアップファイルの破棄に関するユーザー指定の情報が表示されます。

3. このダイアログボックスを閉じるには、「Close」ボタンを選択します。

バックアップの作成

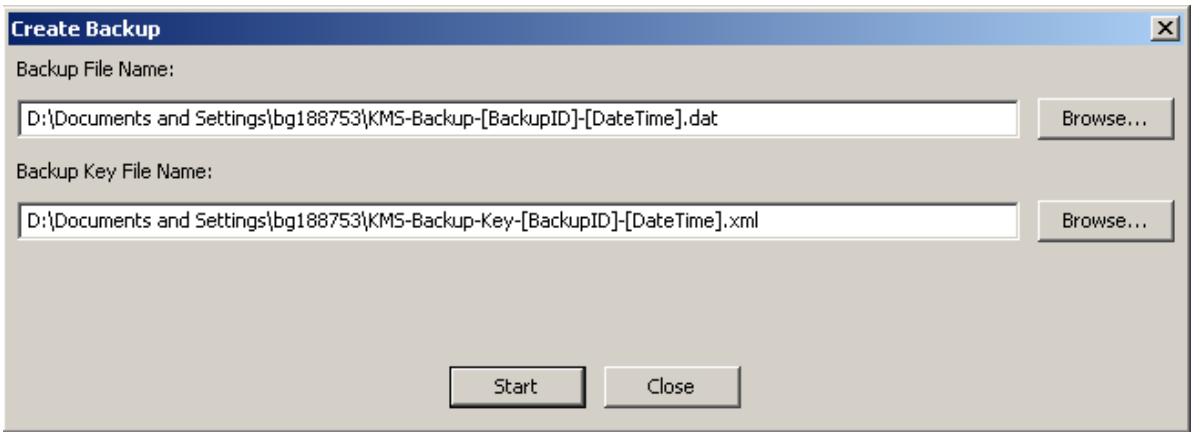
重要 – セキュリティー責任者がコアセキュリティー鍵データをバックアップしたあとでないと、バックアップ責任者はバックアップを作成できません。151 ページの「コアセキュリティーバックアップの作成」を参照してください。

常に、KMA には、バックアップファイルと復元ファイルがそれぞれ 1 つのみ存在します。

このオプションを使用すると、ユーザーは、バックアップファイルとバックアップ鍵ファイルの 2 つのファイルで構成されるバックアップを作成できます。

バックアップを作成するには、次の手順に従います。

1. 「Backup List」画面で、「Create Backup」ボタンを選択します。「Create Backup」ダイアログボックスが表示されます。



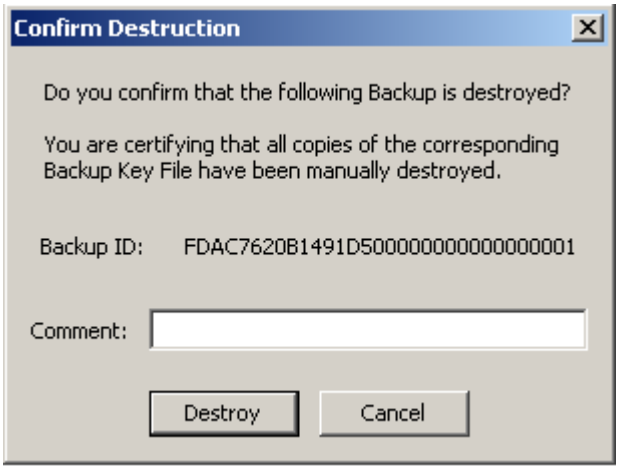
注 – バックアップファイルおよびバックアップ鍵ファイルの名前が自動的に生成されます。ただし、名前は編集できます。「Browse」ボタンを選択して宛先パスを選択することもできます。

2. 「Start」ボタンを選択してバックアップファイルを作成し、バックアップ鍵ファイルをユーザー指定の宛先にダウンロードします。
3. バックアップが完了すると、このことを示すメッセージが表示されます。このダイアログボックスを閉じるには、「Close」ボタンを選択します。
4. 「Backup List」画面が再度表示されます。新しく作成したバックアップファイルが表示されています。

バックアップの破棄の確認

バックアップの破棄を確認するには、次の手順に従います。

1. 「Backup List」画面で、破棄するバックアップを強調表示して「Confirm Destruction」ボタンを選択します。次のダイアログボックスが表示され、選択したバックアップの破棄ステータスの更新することが確認されます。処理を続行する前に、対応するバックアップ鍵ファイルのすべてのコピーが手動で破棄されていることを確認してください。



2. 対応するバックアップ鍵ファイルのすべてのコピーが手動で破棄されていることが確かな場合は、「Yes」ボタンを選択します。それ以外の場合は、「No」ボタンを選択して処理を中止します。

3. 「Yes」ボタンを選択した場合、バックアップおよび関連付けられているデータユニットが「完全に破棄」されます。

その他の機能

バックアップオペレータは、次の操作を行うことができます。

- 監査イベントリストの表示
- システム時刻の表示
- KMA のロックステータスの表示

監査ログの表示手順については、210 ページの「「Audit Event List」メニュー」を参照してください。

KMA の時刻を表示する手順については、164 ページの「「System Time」メニュー」を参照してください。

KMA のロック状態を表示する手順については、160 ページの「Lock/Unlock KMA」を参照してください。

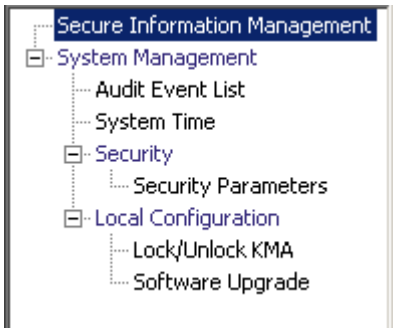
第 9 章

監査者の操作

この章では、監査者ロールを付与されたユーザーが実行できる操作について説明します。ほかのロールが割り当てられている場合は、そのロールの実行手順について、該当する章を参照してください。

監査者ロール

監査者は、「Audit List」イベントと KMA を表示できます。



「Audit List」メニュー

「Audit List」メニューの使用手順については、210 ページの「「Audit Event List」メニュー」を参照してください。

「Security Parameters」メニュー

「Security Parameters List」メニューを使用すると、監査者は、KMA のセキュリティーパラメータを表示できます。「Security Parameters」メニューの使用手順については、146 ページの「「Security Parameters」メニュー」を参照してください。

その他の機能

監査者は、次の操作を行うこともできます。

- KMA のロックおよびロック解除のステータスの表示
- システム時刻の表示

KMA のロックおよびロック解除のステータスの表示手順については、160 ページの「Lock/Unlock KMA」を参照してください。

KMA の時刻の調整手順については、164 ページの「「System Time」メニュー」を参照してください。

インストールされているソフトウェアのバージョンの表示手順については、244 ページの「「Software Upgrade」メニュー」を参照してください。

第 10 章

KMS コンソールの使用法

この章では、KMS コンソールのオプションについて説明します。

KMS コンソールの概要

KMS コンソールは端末テキストベースのインタフェースで、これを使用すると、ユーザーは KMA の基本的な機能を設定することができます。KMS コンソールには、ビデオモニターとキーボードを KMA に物理的に接続してアクセスするか、または ELOM の Web ブラウザインタフェース (20 ページの「Embedded Light Out Manager (ELOM) の起動」を参照) の「リモートコンソール」機能によってアクセスします。

KMA が起動し、ユーザーがこれを終了できなかった場合に、オペレーティングシステムによって KMS コンソールが自動的に起動されます。ユーザーに割り当てられたロールによって、KMS コンソールのオプションは異なります。

KMS コンソールにログインするには、KMS Manager でユーザーアカウントを作成する必要があります。ユーザーが KMS コンソールにログインするには、KMS での認証に使用されたものと同じユーザー名およびパスフレーズを使用する必要があります。

注 – QuickStart プログラムを起動すると、最初のセキュリティー責任者のアカウントだけが作成されます。

KMA へのログイン

KMA の起動後、次の情報が表示されます。

```
Sun Microsystems, Inc.
Key Management System Version xxx
------------------------------------------------------------
Please enter your User ID:
```

1. プロンプトで、ユーザー名を入力して Enter キーを押します。
2. 「`Please enter your Passphrase:`」プロンプトで、パスフレーズを入力して Enter キーを押します。ユーザーに割り当てられたロールによって、KMS コンソールのオプションは異なります。メニューには、KMA のバージョンおよびログオンしているユーザーが表示されます。

ユーザーのロールの操作については、以降のページで説明します。これには、次のロールが含まれます。

- オペレータ (262 ページの「オペレータロールの機能」を参照)
- セキュリティー責任者 (269 ページの「セキュリティー責任者ロールの機能」を参照)
- その他のロール (285 ページの「その他のロールの機能」を参照)

オペレータ

次のメニューには、オペレータロールに関するオプションが示されています。

```
Key Management System Version xxx (KMA1)
------------------------------------------------------------
Please enter your User ID: OP

Please enter your Passphrase:

Key Management System Version xxx (OP on KMA1)
------------------------------------------------------------

(1) Reboot KMA
(2) Shutdown KMA
(3) Technical Support
(4) Primary Administrator
(5) Set Keyboard Layout
(0) Logout
------------------------------------------------------------
Please enter your choice:
```

セキュリティー責任者

次のメニューには、セキュリティー責任者ロールに関するオプションが示されています。

```
Key Management System Version xxx (KMA1)
------------------------------------------------------------
Please enter your User ID: SO

Please enter your Passphrase:

Key Management System Version xxx (SO on KMA1)
------------------------------------------------------------

(1) Log KMA into Cluster
(2) Set User's Passphrase
(3) Set KMA IP Addresses
(4) Reset to Factory Default State
(5) Technical Support
(6) Primary Administrator
(7) Set Keyboard Layout
(0) Logout
------------------------------------------------------------
Please enter your choice:
```

注 – ユーザーにオペレータとセキュリティーの両方のロールが割り当てられている場合、メニューオプションは次のように組み合わせて表示されます。

```
Key Management System Version xxx (KMA1)
------------------------------------------------------------
Please enter your User ID:

Please enter your Passphrase:

Key Management System Version xxx (xx on KMA1)
------------------------------------------------------------

(1) Log KMA into Cluster
(2) Set User's Passphrase
(3) Set KMA IP Addresses
(4) Reset to Factory Default State
(5) Reboot KMA
(6) Shutdown KMA
(7) Technical Support
(8) Primary Administrator
(9) Set Keyboard Layout
(0) Logout
------------------------------------------------------------
Please enter your choice:
```

その他のロール

バックアップオペレータ、コンプライアンス責任者、監査者と、その他のすべてのロールでは、次のようなメニューが表示されます。使用可能なオプションは、KMA からのログアウトとキー配列の設定のみです。

```
Key Management System Version xxx (co1)
------------------------------------------------------------

(1) Set Keyboard Layout
(0) Logout

------------------------------------------------------------
Please enter your choice:
```

オペレータロールの機能

この節では、オペレータが実行できる機能について説明します。次の機能があります。

- KMA の再起動
- KMA の停止
- 技術サポートの有効化または無効化
- 主管理者の無効化
- キー配列の設定
- KMA からのログアウト

オペレータのメニューは次のとおりです。

```
Key Management System Version xxx (KMA1)
------------------------------------------------------------
Please enter your User ID: OP

Please enter your Passphrase:

Key Management System Version xxx (OP on KMA1)
------------------------------------------------------------

(1) Reboot KMA
(2) Shutdown KMA
(3) Technical Support
(4) Primary Administrator
(5) Set Keyboard Layout
(0) Logout
------------------------------------------------------------
Please enter your choice:
```

注 – 技術サポートおよび主管理者のメニュー項目は、それらの設定が現在有効になっている場合にのみ表示されます。

KMA の再起動

「Reboot KMA」メニューオプションを使用すると、オペレータが、KMA を停止および再起動して、オペレーティングシステムを再起動することができます。この機能は、障害追跡のみに使用します。

KMA を再起動するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、1 を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Reboot KMA
------------------------------------------------------------
Press Ctrl-c to abort.
Are you sure that you want to reboot the KMA? [y/n]:
```

2. プロンプトで、y を入力して Enter キーを押します。KMA の再起動が開始されると、現在の KMS コンソールセッションが終了します。KMA の再起動後、KMS コンソールのログインプロンプトが表示されます。

KMA の停止

このオプションを使用すると、KMA のすべてのサービスを終了 (停止) して、KMA 自体を物理的に停止することができます。

KMA を停止するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、2 を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Shutdown KMA
------------------------------------------------------------
Press Ctrl-c to abort
Are you sure that you want to shut down the KMA? [y/n]:
```

2. プロンプトで、y を入力して Enter キーを押します。次の情報が表示され、システムの停止中であることが示されます。

```
Shutting down...
```

3. 停止処理が表示されます。停止処理が完了すると、次の情報が表示されます。

```
Power down.
```

4. KMA の電源が切断されました。電源ボタンまたは ELOM の遠隔電源制御機能のいずれかを使用して、KMA の電源を入れることができます。

技術サポートアカウントの有効化

「Technical Support」メニューオプションを使用すると、オペレータはオペレーティングシステムのサポートアカウントとそのアカウントの SSH アクセスを有効または無効にすることができます。デフォルトでは、技術サポートアカウントおよび SSH アクセスはどちらも無効です。サポートアカウントのパスフレーズは Sun サポートのみが知っているため、このサポートアカウントを有効にすると、コンソールユーザーが KMA にこれ以上アクセスすることは許可されません。

1. 技術サポートアカウントを有効にするには、次の手順を実行します。

メインメニューの「Please enter your choice:」プロンプトで、3 を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが無効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently DISABLED.
************************ IMPORTANT ************************
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
************************************************************
Would you like to ENABLE this account? [y/n]:
```

2. プロンプトで、y と入力して、Enter キーを押します。次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to commit these changes? [y/n]:
```

3. プロンプトで、y を入力して Enter キーを押します。次の情報が表示され、アカウントが有効であることが示されます。Enter キーを押して、メインメニューに戻ります。

```
Press Enter to continue:
```

技術サポートアカウントの無効化

技術サポートアカウントを無効にするには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、3 を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently ENABLED.
************************* IMPORTANT *************************
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
*************************************************************
Would you like to DISABLE this account? [y/n]:
```

2. プロンプトで、y を入力して Enter キーを押し、アカウントを無効にします。
3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to commit these changes? [y/n]:
```

4. プロンプトで、y を入力して Enter キーを押します。SSH サービスは自動的に停止します。

主管理者の無効化

「Primary Administrator」メニューオプションを使用すると、KMA に対する主管理者のアクセスを有効または無効にすることができます。

注 – このタスクは、セキュリティー責任者のみが有効にすることができます。また、オペレータまたはセキュリティー責任者のどちらでも無効にすることができます。

主管理者のアクセスの無効化は即時に実行されます。別のユーザーが主管理者として接続している場合に、このアクセスを無効にすると、そのユーザーが次に実行しようとしたコマンドは失敗します。

1. 主管理者のアクセスを無効にするには、次の手順を実行します。

メインメニューの「`Please enter your choice:`」プロンプトで、**4** を入力して Enter キーを押します。次の情報が表示され、アクセスが有効であることが示されます。

```
Primary Administrator
-------------------------------------------------------------

Press Ctrl-c to abort.

The Primary Administrator role is currently ENABLED.

Would you like to DISABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to DISABLE these privileges for the
support account? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. プロンプトで、**y** を入力して Enter キーを押し、アカウントを無効にします。

3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. プロンプトで、**y** を入力して Enter キーを押します。主管理者のアクセスが無効になりました。

キー配列の設定

このオプションを使用すると、キー配列を英語から各種言語に変更できます。

注 – 押したキーを KMA が正しく解釈するために、キー配列の設定が KMA に接続されたキーボードの配列と一致するようにしてください。

キー配列を設定するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、**5** を入力して Enter キーを押します。次のようにキー配列が表示されます。

```
Set Keyboard Layout
------------------------------------------------------------

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian ( 2) Belarusian ( 3) Belgian
( 4) Bulgarian ( 5) Croatian ( 6) Danish
( 7) Dutch ( 8) Finnish ( 9) French
(10) German (11) Icelandic (12) Italian
(13) Japanese-type6 (14) Japanese (15) Korean
(16) Malta_UK (17) Malta_US (18) Norwegian
(19) Portuguese (20) Russian (21) Serbia-And-Montenegro
(22) Slovenian (23) Slovakian (24) Spanish
(25) Swedish (26) Swiss-French (27) Swiss-German
(28) Taiwanese (29) TurkishQ (30) TurkishF
(31) UK-English (32) US-English


The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. 「Please enter the number for the keyboard layout:」プロンプトで、キー配列を変更する番号を入力します。新しいキー配列が適用されます。

3. 次の情報が表示されます。

```
Press <Enter> to continue.
```

ログアウト

現在の KMS コンソールセッションからログアウトするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**0** を入力して Enter キーを押します。
2. 現在のセッションが終了して、ログインプロンプトが表示されます。ユーザーは、このログインプロンプトを使用して、KMS コンソールにふたたびログインできます。

セキュリティー責任者ロールの機能

この節では、セキュリティー責任者が実行できる機能について説明します。次の機能があります。

- KMA のクラスタへのログイン
- ユーザーのパスフレーズの設定
- KMA の IP アドレスの設定
- KMA の出荷時のデフォルト状態へのリセット
- 技術サポートの有効化または無効化
- 主管理者の有効化または無効化
- キー配列の設定
- KMA からのログアウト

セキュリティー責任者のメニューは次のとおりです。

```
Key Management System Version xxx (KMA1)
------------------------------------------------------------
Please enter your User ID: SO

Please enter your Passphrase:

Key Management System Version xxx (SO on KMA1)
------------------------------------------------------------

(1) Log KMA into Cluster
(2) Set User's Passphrase
(3) Set KMA IP Addresses
(4) Reset to Factory Default State
(5) Technical Support
(6) Primary Administrator
(7) Set Keyboard Layout
(0) Logout
------------------------------------------------------------
Please enter your choice:
```

KMA のクラスタへのログイン

このメニューオプションを使用すると、セキュリティー責任者は、パスフレーズの変更後、KMA からクラスタにログインし直すことができます。このタスクを実行するには、その前に次の処理を行う必要があります。

1. KMS Manager を起動します。
2. 既存の KMA にセキュリティー責任者としてログインします。
3. 「KMA List」パネルに移動します。
4. KMA エントリを作成します。

KMA からクラスタにログインするには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、1 を入力して Enter キーを押します。次の情報が表示されます。

```
Log KMA into Cluster
------------------------------------------------------------
Press Ctrl-c to abort.
Please enter the Management Network IP Address of an existing
KMA in the cluster:

The KMA Passphrase is a Passphrase that you have
previously configured for this KMA to join a Cluster.

Please enter this KMA's Passphrase:
```

2. 既存の KMA (たとえば、129.80.60.172) にセキュリティー責任者としてログインします。
3. プロンプトで、KMA 用に最初に設定したパスフレーズを入力して Enter キーを押し、クラスタにログインします。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #1:

Please enter Key Split Passphrase #1:

Press Enter to continue:
```

4. KMS Manager の鍵分割資格変更機能で、はじめての KMA の QuickStart 中に設定した最初の鍵分割ユーザー名を入力します (155 ページの「鍵分割設定の変更」を参照)。

注 – セキュリティー責任者は、入力する鍵分割ユーザーの数、つまり鍵分割しきい値が何であるかを知っている必要があります。この例では、鍵分割しきい値は 2 です。

5. 鍵分割ユーザー用のパスフレーズを入力して、Enter キーを押します。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #2:

Please enter Key Split Passphrase #2:

Press Enter to continue:
```

6. 2 つめの鍵分割ユーザー名を入力します。

7. 鍵分割ユーザー用のパスフレーズを入力して、Enter キーを押します。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #3:

Are you sure that you want to log the KMA back into the Cluster?
[y/n]: n

Press Enter to continue:
```

8. Key Split User Name #3 が表示されたら Enter キーを押して、鍵分割ユーザーの承認を終了します。

9. n を入力して Enter キーを押します。

ユーザーのパスフレーズの設定

このメニューオプションを使用すると、セキュリティー責任者は、セキュリティー責任者を含む任意のユーザーに対してパスフレーズを設定することができます。

ユーザーのパスフレーズを設定するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、2 を入力して Enter キーを押します。次の情報が表示されます。

```
Set User's Passphrase
------------------------------------------------------------
Press Ctrl-c to abort.
Please enter the User Name:
```

2. プロンプトで、ユーザー名を入力して Enter キーを押します。次の情報が表示されます。

```
Passphrases must be at least 8 characters and at most 64
characters in length.
Passphrases must not contain the User's User Name.
Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter the desired Passphrase:

Please re-enter the desired Passphrase:

Press Enter to continue:
```

3. プロンプトで、パスフレーズを入力して Enter キーを押します。

4. 「Please re-enter the desired Passphrase:」プロンプトで、同じパスフレーズを入力して Enter キーを押します。次の情報が表示され、パスフレーズが設定されていることが示されます。Enter キーを押して、メインメニューに戻ります。

```
Press Enter to continue:
```

KMA の IP アドレスの設定

このオプションは、KMA の IP アドレスの設定を変更します。この情報は、最初に QuickStart プログラムで設定され (27 ページの「IP アドレスの設定」を参照)、このオプションで変更することができます。

大規模なマルチサイトクラスタでは、ドライブがクラスタ内のすべての KMA のサブセットにのみ接続されている場合があります。次の注意事項は、ドライブを接続できる一連の KMA に適用されます。

注意 – この機能は、慎重に使用するようにしてください。ある KMA の情報を変更すると、その他のすべての KMA は、これらが接続されていれば、その更新をただちに受信します。KMA が接続されていない場合は、KMA がふたたび接続可能になると、その他の KMA を更新します。

ただし、たとえば、ネットワーク異常により相互に接続していない 2 つの KMA が存在する場合に、両方の IP アドレスを変更すると、ネットワークが修復されてもそれらを再接続することはできません。

この場合、一方の KMA に対して「KMA のクラスタへのログイン」機能を使用してもう一方の KMA に再接続し、最初にパスフレーズを更新する必要があります。たとえば、KMA A と KMA B が接続されていない場合に、両方の IP アドレスを変更すると、A にログインして B のパスフレーズを変更する必要があります。次に、B のコンソールにログインし、「KMA のクラスタへのログイン」機能を使用して A に再度接続します。

テープドライブを使用する場合も注意してください。テープドライブは、更新された IP 情報を自動的に受信しません。テープドライブは、テープがマウントされるときにのみ、更新された IP 情報を取得します。このため、夜間にのみテープジョブを実行し、日中にすべての KMA の IP アドレスを変更する典型的な環境である場合、ドライブはどの KMA とも通信できません。この状況が発生した場合は、ドライブを KMS クラスタに再登録する必要があります。これを回避するために、KMA の IP アドレスを 1 つずつ変更し、すべてのドライブがその変更を受信するまで待機してから、次の変更を行なってください。

KMA の IP アドレスを設定するには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、3 を入力して Enter キーを押します。現在の設定が表示されます。

```
Set KMA IP Addresses
------------------------------------------------------------


Press Ctrl-c to abort.

An IP Address configuration must be defined in order for
the KMA to communicate with other KMAs, Agents, or Users
in your system.

Current settings:
  Management Hostname : balblair
  Management IP Address : 10.80.41.5
  Management Subnet Mask : 255.255.254.0

  Service Hostname : balblairsvc
  Service IP Address : 192.168.5.1
  Service Subnet Mask : 255.255.255.0

  Gateway IP Address : 10.80.41.254
  DNS IP Address : 10.80.0.4
  DNS Domain : stortek.com

Please enter the Management Network Hostname: balblair

Do you want to use DHCP to configure the Management Network
interface? [y/n]:

Please enter the Management Network IP Address: 10.80.41.5

Please enter the Management Network Subnet Mask: 255.255.254.0

Please enter the Service Network Hostname: balblairsvc

Do you want to use DHCP to configure the Service Network interface?
[y/n]:

Please enter the Service Network IP Address: 192.168.5.1

Please enter the Service Network Subnet Mask: 255.255.255.0

Please enter the Gateway IP Address (optional but necessary
if this KMA is to communicate with an entity on a different
IP Subnet): 10.80.41.254

Please enter the Primary DNS Server IP Address (optional):
10.80.0.4

Please enter the DNS Domain: stortek.com

Are you sure that you want to commit these changes? [y/n]: y

Press Enter to continue:
```

2. 管理ネットワークのホスト名を入力します。

3. 「Do you want to use DHCP to configure the Management Network interface」プロンプトで、n または y のいずれかを入力します。n を入力した場合は、手順 4 に進みます。y を入力した場合は、手順 6 に進みます。

4. プロンプトで、管理ネットワークの IP アドレスを入力して Enter キーを押します。

5. 「Please enter the Management Network Subnet Mask:」プロンプトで、サブネットマスクアドレス (255.255.254.0 など) を入力して Enter キーを押します。

6. 保守用ネットワークのホスト名を入力して、Enter キーを押します。

7. 「**Do you want to use DHCP to configure the Service Network interface**」プロンプトで、n または y のいずれかを入力します。n を入力した場合は、手順 8 に進みます。y を入力した場合は、手順 10 に進みます。

8. プロンプトで、保守用ネットワークの IP アドレスを入力して Enter キーを押します。

9. 「Please enter the Service Network Subnet Mask:」プロンプトで、サブネットマスクアドレス (たとえば、255.255.255.0) を入力して Enter キーを押します。

10. ゲートウェイ IP アドレスを入力して、Enter キーを押します。

11. 「Please enter the Primary DNS Server IP Address (optional):」プロンプトで、値を入力して Enter キーを押します。

12. DNS ドメインを入力して、Enter キーを押します。

13. 「Are you sure that you want to commit these changes? [y/n]:」プロンプトで、y と入力します。

注 – Ctrl+c を押すと常に、変更が保存されずにメインメニューに戻ります。ユーザーが最後のプロンプトで y を入力することによって、操作が確認された場合にかぎり、変更は受け入れられます。y を入力したあと、メインメニューに戻ります。

KMA の出荷時のデフォルトへのリセット

このメニューオプションを使用すると、セキュリティー責任者は、KMA を出荷時のデフォルト状態にリセットできます。

注意 – リセットは回復不可能なため、KMA の情報は失われます。

これは破壊的な処理で、ハードディスクに格納されているすべてのデータが失われることになります。システムは強制的に再起動されます。ファイルシステムは再フォーマットされ、新しい暗号化鍵を使用するための準備が行われます。

KMA を出荷時のデフォルトにリセットするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**4** を入力して Enter キーを押します。次の情報が表示されます。

```
Reset to Factory Default State
------------------------------------------------------------

Press Ctrl-c to abort.

WARNING:
All information stored on this KMA will be destroyed!
Access to all protected data will be lost unless a backup
of the KMA data has been created or Cluster Peer
KMAs are present.
Please consult the Administrative Guide before proceeding
with this operation.

The system will be rebooted after performing the reset.

Zeroize KMA before resetting (this process will take approximately
4 hours) [y/n]:

Are you sure that you want to reset the KMA to the
Factory Default State?

Type RESET to confirm: no

Press Enter to continue:
```

注意 – この KMA のすべての情報は破壊されます。KMA のデータのバックアップが作成されているか、クラスタピア KMA が存在する場合を除き、すべての保護されたデータへのアクセスは失われます。

---

2. 「`Zeroize KMA before resetting`」プロンプトで、**n** または **y** のいずれかを入力します。**y** を入力した場合、ハードドライブのすべての情報が確実に完全消去されます。

注 – この処理には、約 4 時間かかります。

3. 「`Type RESET to confirm`」プロンプトで、RESET と入力して Enter キーを押します。次の情報が表示され、KMA のリセット中であることが示されます。

```
Resetting...
```

4. 認証が完了すると、QuickStart に戻ります。25 ページの「QuickStart プログラムの実行」を参照してください。

技術サポートアカウントの有効化

「Technical Support」メニューオプションを使用すると、オペレータはオペレーティングシステムのサポートアカウントとそのアカウントの SSH アクセスを有効または無効にすることができます。デフォルトでは、技術サポートアカウントおよび SSH アクセスはどちらも無効です。サポートアカウントのパスフレーズは Sun サポートのみが知っているため、このサポートアカウントを有効にすると、コンソールユーザーが KMA にこれ以上アクセスすることは許可されません。

1. 技術サポートアカウントを有効にするには、次の手順を実行します。

メインメニューの「Please enter your choice:」プロンプトで、5 を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが無効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently DISABLED.
************************ IMPORTANT ************************
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
************************************************************
Would you like to ENABLE this account? [y/n]:
```

2. プロンプトで、y を入力して Enter キーを押し、アカウントを有効にします。次の情報が表示され、SSH アクセスが使用不可であることを示します。SSH アクセスを使用可能にすると、技術サポートは遠隔から問題の診断を行うことができます。

```
SSH access for the support account is currently DISABLED.
Enabling SSH access for the support account allows a
Technical Support representative to connect to the KMA
from a remote location in order to diagnose a potential
problem.
Would you like to ENABLE SSH access for the support account? [y/n]:
```

3. プロンプトで、y を入力して Enter キーを押します。次の情報が表示され、SSH ホスト鍵の目的が示されます。

```
When a Technical Support representative connects to the
KMA using SSH, SSH host keys must be verified via an
alternative secure communication channel in order to detect
a potential “man-in-the-middle” attack.
Please record and store these SSH host keys securely.

SSH host keys are generated when SSH is enabled for the
first time. They may be subsequently regenerated to invalidate
the existing SSH host keys.

Would you like to regenerate the SSH host keys? [y/n]:
```

4. プロンプトで、y を入力して Enter キーを押します。次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to commit these changes? [y/n]:
```

5. プロンプトで、y を入力して Enter キーを押します。次の情報が表示され、アカウントが有効であることが示されます。Enter キーを押して、メインメニューに戻ります。

```
Press Enter to continue:
```

技術サポートアカウントの無効化

技術サポートアカウントを無効にするには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、5 を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.
Please refer to accompanying user documentation for Technical
Support contact information.
The support account is currently ENABLED.
************************ IMPORTANT ************************
Enabling the support account and SSH access is a security
risk. These should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
************************************************************
Would you like to DISABLE this account? [y/n]:
```

2. プロンプトで、y を入力して Enter キーを押し、アカウントを無効にします。
3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to commit these changes? [y/n]:
```

4. プロンプトで、y を入力して Enter キーを押します。SSH サービスは自動的に停止します。

主管理者の有効化

「Primary Administrator」メニューオプションを使用すると、KMA に対する主管理者のアクセスを有効または無効にすることができます。

- 主管理者のアクセスを有効にするには、最初に技術サポートを有効にする必要があります (オプション 5)。
- このタスクは、セキュリティー責任者のみが有効にすることができます。また、オペレータまたはセキュリティー責任者のどちらでも無効にすることができます。

注意 – 主管理者機能を使用すると、ユーザーは、技術サポートとしてログインし、root によるアクセスと同等の主管理者のアクセスが許可されます。これは危険ですが、状況によっては、問題からシステム回復させるために必要になる場合があります。ただし、バックラインサポートまたはエンジニアリングからの直接のガイダンスが必要なことがあります。

---

1. 主管理者のアクセスを有効にするには、次の手順を実行します。

メインメニューの「Please enter your choice:」プロンプトで、6 を入力して Enter キーを押します。次の情報が表示され、主管理者のアクセスが無効であることが示されます。

```
Primary Administrator
------------------------------------------------------------

Press Ctrl-c to abort.

The Primary Administrator role is currently DISABLED.

************************* WARNING ************************
Providing the support account with Primary Administrator
privileges
is a security risk.  This setting should not be left enabled unless
required for troubleshooting purposes.

Ensure that these privileges are disabled when not required.
**********************************************************

Would you like to ENABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. プロンプトで、y を入力して Enter キーを押し、アカウントを有効にします。

3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]:
```

4. プロンプトで、y を入力して Enter キーを押します。主管理者のアクセスが有効になりました。

主管理者の無効化

「Primary Administrator」メニューオプションを使用すると、KMA に対する主管理者のアクセスを有効または無効にすることができます。

注 – このタスクは、セキュリティー責任者のみが有効にすることができます。また、オペレータまたはセキュリティー責任者のどちらでも無効にすることができます。

主管理者のアクセスの無効化は即時に実行されます。別のユーザーが主管理者として接続している場合に、このアクセスを無効にすると、そのユーザーが次に実行しようとしたコマンドは失敗します。

1. 主管理者のアクセスを無効にするには、次の手順を実行します。

メインメニューの「Please enter your choice:」プロンプトで、6 を入力して Enter キーを押します。次の情報が表示され、アクセスが有効であることが示されます。

```
Primary Administrator
------------------------------------------------------------

Press Ctrl-c to abort.

The Primary Administrator role is currently ENABLED.

Would you like to DISABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to DISABLE these privileges for the
support account? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. プロンプトで、y を入力して Enter キーを押し、アカウントを無効にします。

3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. プロンプトで、y を入力して Enter キーを押します。主管理者のアクセスが無効になりました。

キー配列の設定

このオプションを使用すると、キー配列を英語から各種言語に変更できます。

注 – 押したキーを KMA が正しく解釈するために、キー配列の設定が KMA に接続されたキーボードの配列と一致するようにしてください。

キー配列を設定するには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**7** を入力して Enter キーを押します。次のようにキー配列が表示されます。

```
Set Keyboard Layout
-------------------------------------------------------------

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian ( 2) Belarusian ( 3) Belgian
( 4) Bulgarian ( 5) Croatian ( 6) Danish
( 7) Dutch ( 8) Finnish ( 9) French
(10) German (11) Icelandic (12) Italian
(13) Japanese-type6 (14) Japanese (15) Korean
(16) Malta_UK (17) Malta_US (18) Norwegian
(19) Portuguese (20) Russian (21) Serbia-And-Montenegro
(22) Slovenian (23) Slovakian (24) Spanish
(25) Swedish (26) Swiss-French (27) Swiss-German
(28) Taiwanese (29) TurkishQ (30) TurkishF
(31) UK-English (32) US-English


The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. 「`Please enter the keyboard layout [ US-English ] :`」プロンプトで、キー配列を変更する言語を入力します。
3. プロンプトで、**y** を入力して Enter キーを押します。次の情報が表示され、変更が行われたことが示されます。Enter キーを押して、メインメニューに戻ります。

```
The keyboard layout has been applied successfully.

Press Enter to continue:
```

ログアウト

現在の KMS コンソールセッションからログアウトするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**0** を入力して Enter キーを押します。
2. 現在のセッションが終了して、ログインプロンプトが表示されます。ユーザーは、このログインプロンプトを使用して、KMS コンソールにふたたびログインできます。

その他のロールの機能

この節では、その他のロール (コンプライアンス責任者、バックアップオペレータ、監査者) が実行できる機能について説明します。次の機能があります。

- キー配列の設定
- KMA からのログアウト

```
Key Management System Version xxx (co1)
------------------------------------------------------------

(1) Set Keyboard Layout
(0) Logout

------------------------------------------------------------
Please enter your choice:
```

キー配列の設定

このオプションを使用すると、キー配列を英語から各種言語に変更できます。

注 – 押したキーを KMA が正しく解釈するために、キー配列の設定が KMA に接続されたキーボードの配列と一致するようにしてください。

キー配列を設定するには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**1** を入力して Enter キーを押します。次のようにキー配列が表示されます。

```
Set Keyboard Layout
-------------------------------------------------------------

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian ( 2) Belarusian ( 3) Belgian
( 4) Bulgarian ( 5) Croatian ( 6) Danish
( 7) Dutch ( 8) Finnish ( 9) French
(10) German (11) Icelandic (12) Italian
(13) Japanese-type6 (14) Japanese (15) Korean
(16) Malta_UK (17) Malta_US (18) Norwegian
(19) Portuguese (20) Russian (21) Serbia-And-Montenegro
(22) Slovenian (23) Slovakian (24) Spanish
(25) Swedish (26) Swiss-French (27) Swiss-German
(28) Taiwanese (29) TurkishQ (30) TurkishF
(31) UK-English (32) US-English


The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. 「`Please enter the keyboard layout [ US-English ] :`」プロンプトで、キー配列を変更する言語を入力します。
3. プロンプトで、**y** を入力して Enter キーを押します。次の情報が表示され、変更が行われたことが示されます。Enter キーを押して、メインメニューに戻ります。

```
The keyboard layout has been applied successfully.

Press Enter to continue:
```

ログアウト

現在の KMS コンソールセッションからログアウトするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**0** を入力して Enter キーを押します。
2. 現在のセッションが終了して、ログインプロンプトが表示されます。ユーザーは、このログインプロンプトを使用して、KMS コンソールにふたたびログインできます。

用語集

A

Advanced Encryption Standard (AES) FIPS で承認された NIST 暗号化規格で、電子データの保護に使用されます。

AES 「Advanced Encryption Standard」を参照してください。

B

BOT Beginning of Tape (テープの先頭) の略。

C

CA 「認証局 (CA)」を参照してください。

E

EKT Enabling Key Token の略。有効化鍵トークン (デバイス鍵) のことです。KMS Version 1.x の用語。

F

FIPS Federal Information Processions Standards (連邦情報処理標準) の略。National Institute of Standards and Technology (NIST、米国標準規格局) は、米国商務省の技術管理部内の非規制連邦機関であり、次のような標準規格や技術の開発および促進を行なっています。

- Computer Security Division and Resource Center (CSRC)
- Federal Information Processing Standards (FIPS、連邦情報処理標準)

詳細は、次の URL にアクセスしてください。
http://www.nist.gov/

G

GUI Graphical User Interface (グラフィカルユーザーインタフェース) の略。

H

Hash Message Authentication Code (HMAC) 暗号化での HMAC (keyed-Hash Message Authentication Code) とは、暗号化ハッシュ関数と秘密鍵を組み合わせて計算される、メッセージ認証コード (Message Authentication Code、MAC) の一種です。

K

Key Management Appliance (KMA) KMS 2.0 ソフトウェアがプリインストールされた SunFire X2100-M2 サーバー。Solaris 10 オペレーティングシステムが実装された、実証済みのデュアルコアプロセッサアプライアンスであり、ポリシーベースの鍵管理サービスおよび鍵プロビジョニングサービスを提供します。

Key Management System (KMS) 鍵管理を提供するシステム。Sun/StorageTek システムには、暗号化エージェントの代わりに鍵管理を提供する KMS コンポーネントがあります。

KMA 「Key Management Appliance」を参照してください。

KMS 「Key Management System」を参照してください。

KMS クラスタ 相互接続された 1 つ以上の KMA の集合。KMS クラスタ内のすべての KMA は、同一の情報を持ちます。ただし、ある KMS が停止している場合、または新たに作成された情報の一部が KMS クラスタ内のすべての KMA にはまだ伝播さ

れていない場合はこの限りではありません。KMS クラスタ内の任意の KMA で実行された動作は、最終的に KMS クラスタ内のすべての KMA に伝播されます。

N

NIST National Institute of Standards and Technology (米国標準規格局) の略。

O

OKT Operational Key Token の略。運用中鍵トークン (媒体鍵) のことです。KMS Version 1.x の用語。

P

PC 鍵 テープドライブの暗号化モードでの読み取りと書き込みを有効にします。

R

Rijndael アルゴリズム 米国標準規格局 (NIST) によって Advanced Encryption Standard (AES) 用に選択されたアルゴリズム。「ラインダール」と読むこのアルゴリズムは、Vincent Rijmen と Joan Daemen という 2 人のベルギー人暗号研究者によって考案されたものであり、暗号名にはこの 2 人の姓が反映されています。

RSA 暗号化での RSA とは、MIT の Ron Rivest、Adi Shamir、および Leonard Adleman によって考案された公開鍵暗号化アルゴリズムです。RSA という略称は、この 3 人の姓の頭文字です。

S

Secure Hash Algorithms (SHA) Secure Hash Algorithms は、米国国家安全保障局 (NSA) によって策定され、NIST によって米国連邦情報処理標準として公開された暗号化ハッシュ関数です。

Shamir の秘密の共有法 暗号化アルゴリズムの一種。秘密情報が分割され、それぞれの分割部分には一意の内容のみが含まれるため、秘密情報の再構築にはこれらの分割部分の一部またはすべてが必要になります。秘密情報を再構築するためにすべての分割部分を組み合わせることは現実的ではありません。このため、定足数またはしきい値スキーマが使用されています。

T

T10000 テープドライブ T10000 テープドライブは、データの大容量ストレージとして設計された、小型のモジュラー型高性能テープドライブです。最大 500 G バイトの非圧縮データに対応できます。

Transport Layer Security (TLS) 暗号化プロトコルの一種。Web 参照、電子メール、インターネットファックス送信、インスタントメッセージ、その他のデータ転送などを目的として、インターネット上のセキュリティー保護された通信を提供します。

U

UID 暗号化エージェントやユーザーなどの KMS 構成要素の一意の識別子として機能する文字列。

Ultra Tape Drive Encryption Agent Ultra 2.0 準拠の暗号化テープドライブでは、鍵管理に Ultra Tape Drive Encryption Agent ソフトウェアを活用します。このようなドライブでは、テープボリュームで使用される鍵データを KMS から取得します。このため、BOT からの書き込みごとに、ボリューム上のデータの暗号化に新しい鍵データが使用されます。その結果、データユニットの定義がテープボリュームに割り当てられ、データユニットの外部 ID はボリュームシリアル番号になります。

UTC Coordinated Universal Time (協定世界時) の略。

あ

暗号化 データを暗号に変換することです。暗号化は、データの安全性を確保するもっとも有効な方法の一つです。暗号化されたファイルを読み取るには、復号化を可能にする特殊な鍵またはパスワードにアクセスできる必要があります。

暗号化アクセラレータ 暗号化アクセラレータは、データ暗号化および復号化の処理速度向上を目的として使用されるハードウェアデバイス (カード) です。これにより、需要が高い状況でのシステム性能が向上します。

暗号化使用可能 デバイスでの暗号化をオンに設定して暗号化を行う機能を持つテープドライブ。

暗号化動作中 ドライブで暗号化機能がオンになっている状態の暗号化対応テープドライブ。

暗号化有効期間 鍵を暗号化に使用できる期間。鍵が最初にドライブに割り当てられた時点から開始されます。この値は、NIST 800-57 の「Originator Usage Period」に対応しています。

暗号法 暗号化テキストと呼ばれる判読不能の形式に情報を変換 (暗号化) することによって情報を保護する技術。特別な鍵を所有しているユーザーのみが、メッセージを元の形式に解読 (復号化) できます。

い

インターネットプロトコル (IP) インターネット環境でデータの発信元から受信先への経路指定に使用されるプロトコル。

インターネットプロトコル (IP) アドレス デバイスを識別してネットワーク経由でアクセスできるようにする 4 バイトの値。IP アドレスの書式は、ピリオドで区切られた 4 つの数値で表される 32 ビットの数値アドレスです。それぞれの数値は 0 ～ 255 の値を取ります。たとえば、IP アドレスは 129.80.145.23 のようになります。「TCP/IP アドレス」としても知られています。

え

エージェント 鍵データを作成および取得するために KMS と対話するさまざまなタイプの暗号化エージェントを作成できます。StorageTek T10000 モデル A と B、T9840D、および HP LTO4 の各テープドライブは、暗号化機能に対して使用可能にすると、一種の暗号エージェントになります。

エージェント API 「エージェントライブラリ API」を参照してください。

エージェントライブラリ エージェントライブラリは、鍵データを KMS から取り出すために、エージェントによって使用されます。

エージェントライブラリ API エージェントライブラリによって提供される API。エージェントはこの API を呼び出します。

お

オペレータ システムの日常業務の管理を担当するユーザーのロール。

か

鍵 ここでは、鍵は対称データ暗号化鍵のことです。エージェントは、1 つ以上のデータユニットに対応するデータの暗号化を行うために、新しい鍵データを要求できます。鍵は単一の鍵グループに属しているため、その鍵グループに関連付けられているエージェントのみが、対応する鍵にアクセスできます。鍵には、その鍵が属している鍵グループに関連付けられている鍵ポリシーで規定された、暗号化と復号化の暗号化有効期間があります。鍵のタイプ、つまり鍵の長さとアルゴリズムは、暗号化エージェントによって指定されます。

鍵 Key Management System によって生成されるランダムなビット文字列。キーボードを使用して入力するか、または購入します。鍵には、次のタイプがあります。

- デバイス鍵は、テープドライブの暗号化機能を使用可能にします。
- 媒体鍵は、テープカートリッジ上の顧客データを暗号化および復号化します。
- PC 鍵は、テープドライブの暗号化機能を使用可能にします。
- 通信鍵は、トークンからドライブへの LAN を介した転送中に、暗号化 (認証) を行うための別の層を媒体鍵に追加します。
- 分割鍵はドライブごとに一意であり、保護を実現するためにラップ鍵と連携します。
- ラップ鍵は、LAN 上の媒体鍵とトークンを暗号化します。

鍵グループ 鍵グループは、鍵を整理して鍵ポリシーと関連付けるために使用されます。また、鍵グループは、暗号化エージェントによる鍵データへのアクセスを強制するためにも使用されます。

書き込み鍵 データをテープに書き込む場合に使用される媒体鍵です。

鍵転送パートナー 鍵転送パートナーとは、KMS 間でエクスポートされる鍵の受信側のことです。

鍵転送ファイル 鍵と関連データユニット (定義されている場合) が含まれるファイル。鍵データを KMS クラスタ間で移動する場合に使用されます。転送にかかわる双方で、交換の相手側となる鍵転送パートナーが設定されている必要があります。鍵転送ファイルは、転送される情報の機密性と完全性を確実にするため、署名および暗号化されます。

鍵ポリシー 鍵ポリシーによって、鍵に適用される暗号化有効期間の設定値が提供されます。各鍵グループには鍵ポリシーがあり、鍵ポリシーは 0 個以上の鍵グループに適用できます。ポリシーで指定された暗号化と復号化の暗号化有効期間によって、鍵の使用法が制限され、鍵の無効化、破棄など、鍵のライフサイクルイベントが発生します。

また、鍵ポリシーによって制御される鍵を、どのような状況でほかの鍵転送パートナーにエクスポートできるか、またはその他の鍵転送パートナーからインポートできるかも、鍵ポリシーで制御されます。

監査 「監査ログ」を参照してください。

監査者 監査リストイベント、KMA セキュリティーパラメータなどのシステム監査証跡を表示できるユーザーのロール。

監査ログ KMS クラスタでは、システム全体で発生する監査可能なすべてのイベントに関するログを維持します。エージェントは、監査可能なイベントについて、このログにエントリを追加できます。

く

クラスタ クラスタは、耐障害性、可用性、および拡張性を向上させるために単一システムにまとめられた一連の Key Management Appliance です。

クリティカルセキュリティーパラメータ セキュリティー関連情報 (たとえば、暗号化の公開鍵と秘密鍵、パスワードや PIN などの認証データ) のことです。この情報が公開されたり変更されると、暗号化モジュールのセキュリティーが損なわれる可能性があります。

こ

コンプライアンス責任者 組織内のデータの流れを管理するユーザーのロール。データコンテキスト (鍵グループ) と、データの保護方法および最終的な破棄方法を決定する規則 (鍵ポリシー) を定義および配備できます。

さ

サイト サイトは、各 KMS および暗号化エージェントの属性であり、ネットワークの場所を示します。暗号化エージェントは、KMS クラスタに接続する場合に、可能なかぎり同じサイト内の KMA との通信を確立しようとします。

し

システムダンプ ユーザーによって開始される操作。すべての関連データが単一ファイルにまとめられ、ユーザーがこの操作を開始したマシンにそのファイルがダウンロードされます。ダウンロードが完了すると、ファイルは KMA から削除されます。

証明書 証明書はデジタル署名されたドキュメントで、所有者の承認状況と名前の妥当性検査に使用されます。このドキュメントは、特殊な形式のデータブロックで構成されており、認証に必要な証明書の所有者名 (サブジェクト DN)、シリアル番号、有効期間、所有者の公開鍵、発行者の DN、および発行者のデジタル署名が含まれます。発行者は、所有者の名前がドキュメントの公開鍵に関連付けられている名前であることとを保証します。

自律ロック 自律ロック解除が使用可能の場合、ロックされている KMA のロックを解除するには、定足数のセキュリティー責任者が必要です。使用不可の場合は、任意のセキュリティー責任者が KMA のロックを解除できます。

せ

セキュリティーポリシー 組織データの機密性、データにアクセスする可能性のある各種実体、およびアクセスの管理と制限に適用される規則を厳密に記述したもの。

セキュリティー責任者 セキュリティー設定値、ユーザー、サイト、および転送パートナーを管理するユーザーのロール。

ゼロ化 データを復旧できないようにデータストレージの内容を変更または削除することによって、電子的に格納されたデータ、暗号化鍵、およびクリティカルセキュリティーパラメータを消去すること。

た

タスクの異常終了 (不正終了) コンピュータの処理タスクを停止する、ソフトウェアまたはハードウェアの問題。

つ

通信鍵 トークンからドライブへの LAN を介した転送中に暗号化および認証を行うための別の層を追加します。

て

データユニット データユニットは KMS 内部の抽象的な構成要素で、KMS ポリシーや暗号鍵に関連付けられたストレージオブジェクトを表します。データユニットの具体的な定義は、データユニットを作成した暗号化エージェントによって定義されます。テープドライブの場合、データユニットはテープカートリッジです。

デバイス鍵 テープドライブでの暗号化を有効にします。KMS Version 1.x の用語。

と

トークン KMS Version 1.x の用語。
トークンとは、Ethernet 接続のトークンベイに接続される、コンパクトなインテリジェントデバイスです。トークンには、次の 2 つの役割があります。

- 有効化鍵トークン
- 運用中鍵トークン

トークンベイ KMS Version 1.x の用語。
物理トークンを格納し、1 つまたは 2 つのトークンに対して背面のブラインドメイトコネクタ経由で電源と接続を提供するシャーシのことです。トークンベイは、標準 19 インチラック (1U フォームファクタ) と互換性があります。トークンベイには、デスクトップ型とラックマウント型の 2 つのタイプがあります。

に

認証局 (CA) 認証局は、エンドユーザーの登録および証明書の発行を行います。また、エンドユーザーの下に CA を作成することもできます。KMS 2.0 では、KMA 自体が認証局として機能し、ユーザー、エージェント、およびその他の KMA に対して証明書を発行します。

ね

ネットワーク ソフトウェアおよびハードウェアによるリンクを介してデータ処理デバイスを相互に接続し、情報の交換を容易にするノードと分岐の配置。

は

媒体鍵 テープカートリッジ上の顧客データを暗号化および復号化します。

バックアップオペレータ データと鍵のセキュリティー保護と格納の責任を負うユーザーのロール。

バックアップ鍵ファイル バックアップ処理中に生成されるファイルで、バックアップファイルの暗号化に使用される鍵が格納されます。このファイルは、システムマスター鍵を使用して暗号化されます。マスター鍵は、定足数の鍵分割資格を使用して、コアセキュリティーバックアップファイルから抽出されます。

バックアップファイル バックアップ処理中に作成されるファイルで、KMA の復元に必要なすべての情報が含まれています。バックアップ専用に生成された鍵を使用して暗号化されています。鍵は、対応するバックアップ鍵ファイルに格納されます。

ほ

ボリュームシリアル番号 テープボリュームの特定に使用される、6 文字の英数字ラベル。

ゆ

有効化鍵 テープドライブを使用可能にするために使用される、64 文字の一意の鍵。「PC 鍵」も参照してください。

よ

読み取り鍵 データをテープから読み取る場合に使用される媒体鍵です。

ら

ラップ鍵 LAN 上およびトークン上の媒体鍵を暗号化します。

索引

T

U

W

あ

い

う

え

お

か

き

く

こ

さ

し

せ

そ

た

つ

て

と

に

ね

は

ほ

め

ゆ

よ

ら

ろ

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com

Argentina: 5411-4317-5636 • **Australia:** 1-800-550-786 • **Austria:** 43-1-601-26-0 • **Balkans:** 301-6188-111 • **Belgium:** 32 2-704 89 83 • **Brazil:** 55-11-51872100 • **Brunei:** 65-216-8333 • **Canada:** 1-800-422-8020 **(General);** 416-964-2001 **(Learning Management System Sales,Toronto)** • **Chile:** 562-372-4500 • **Colombia:** 571-629-2323 **Czech Republic:** 420 2 33009311 • **Denmark:** 45 4556 5040 • **Egypt:** 00 202 570 9442 • **Finland:** 358-9-525-561 • **France:** 33-1-41-33-17-17 • **Germany:** 49-89-460-08-2788 • **Greece:** 30-01-6188101 • **Hong Kong:** 852-2877-7077 • **Hungary:** 361-202-4415 • **India:** 91-80-229-8989 • **Indonesia:** 65-216-8333 • **Ireland:** 353-1-668-4377 **Israel:** 972-9-9710500 • **Italy:** 39-02-9259511 • **Japan:** 81-3-5779-1820 • **Korea:** 82-2-3453-6602 • **Malaysia:** 603-2116-1887 • **Middle East:** 00 9714 3366333 • **Mexico:** 525-261-0344 • **Netherlands:** 31-33-4515200 • **New Zealand:** 0800-786-338 • **North West Africa:** 00 9714 3366333 • **Norway: From Norway:** 47-22023950, **To Norway:** 47-23369650 • **Pakistan:** 00-9714-3366333 • **People's Republic of China:** 8610-6803-5588 • **Philippines:** 632-885-7867 • **Poland:** 48-22-8747848 • **Portugal:** 351-21-413-4000 • **Russia:** 7-095-935-8411 • **Saudi Arabia:** 00 9714 3366333 • **Singapore:** 65-216-8300 • **South Africa:** 27-11-256-6300 • **Spain:** 34-902-210-412 • **Sri Lanka:** 65-2168333 • **Sweden:** 46-8-631 22 00 • **Switzerland:** 41-1-908-90-50 **(German)** 41-22-999-0444 **(French)** • **Taiwan:** 886-2-25185735 • **Thailand:** 662-344-6855 • **Turkey:** 90 212 335 22 00 • **United Kingdom:** 44-1276-416-520 • **United States:** 1-800-422-8020 • **Venezuela:** 582-905-3800 • **Vietnam:** 65-216-8333 • **Worldwide Headquarters:** 1-650-960-1300