



# Crypto Key Management System (KMS)

---

Guide d'administration

Version 2.0

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

N° de référence : 316030001  
Février 2008

Copyright 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie décrite dans ce document. En particulier, et sans limitation aucune, ces droits de propriété intellectuelle peuvent porter sur un ou plusieurs brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et un ou plusieurs brevets supplémentaires ou demandes de brevet en instance aux États-Unis et dans d'autres pays.

Ce document et le produit afférent sont exclusivement distribués avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou de ce document ne peut être reproduite sous quelque forme que ce soit, par quelque moyen que ce soit, sans l'autorisation écrite préalable de Sun et de ses éventuels bailleurs de licence.

Les logiciels détenus par des tiers, y compris la technologie relative aux polices de caractères, sont protégés par copyright et distribués sous licence par des fournisseurs de Sun.

Des parties de ce produit peuvent être dérivées des systèmes Berkeley BSD, distribués sous licence par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays, distribuée exclusivement sous licence par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, Solaris et StorageTek sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant la marque SPARC reposent sur une architecture développée par Sun Microsystems, Inc.

L'interface graphique utilisateur d'OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. à l'intention des utilisateurs et détenteurs de licences. Sun reconnaît les efforts de pionniers de Xerox en matière de recherche et de développement du concept des interfaces graphiques ou visuelles utilisateur pour l'industrie informatique. Sun détient une licence non exclusive de Xerox sur l'interface graphique utilisateur (IG) Xerox, cette licence couvrant également les détenteurs de licences Sun qui implémentent des IG OPEN LOOK et se conforment par ailleurs aux contrats de licence écrits de Sun.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTE AUTRE CONDITION, DÉCLARATION ET GARANTIE, EXPRESSE OU TACITE, EST FORMELLEMENT EXCLUE, DANS LA MESURE AUTORISÉE PAR LA LOI EN VIGUEUR, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.

---

Vos commentaires sont les bienvenus. Contactez le système de réception de commentaires de Sun Learning Services à l'adresse :

SLSFS@Sun.com

ou

Sun Learning Services

Sun Microsystems, Inc.

One StorageTek Drive

Louisville, CO 80028-3256

États-Unis

Veuillez indiquer le nom de la publication, son numéro de référence et son numéro d'édition (le cas échéant) dans votre courrier. Cela accélérera notre réponse.



# Avis

---

Veillez prendre connaissance des déclarations de conformité et des mises en garde suivantes relatives à ce produit.

---

**Attention** – *Risque d'endommagement de l'équipement* : les câbles reliant les périphériques doivent être blindés et mis à la terre (voir les descriptions dans les manuels d'instruction fournis avec les câbles). L'utilisation de cet équipement avec des câbles non blindés et mal mis à la terre peut provoquer des interférences avec la réception des fréquences radio et des chaînes de télévision.

---

Les changements ou modifications apportés à cet équipement non approuvés au préalable par StorageTek annuleront la garantie. Ces changements ou modifications pourraient par ailleurs rendre cet équipement responsable de dangereuses interférences.

---

## Déclaration de conformité FCC aux ÉtatsHUnis

La déclaration de conformité suivante concerne les règles FCC (Federal Communications Commission) 47 CFR 15.105 :

---

**Remarque** – Cet équipement a été testé et déclaré conforme aux exigences relatives à un appareil numérique de la classe A en vertu de l'article 15 de la réglementation FCC. Ces limites ont été définies dans le but de fournir une protection raisonnable contre les interférences nuisibles dans le cadre d'une utilisation en environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie en fréquences radioélectriques ; s'il n'est pas installé et utilisé conformément aux instructions du manuel d'instructions, il peut créer des interférences nuisibles aux communications radio. L'utilisation de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, que l'utilisateur devra corriger par ses propres moyens.

---

## Mises en garde CISPR 22 et EN55022

Il s'agit d'un produit de classe A. Dans un environnement domestique, ce produit peut causer des interférences radio, auquel cas l'utilisateur sera peut-être amené à prendre des mesures adéquates.

---

## Déclaration de conformité japonaise

La déclaration de conformité suivante en japonais concerne les réglementations VCCI EMI :

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。

**Traduction en français :** il s'agit d'un produit de classe A reposant sur la réglementation technique VCCI (Voluntary Control Council for Interference) en matière de technologies de l'information. Dans un environnement domestique, ce produit peut causer des interférences radio, auquel cas l'utilisateur sera peut-être amené à prendre des mesures correctives.

---

## Déclaration de mise en garde taiwanaise

La déclaration de mise en garde suivante concerne les réglementations BSMI de Taiwan (République de Chine) :

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

**Traduction française :** il s'agit d'un produit de classe A. Dans un environnement domestique, ce produit peut causer des interférences radio, auquel cas l'utilisateur sera peut-être amené à prendre des mesures adéquates.

---

# Déclaration de licence du code interne

La déclaration suivante présente l'accord de licence du code interne de StorageTek :

La déclaration suivante présente l'accord de licence du code interne de StorageTek :

## **AVIS**

### LICENCE DU CODE INTERNE

LISEZ ATTENTIVEMENT CET AVIS AVANT D'INSTALLER ET D'UTILISER CET ÉQUIPEMENT. CET AVIS EST UN ACCORD JURIDIQUE CONCLU ENTRE VOUS-MÊME (EN TANT QU'INDIVIDU OU ENTITÉ), L'UTILISATEUR FINAL, ET LA SOCIÉTÉ STORAGE TECHNOLOGY CORPORATION (« STORAGETEK »), LE FABRICANT DE CET ÉQUIPEMENT. EN OUVRANT LE COFFRET ET EN ACCEPTANT/UTILISANT TOUT COMPOSANT DE L'ÉQUIPEMENT DÉCRIT DANS CE DOCUMENT, VOUS RECONNAISSEZ ÊTRE LIÉ PAR LES CONDITIONS DES PRÉSENTES. SI VOUS N'ÊTES PAS D'ACCORD AVEC LES CONDITIONS DE CET ACCORD, N'OUVREZ **PAS** LE COFFRET ET N'UTILISEZ PAS L'ÉQUIPEMENT. SI VOUS N'AVEZ PAS LE NIVEAU DE RESPONSABILITÉ REQUIS POUR LIER VOTRE ENTREPRISE PAR CET ACCORD, N'OUVREZ **PAS** LE COFFRET ET N'UTILISEZ PAS L'ÉQUIPEMENT. POUR TOUTE QUESTION, CONTACTEZ LE DISTRIBUTEUR STORAGETEK AGRÉÉ OU LE REVENDEUR AUPRÈS DUQUEL VOUS AVEZ ACHETÉ CET ÉQUIPEMENT. SI VOUS AVEZ FAIT L'ACQUISITION DE CET ÉQUIPEMENT DIRECTEMENT AUPRÈS DE STORAGETEK, CONTACTEZ LE REPRÉSENTANT STORAGETEK DE VOTRE RÉGION.

1. **Définitions** : les termes énoncés ci-dessous sont définis de la manière suivante :
  - a. Les « Oeuvres dérivées » se définissent comme des œuvres s'appuyant sur un ou plusieurs travaux préexistants, tels qu'une traduction ou un arrangement musical, ou toute autre forme sous laquelle une œuvre peut être retravaillée, transformée ou adaptée. Une œuvre composée de révisions éditoriales, d'annotations, de corrections ou d'autres modifications qui, prises dans leur ensemble, représentent une œuvre originale d'un auteur est une œuvre dérivée.
  - b. Le « code interne » est un Microcode qui (i) fait partie intégrante de l'Équipement, (ii) est indispensable à l'Équipement pour s'acquitter de ses fonctions de stockage et de récupération de données, et (iii) s'exécute sous l'interface utilisateur d'un tel Équipement. Le Code interne ne comprend pas d'autres Microcodes ou logiciels (fichiers de données inclus), pouvant résider ou s'exécuter sur un tel Équipement, ou être utilisés par ou en rapport avec ce dernier, y compris mais non exclusivement, le Code de maintenance.
  - c. Le « Code de maintenance » se définit comme un Microcode ou autre logiciel (fichiers de données inclus) pouvant résider ou s'exécuter sur un tel Équipement, ou être utilisés par ou en rapport avec ce dernier, et permettant de détecter, d'enregistrer, d'afficher et/ou d'analyser les dysfonctionnements que présente l'Équipement.
  - d. Le « Microcode » se définit comme un ensemble d'instructions (logicielles) incorporé ou chargé dans l'Équipement et s'exécutant sous l'interface utilisateur externe de cet Équipement. Le Microcode comprend à la fois le Code interne et le Code de maintenance ; il peut résider sur un support magnétique ou tout autre support de stockage, sur un circuit intégré ou autre support.
2. L'Équipement que vous avez acheté ou loué a été fabriqué par ou pour StorageTek et contient un Microcode. En acceptant les conditions de cet accord et en utilisant cet Équipement, vous reconnaissez que StorageTek ou ses bailleurs de licences conservent la propriété exclusive de tous les Microcodes et copies sous-jacentes pouvant être exécutés ou utilisés lors de l'utilisation ou de la maintenance de l'Équipement et que ces Microcodes sont protégés par copyright par StorageTek ou ses bailleurs de licences.
3. StorageTek vous accorde par les présentes à vous, l'utilisateur final de cet Équipement, une licence personnelle, non cessible (sauf autorisation dans les conditions de cession stipulées ci-dessous) et non exclusive d'utilisation de chaque exemplaire du Code interne (ou de toute copie de remplacement fournie par StorageTek ou votre revendeur ou distributeur StorageTek agréé). Cette licence vous autorise, vous, l'utilisateur final, à exécuter le Code interne dans le but exclusif de permettre à l'unité spécifique de l'Équipement pour laquelle la copie du Code interne vous a été fournie de s'acquitter de ses fonctions de stockage et de récupération de données conformément aux spécifications publiées officielles de StorageTek (ou de ses bailleurs de licences).
4. Votre licence se limite à l'utilisation du Code interne tel qu'il est stipulé dans les présentes. Il vous est formellement interdit d'utiliser le Code interne dans tout autre but. Vous ne pouvez pas, par exemple, effectuer l'une des opérations suivantes :
  - (i) obtenir, copier, afficher, imprimer, adapter, altérer, modifier, corriger, préparer des Oeuvres dérivées du Code Interne, transférer ou diffuser (par voie électronique ou autre) ou utiliser de toute autre manière le Code interne ;
  - (ii) désassembler, décoder, convertir, décompiler ou effectuer toute opération d'ingénierie inverse sur le Code interne (sauf décompilation contraire expressément autorisée par la législation européenne en vigueur dans le but exclusif d'obtenir des informations qui permettront l'interopérabilité lorsque de telles informations ne sont pas disponibles par aucun autre moyen) ;
  - ou
  - (iii) octroyer en sous-licence, céder ou louer le Code interne ou autoriser une autre personne à utiliser ledit Code interne ou une copie de ce dernier.

5. Aucune condition de la licence énoncée ci-dessus ou de l'Avis entier ne saurait vous céder, de quelque manière que ce soit, une licence ou un titre quelconque, ou tout autre droit d'utilisation du Code de maintenance, ou tout exemplaire d'un tel Code de maintenance. Le Code de maintenance de même que les outils et manuels de maintenance de StorageTek peuvent être conservés sur votre site ou vous être fournis avec une unité de l'Équipement qui vous a été envoyée et/ou est incluse sur le même support que le Code interne. Ils devront cependant être exclusivement réservés à l'usage du personnel du service clientèle de StorageTek ou du personnel d'une entité détenant une licence StorageTek, tous les droits inhérents à ce Code de maintenance, ces outils et manuels de maintenance étant réservés par StorageTek ou ses bailleurs de licences. Vous acceptez de ne pas utiliser ou de tenter d'utiliser le Code de maintenance, ou de permettre à une partie tierce d'utiliser ou d'obtenir ledit Code de maintenance.
6. Vous, l'utilisateur final, acceptez de prendre toutes les mesures qui s'imposent afin de garantir que l'ensemble de vos obligations énoncées dans le présent Avis soit étendu à toute partie tierce ayant accès à l'Équipement.
7. Vous pouvez céder le Code interne à une partie tierce à la condition expresse que cette cession soit effectuée en même temps que celle de l'Équipement sur lequel son utilisation est autorisée. En outre, votre licence d'utilisation du Code interne est déclarée nulle lorsque vous cessez d'être le propriétaire ou le détenteur légal de l'Équipement. Vous devez donner au cessionnaire tous les exemplaires du Code interne de l'Équipement cédé qui sont en votre possession, de même qu'une copie de toutes les conditions de cet Avis.  
Toute cession de ce type se trouve automatiquement (sans action supplémentaire requise de la part de l'une ou l'autre partie) et expressément soumise aux conditions générales du présent Avis transféré dans son intégralité à la partie à laquelle ledit Équipement a été cédé, et ledit cessionnaire accepte les conditions de cette licence dès lors qu'il utilise le Code interne. Vous ne pouvez pas concéder au cessionnaire de l'Équipement des droits supérieurs à ceux qui vous sont été octroyés dans le cadre de cet Avis. StorageTek ne saurait être tenu responsable de toute revendication du contraire par le cessionnaire ou ses successeurs ou ayants droit. En outre, les conditions générales du présent Avis s'appliquent à toutes les copies du Code interne actuellement en votre possession ou utilisation ou acquises par la suite auprès de StorageTek ou d'une partie tierce.
8. Vous reconnaissez que des copies du Code interne et du Code de maintenance peuvent être installées sur l'Équipement avant sa livraison ou fournies avec ledit Équipement et d'autres matériaux qui vous sont expédiés et ce, pour des raisons de commodité pour le personnel de maintenance de StorageTek ou les prestataires de service sous licence par StorageTek. De plus, pendant toute la période de garantie (le cas échéant) couvrant l'Équipement et pendant toutes les périodes où l'Équipement est couvert par un contrat de maintenance auprès de StorageTek ou de prestataires de services sous licence par StorageTek, le Code interne et le Code de maintenance peuvent résider et être exécutés sur ledit Équipement ou utilisés en rapport avec lui. Vous reconnaissez par ailleurs qu'aucun droit sur le Code de maintenance ne vous est conféré dans le cadre de ces périodes. StorageTek ou le prestataire de services sous licence peut conserver le Code de maintenance et les manuels et outils de maintenance sur votre site, mais ces derniers ne peuvent être utilisés que par le personnel du service clientèle de StorageTek ou celui du prestataire de services sous licence par StorageTek. Vous acceptez d'autre part que lors de
  - (i) toute résiliation du contrat de garantie ou du contrat de maintenance ; ou lors de
  - (ii) toute cession de l'Équipement à une partie tierce, StorageTek et ses prestataires de services agréés seront en droit, concernant l'Équipement concerné, de retirer tous les manuels ou outils de maintenance et de supprimer ou de désactiver tous les Codes de maintenance et/ou de remplacer le Microcode comprenant le Code interne et le Code de maintenance par un Microcode uniquement composé du Code interne.

# Historique des révisions

---

<b>CODE</b>	<b>Date</b>	<b>Révision</b>	<b>Description</b>
000227	Mars 2008	A	<i>Guide d'administration de Crypto Key Management System 2.0</i>



# Table des matières

---

<b>Avis</b>	<b>iii</b>
<b>Historique des révisions</b>	<b>ix</b>
<b>Table des matières</b>	<b>xi</b>
<b>Figures</b>	<b>xxi</b>
<b>Tableaux</b>	<b>xxiii</b>
<b>Préface</b>	<b>xxv</b>
<b>1. Introduction</b>	<b>1</b>
Présentation	1
Concepts du logiciel KMS	2
Cluster KMS	2
Agents	2
Connexions réseau	2
Configuration initiale - Connexion directe ou console distante (ELOM)	3
Configuration initiale - programme QuickStart	4
Cycle de vie des clés	4
Transition d'état	5
États et transitions disponibles dans le logiciel KMS	6
Préactivation	6
Active (Actif)	6
Deactivated (Désactivé)	7
Compromised (Compromis)	7

Destroyed (Détruit)	7
Destroyed and Compromised (Détruit et compromis)	8
Utilisateurs et contrôle d'accès basé sur les rôles	9
Opérations autorisées par rôle	9
Protection par quorum	9
Unités de données, clés, groupes de clés et stratégies de clés	10
Connexions TCP/IP et le KMA	11
KMS au sein du réseau	12
Configuration logicielle requise de KMS Manager	13
Utilisation de l'aide en ligne	13
Contrôle d'accès basé sur les rôles	13
Opérations basées sur les rôles	14
Configuration et gestion du dispositif de gestion des clés (KMA)	18
<b>2. Démarrage</b>	<b>19</b>
Démarrage du logiciel ELOM (Embedded Light Out Manager)	20
Connexion au KMA	20
Utilisation d'une connexion réseau	22
Exécution du programme QuickStart	26
Lancement de QuickStart	27
Définition de l'adresse IP	28
Initialisation du KMA	30
Configuration du cluster	31
Références de scission de clés	32
Références initiales de l'utilisateur responsable de la sécurité	35
Préférence de déverrouillage autonome	36
Synchronisation horaire des KMA	37
Intégration à un cluster existant	38
Restauration d'un cluster à partir d'une sauvegarde	41

<b>3. Utilisation de KMS Manager</b>	<b>47</b>
Présentation de KMS Manager	47
Installation du logiciel KMS Manager	48
Appel de KMS Manager	54
Démarrage de KMS Manager sous Windows	54
Démarrage de KMS Manager sous Solaris	54
Présentation de l'IG de KMS Manager	55
Menu System (Système)	56
Menu View (Affichage)	57
Menu Help (Aide)	58
Boutons de barre d'outils	60
Raccourcis clavier	60
Touches d'accès rapide aux menus	60
Utilisation de l'aide en ligne	61
Volets de l'IG de KMS Manager	62
Arborescence des opérations de gestion de KMS	62
Volet des détails des opérations de gestion de KMS	63
Volet du journal d'audit des sessions	64
Barre d'état	65
Panneaux	66
Désinstallation du logiciel KMS Manager	68
Appel du fichier exécutable	68
Appel de l'utilitaire Ajout/Suppression de programmes (Windows uniquement)	68
Fin du processus de désinstallation	69
<b>4. Utilisation du menu System (Système)</b>	<b>71</b>
Connexion au cluster	71
Création d'un profil de cluster	71
Suppression d'un profil de cluster	75
Déconnexion d'un KMA	75
Modification de la phrase de passe	76
Définition des paramètres de configuration	77
Quitter KMS Manager	79

<b>5. Tâches du responsable de la sécurité</b>	<b>81</b>
Rôle Security Officer (Responsable de la sécurité)	82
Menu KMA List (Liste des KMA)	83
Affichage des KMA	84
Création d'un KMA	87
Affichage/Modification des détails d'un KMA	90
Définition de la phrase de passe d'un KMA	92
Suppression d'un KMA	93
Menu User List (Liste des utilisateurs)	94
Affichage des utilisateurs	95
Création d'un utilisateur	98
Affichage/Modification des détails d'un utilisateur	100
Définition de la phrase de passe d'un utilisateur	101
Suppression d'un utilisateur	102
Menu Role List (Liste des rôles)	103
Affichage des rôles	103
Affichage des opérations associées à un rôle	105
Menu Site List (Liste des sites)	106
Affichage des sites	107
Création d'un site	110
Affichage/Modification des détails d'un site	112
Suppression d'un site	113
Menu SNMP Manager List (Liste des gestionnaires SNMP)	114
Affichage des gestionnaires SNMP d'un KMA	114
Création d'un nouveau gestionnaire SNMP	117
Affichage/Modification des détails d'un gestionnaire SNMP	119
Suppression d'un gestionnaire SNMP	120
Transfert de clés	121
Présentation	121
Fonction Key Transfer Partners (Partenaires de transfert de clés)	121
Processus de transfert de clés	122
Configuration de partenaires de transfert de clés	122
Exportation/Importation de clés	124

Menu Transfer Partners (Partenaires de transfert)	125
Menu Transfer Partner List (Liste des partenaires de transfert)	126
Création d'un partenaire de transfert	130
Affichage/Modification des détails du partenaire de transfert	133
Suppression d'un partenaire de transfert	136
Menu Key Transfer Public Key List (Liste des clés publiques de transfert de clés)	137
Affichage de la liste de clés publiques de transfert	137
Affichage des informations détaillées sur les clés publiques de transfert	140
Création d'une clé publique de transfert	141
Menu Backup List (Liste des sauvegardes)	142
Affichage de l'historique des fichiers de sauvegarde	143
Affichage d'informations détaillées sur une sauvegarde	146
Restauration d'une sauvegarde	148
Menu System Dump (Vidage système)	150
Création d'un vidage système	150
Menu Security Parameters (Paramètres de sécurité)	152
Récupération des paramètres de sécurité	152
Modification des paramètres de sécurité	154
Sécurité principale	155
Menu Core Security (Sécurité principale)	156
Backup Core Security (Sauvegarder la sécurité principale)	157
Création d'une sauvegarde de sécurité principale	157
Key Split Configuration (Configuration de scissions de clé)	159
Affichage de la configuration de scissions de clé	159
Modification de la configuration de scissions de clé	161
Autonomous Unlock Option (Option de déverrouillage autonome)	163
Menu Local Configuration (Configuration locale)	165
Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA)	166
Verrouillage du KMA	166
Déverrouillage du KMA	167
Menu System Time (Heure système)	170
Récupération des informations sur l'horloge locale	170
Réglage de l'horloge locale du KMA	172

<b>6. Tâches du responsable de la conformité</b>	<b>173</b>
Rôle Compliance Officer (Responsable de la conformité)	174
Stratégies de clés	175
Menu Key Policy List (Liste des stratégies de clés)	175
Affichage des stratégies de clés	176
Création d'une stratégie de clés	180
Affichage/Modification d'une stratégie de clés	182
Suppression d'une stratégie de clés	183
Groupes de clés	184
Menu Key Groups (Groupes de clés)	186
Menu Key Group List (Liste des groupes de clés)	186
Affichage des groupes de clés	187
Création d'un groupe de clés	190
Affichage/Modification des détails d'un groupe de clés	192
Suppression d'un groupe de clés	193
Menu Agent Assignment to Key Groups (Assignment d'un agent à des groupes de clés)	194
Assignment d'un agent à un groupe de clés	196
Suppression d'un agent dans un groupe de clés	198
Menu Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent)	200
Assignment d'un groupe de clés à un agent	203
Suppression d'un groupe de clés pour un agent	205
Menu Key Group Assignment to Transfer Partners (Assignment d'un groupe de clés à un partenaire de transfert)	207
Affichage des assignments de groupes de clés	208
Ajout d'un groupe de clés à un partenaire de transfert	209
Suppression d'un groupe de clés d'un partenaire de transfert	210
Menu Transfer Partner Assignment to Key Groups (Assignment d'un partenaire de transfert à des groupes de clés)	211
Affichage des assignments de groupes de transfert	212
Ajout d'un partenaire de transfert à un groupe de clés	213
Suppression d'un partenaire de transfert d'un groupe de clés	214
Importation d'un fichier d'exportation de clés KMS 1.0	215

Menu Audit Event List (Liste des événements d'audit)	216
Affichage des journaux d'audit	216
Affichage des détails du journal d'audit	221
Exportation d'un journal d'audit	222
Menu Data Units (Unités de données)	223
Autres fonctions	224
<b>7. Tâches de l'opérateur</b>	<b>225</b>
Rôle Operator (Opérateur)	225
Menu Key Groups (Groupes de clés)	226
Key Group List (Liste des groupes de clés)	226
Agent Assignment to Key Groups (Assignment d'un agent à des groupes de clés)	226
Transfer Partner Assignment to Key Groups (Assignment d'un partenaire de transfert à des groupes de clés)	226
Menu Agent List (Liste des agents)	227
Affichage de la liste des agents	228
Création d'un agent	231
Affichage/Modification d'un agent	234
Définition de la phrase de passe d'un agent	235
Suppression d'un agent	236
Menu Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent)	237
Menu Import Keys (Importer des clés)	238
Unités de données	240
Menu Data Unit List (Liste des unités de données)	240
Affichage des unités de données	241
Affichage/Modification des informations détaillées sur une unité de données	245
Destruction des clés post-opérationnelles	251
Menu Software Upgrade (Mise à niveau du logiciel)	252
Téléchargement et application d'une mise à niveau logicielle	252
Menu Backup List (Liste des sauvegardes)	254
Menu Audit Event List (Liste des événements d'audit)	254
Menu KMA List (Liste des KMA)	254

Menu Site List (Liste des sites)	254
Menu SNMP Manager List (Liste des gestionnaires SNMP)	254
Menu System Time (Heure système)	254
Menu Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA)	254
<b>8. Tâches du responsable des sauvegardes</b>	<b>255</b>
Rôle Backup Operator (Opérateur des sauvegardes)	255
Menu Backup List (Liste des sauvegardes)	255
Affichage de l'historique des fichiers de sauvegarde	256
Affichage d'informations détaillées sur une sauvegarde	257
Création d'une sauvegarde	259
Confirmation d'une destruction de sauvegarde	260
Autres fonctions	261
<b>9. Tâches du responsable des audits</b>	<b>263</b>
Rôle Auditor (Responsable des audits)	263
Menu Audit List (Liste des audits)	263
Menu Security Parameters (Paramètres de sécurité)	263
Autres fonctions	264
<b>10. Utilisation de la console KMS</b>	<b>265</b>
Présentation de la console KMS	265
Connexion au KMA	266
Operator (Opérateur)	267
Security Officer (Responsable de la sécurité)	268
Autres rôles	269
Fonctions du rôle Operator (Opérateur)	270
Redémarrage du KMA	271
Arrêt du KMA	271
Activation du compte de support technique	272
Désactivation du compte de support technique	273
Désactivation de l'administrateur principal	274
Définition de la disposition du clavier	275
Déconnexion	276

Fonctions du rôle Security Officer (Responsable de la sécurité)	277
Connexion du KMA au cluster	278
Définition de la phrase de passe d'un utilisateur	280
Définition des adresses IP du KMA	281
Réinitialisation de l'état par défaut défini en usine du KMA	284
Activation du compte de support technique	286
Désactivation du compte de support technique	288
Activation de l'administrateur principal	289
Désactivation de l'administrateur principal	290
Définition de la disposition du clavier	291
Déconnexion	292
Fonctions associées aux autres rôles	293
Définition de la disposition du clavier	294
Déconnexion	295

<b>Glossaire</b>	<b>297</b>
------------------	------------

<b>Index</b>	<b>307</b>
--------------	------------



# Figures

---

FIGURE 1-1	Connexions établies avec le KMA	3
FIGURE 1-2	Périodes de cycle de vie des clés	4
FIGURE 1-3	Diagramme des transitions d'état	5
FIGURE 1-4	Déploiement standard de la solution KMS	12
FIGURE 2-1	Écran de connexion d'ELOM	22
FIGURE 2-2	Contrôle de l'alimentation	23
FIGURE 6-1	Relations entre les groupes de clés, les stratégies de clés, les agents et les unités de données	185



# Tableaux

---

TABLEAU 1-1	Opérations système/Rôles d'utilisateur	14
TABLEAU 2-1	Navigateurs Web et versions Java compatibles	21



# Préface

---

---

## Public cible

Ce guide fournit des informations de configuration et d'administration relatives au logiciel Sun Microsystems StorageTek™ Crypto Key Management System (KMS). Il s'adresse aux administrateurs d'espace de stockage, aux programmeurs système et aux opérateurs chargés de la configuration et de la maintenance du logiciel KMS sur leur site.

---

## Organisation de ce guide

Ce guide comprend les chapitres suivants :

- Introduction
- Démarrage
- Utilisation de KMS Manager
- Utilisation du menu System (Système)
- Tâches du responsable de la sécurité
- Tâches du responsable de la conformité
- Tâches de l'opérateur
- Tâches du responsable des sauvegardes
- Tâches du responsable des audits
- Utilisation de la console KMS

Un index et un glossaire sont également inclus.

## Informations supplémentaires

Sun Microsystems, Inc. (Sun) vous propose diverses méthodes pour obtenir des informations supplémentaires.

### Site Web externe de Sun

Le site Web externe de Sun contient des informations d'ordre commercial, de même que sur les produits, les événements, les entreprises et les services. Le site Web externe est accessible pour toute personne disposant d'un navigateur Web et d'une connexion Internet.

L'URL du site Web externe de Sun est : <http://www.sun.com>

L'URL des informations spécifiques à la marque Sun StorageTek™ est :  
<http://www.sun.com/storagetek>

### Centre des ressources client (CRC)

Le centre des ressources client (CRC, Customer Resource Center) des produits Sun StorageTek est un site Web permettant à ses membres de résoudre des problèmes techniques en recherchant des correctifs de code et de la documentation technique concernant les produits de marque StorageTek. L'adhésion au CRC vous donne droit à d'autres services proactifs, tels que les abonnements HIPER, les astuces techniques, les réponses aux questions fréquemment posées (FAQ, foire aux questions), les addenda aux documentations des produits et les coordonnées des services d'assistance produits en ligne. Les clients disposant d'une garantie ou d'un contrat de service de maintenance en cours peuvent devenir membres du site en cliquant sur le bouton Request Password (Demander un mot de passe) de la page d'accueil du CRC. Le personnel de Sun peut accéder au CRC via le portail SunWeb PowerPort.

L'URL du CRC est : <http://www.support.storagetek.com>

### Site des partenaires

Le site Web StorageTek Partners est destiné aux entreprises disposant d'un contrat de partenariat StorageTek. Ce site contient des informations sur les produits, les services, le support client, les événements à venir, les programmes de formation et les outils d'aide à la vente destinés à assister les partenaires StorageTek. L'accès à ce site est restreint au-delà de la page de connexion. Sur la page Partners Login (Connexion des partenaires), le personnel et les partenaires actuels de Sun n'ayant pas encore accès au site peuvent demander un ID et un mot de passe de connexion tandis que des partenaires potentiels peuvent déposer leur candidature pour devenir revendeurs StorageTek.

L'URL des partenaires disposant d'un contrat de partenariat avec Sun est :  
<http://www.sun.com/partners/>

## Sites Web tiers

Sun ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce document. Sun décline toute responsabilité quant au contenu, à la publicité, aux produits ou tout autre matériel disponibles dans ou par l'intermédiaire de ces sites ou ressources. Sun ne pourra en aucun cas être tenu responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.

## Publications imprimées

Contactez un représentant du service des ventes ou du service marketing de Sun pour commander des exemplaires imprimés de cette publication ou toute autre publication client attrayant à des produits StorageTek au format papier.

## Support client

Le support client est disponible 24 heures sur 24, tous les jours de la semaine, pour les clients possédant des contrats de maintenance Sun ou StorageTek et les employés de Sun. Vous trouverez des informations supplémentaires sur le support client sur le site Web du centre de ressources client (CRC) à l'adresse :  
<http://www.support.storagetek.com>

## Maintenance demandée par le client

La maintenance demandée par le client commence par un appel de votre part au service d'assistance de Sun Microsystems pour StorageTek. Vous êtes directement mis en relation avec un membre qualifié du personnel de Sun qui enregistre les informations relatives à votre problème et y répond au moyen du niveau de support adéquat.

Pour contacter le support de Sun Microsystems pour StorageTek concernant un problème :

1. Composez le numéro de téléphone suivant :

**☎ 800.872.4786 (1.800.USA.4SUN)** (depuis les États-Unis)

**☎ 800.722.4786** (depuis le Canada)

Si vous résidez ailleurs, rendez-vous sur

<http://www.sun.com/service/contacting/solution.html>

pour rechercher le numéro de téléphone de votre pays.

2. Décrivez le problème à votre interlocuteur. Celui-ci vous posera plusieurs questions afin de rediriger votre appel ou d'envoyer un technicien sur place.

Vous faciliterez le processus en ayant à portée de main les informations suivantes lors d'un appel au service d'assistance :

---

Nom du compte	_____
Numéro d'emplacement du site	_____
Nom du contact	_____
Numéro de téléphone	_____
Numéro du modèle de l'équipement	_____
Adresse du périphérique	_____
Numéro de série du périphérique (si connu)	_____
Urgence du problème	_____
Code du symptôme de la panne (FSC)	_____
Description du problème	_____
	_____
	_____
	_____

---

## Sièges internationaux de Sun

Vous pouvez contacter n'importe quel siège international de Sun pour évoquer les solutions complètes de stockage, de services et d'assistance disponibles pour votre entreprise. Vous trouverez les adresses et numéros de téléphone correspondants sur le site Web externe de Sun à l'adresse :  
<http://www.sun.com/worldwide/>

## Publications connexes

Les publications suivantes contiennent des informations complémentaires sur des sujets spécifiques liés à l'utilisation du logiciel Key Management System (KMS) :

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

---

# Conventions de lisibilité

## Noms des produits

KMS fait référence à l'implémentation 2.0 du logiciel Sun StorageTek™ Crypto Key Management System.

## Conventions typographiques

Ce guide contient des exemples en *italique*. Les caractères en italique indiquent des variables. Vous devez remplacer ces variables par des valeurs réelles.

L'utilisation mixte de caractères en majuscules et en minuscules pour les noms de commandes, les ordres de contrôle et les paramètres signifie que les lettres en minuscules peuvent être omises afin de former des abréviations. Par exemple, vous pouvez tout simplement taper POL afin d'exécuter la commande POLicy.

## Messages d'alerte

Les messages d'alerte sont destinés à attirer votre attention sur des informations particulièrement importantes ou ayant un rapport unique avec le texte ou l'illustration principal(e).

---

**Avertissement** – Informations destinées à vous empêcher d'endommager le matériel ou les logiciels.

---

---

**Attention** – Informations destinées à vous empêcher d'endommager les données.

---

---

**Conseil** – Informations pouvant servir à raccourcir ou à simplifier la tâche en cours ou pouvant tenir lieu de rappel.

---

---

**Remarque** – Informations pouvant présenter un intérêt particulier pour vous. Les remarques servent également à indiquer des exceptions à une règle ou une procédure donnée.

---



# Introduction

---

---

## Présentation

Le logiciel Crypto Key Management System (KMS) permet de créer, stocker et gérer des clés de chiffrement. Il comprend les composants suivants :

- Dispositif de gestion des clés (KMA, Key Management Appliance) : boîtier de sécurisation fournissant des services de gestion des clés du cycle de vie s'appuyant sur des stratégies, d'authentification, de contrôle d'accès et de provisioning de clés. En tant qu'autorité de confiance en matière de réseaux de stockage, le KMA s'assure que tous les périphériques de stockage sont enregistrés et authentifiés, et que toutes les opérations de création, de provisioning et de suppression de clés de chiffrement sont conformes aux stratégies indiquées.
- IG de KMS Manager : interface graphique exécutée sur une station de travail et permettant de communiquer avec le KMA par le biais d'un réseau IP en vue de configurer et de gérer le KMS. L'IG de KMS Manager doit être installée sur une station de travail fournie par le client.
- Cluster KMS : ensemble complet des KMA du système. Ces différents KMA sont conscients les uns des autres et les informations des uns sont répliquées sur tous les autres.
- Agent : périphérique ou logiciel effectuant les opérations de chiffrement au moyen des clés gérées par le cluster KMS. Pour la version 2.0 du logiciel KMS, il s'agit des lecteurs de bande de chiffrement StorageTek. Les agents communiquent avec les KMA par le biais de l'API de l'agent. Il s'agit d'un ensemble d'interfaces logicielles intégrées au logiciel ou au matériel de l'agent.

# Concepts du logiciel KMS

## Cluster KMS

KMS prend en charge le clustering de plusieurs KMA, fonction offrant l'équilibrage de charge et le basculement. Tous les dispositifs de gestion des clés d'un cluster KMS agissent selon un principe actif/actif. Ils peuvent fournir toutes les fonctionnalités à n'importe quel agent. Les actions réalisées sur un KMA sont immédiatement répliquées sur tous les autres dispositifs du cluster.

## Agents

Les agents effectuent des opérations de chiffrement ; plus particulièrement, en les chiffrant lors de leur écriture et en les déchiffrant à mesure de leur lecture. Les agents contactent le cluster KMS afin de créer et de récupérer les clés utilisées pour procéder au chiffrement.

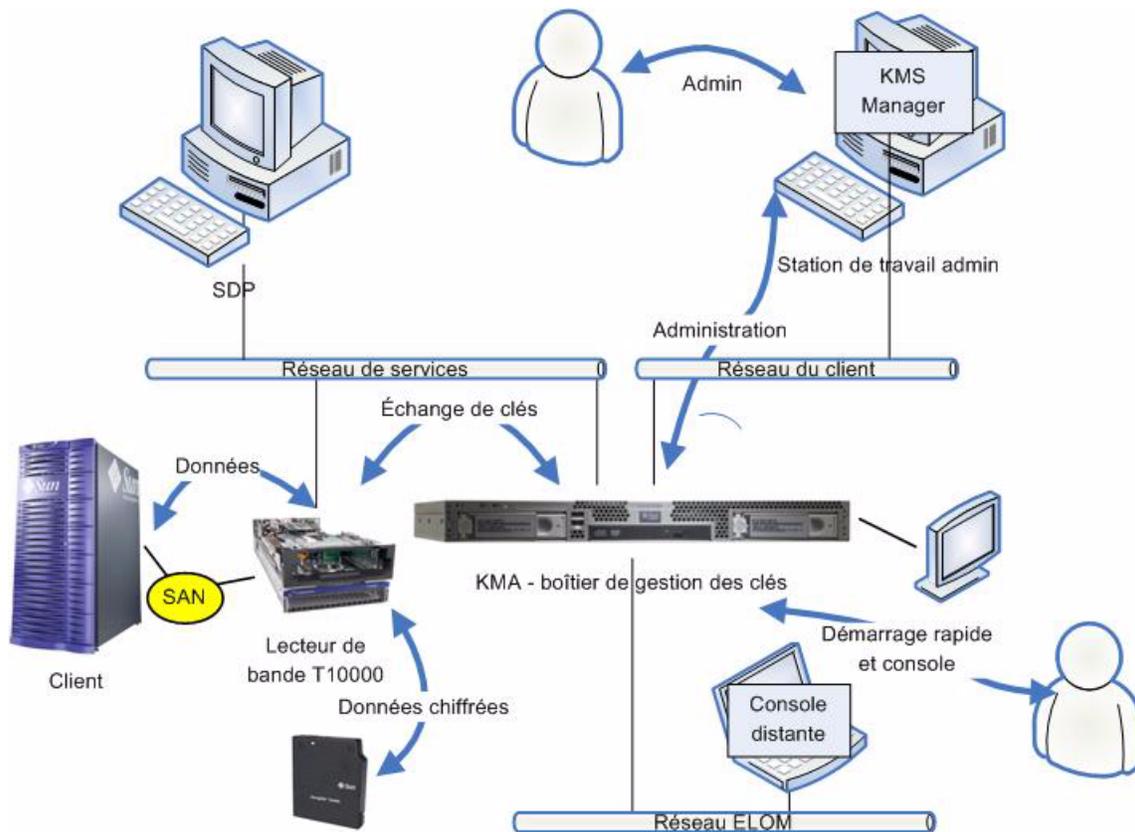
## Connexions réseau

Le logiciel KMS utilise la gestion de réseaux TCP/IP pour établir les connexions entre les KMA, les agents et les machines exécutant l'IG de KMS Manager. Afin de fournir des connexions réseau flexibles, deux interfaces sont disponibles à cet effet sur le KMA :

- la connexion de gestion, prévue pour les connexions au réseau du client ;
- la connexion aux services, prévue pour les connexions aux lecteurs de bande.

Dans le cadre de l'installation KMA de production, es kits d'accessoires de bibliothèques comprenant des commutateurs et des câbles sont disponibles pour les connexions aux unités et au KMA, comme l'illustre la [FIGURE 1-1](#).

**FIGURE 1-1** Connexions établies avec le KMA



## Configuration initiale - Connexion directe ou console distante (ELOM)

La configuration initiale des KMA est effectuée via la connexion à la console. Pour ce faire, vous pouvez vous servir d'un moniteur et d'un clavier reliés directement au KMA ou utiliser la fonction de console distante du gestionnaire ELOM (ELOM, Embedded Lights Out Manager). ELOM permet d'établir des connexions à distance avec la console afin que vous puissiez exécuter des fonctions serveur.

La fonction de console distante d'ELOM nécessite une troisième connexion réseau, intitulée « Réseau ELOM » dans la [FIGURE 1-1](#). Vous devez configurer l'adresse IP d'ELOM de la manière décrite plus loin dans ce document afin de pouvoir vous servir de la fonction de console distante.

---

**Remarque** – Plus généralement, le réseau ELOM sera identique à celui du client.

---

## Configuration initiale - programme QuickStart

Lors de la mise sous tension d'un KMA réglé sur l'état par défaut défini en usine, une fonction d'assistant intitulée QuickStart (Démarrage rapide) est exécutée sur la console à des fins de configuration initiale. Cela fait, la plupart des autres fonctions sont disponibles à partir de l'IG de KMS Manager. Une interface de console de fonctions limitée reste active pour un jeu limité de fonctions.

## Cycle de vie des clés

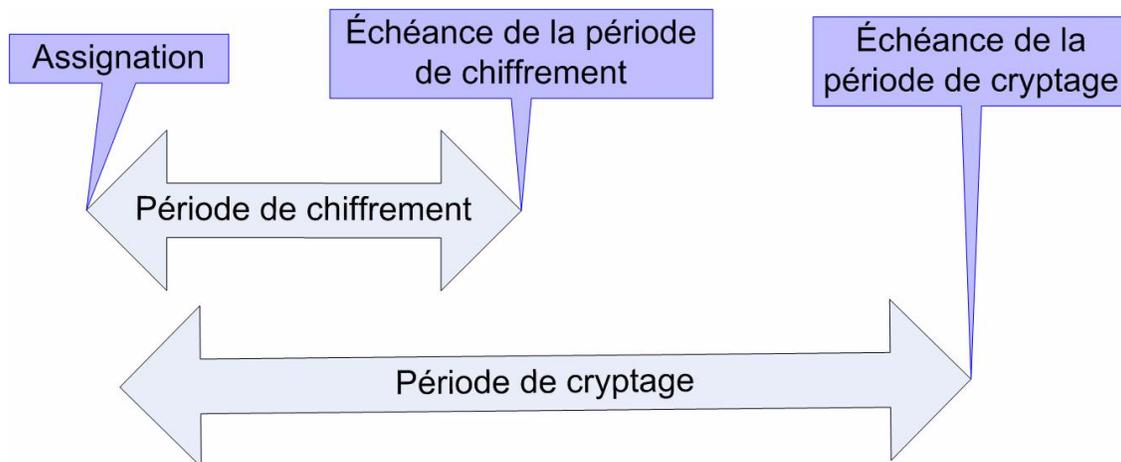
Les clés suivent un cycle de vie reposant sur la stratégie de clés en vigueur. Le cycle de vie imposé par KMS est basé sur les directives NIST 800-57. Quelques états supplémentaires ont été ajoutés afin de gérer les nuances du logiciel KMS.

Le cycle de vie des clés est calculé d'après deux périodes temporelles (voir [FIGURE 1-2](#)) définies dans les stratégies de clés :

- durée d'utilisation du chiffrement ;
- durée de validité du chiffrement.

La durée d'utilisation du chiffrement correspond à la période pendant laquelle une clé peut servir à chiffrer des données une fois qu'elle a été assignée. La durée de validité du chiffrement, elle, désigne la période pendant laquelle la clé peut être utilisée à des fins de déchiffrement. Les deux périodes sont supposées débiter au même moment, lors de l'assignation de la clé.

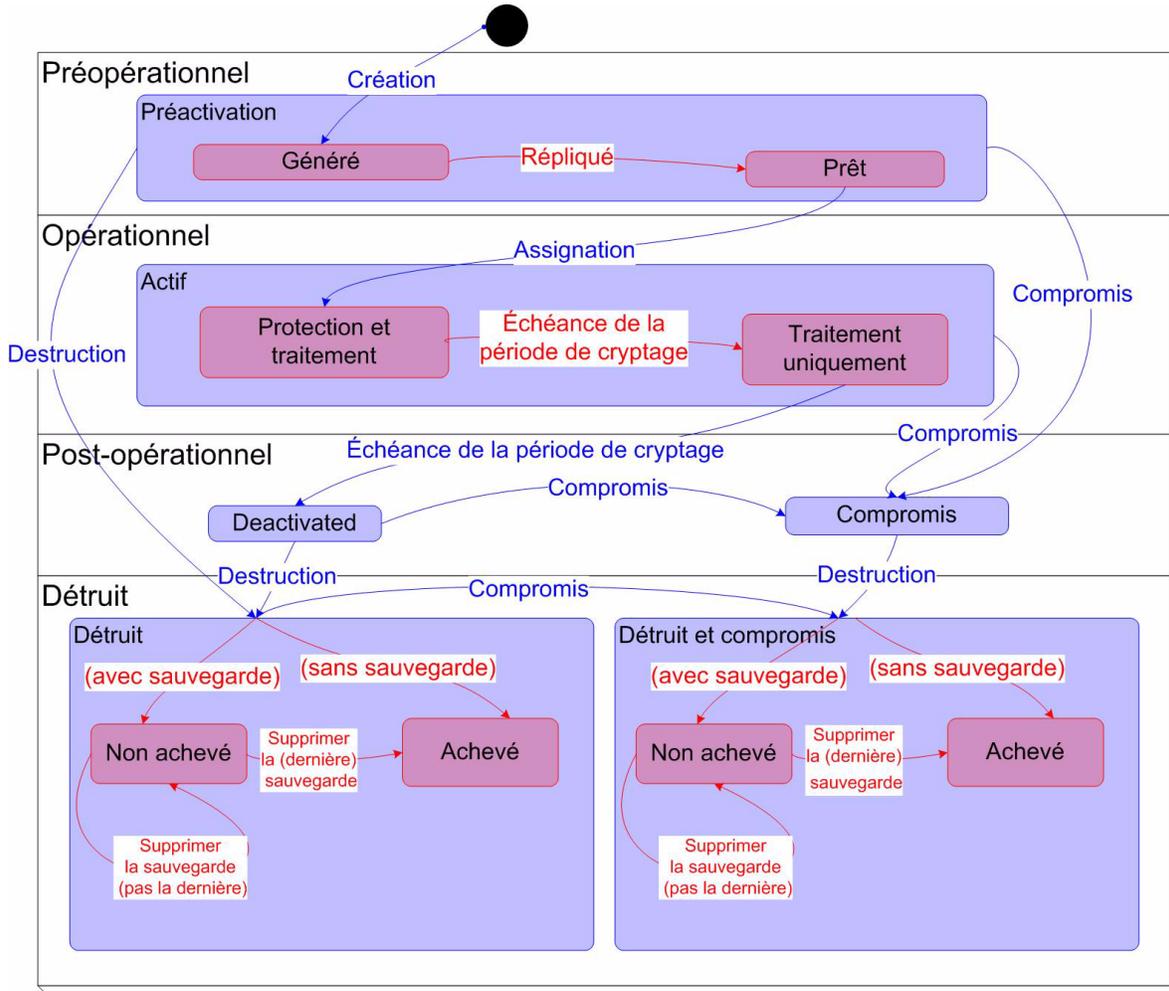
**FIGURE 1-2** Périodes de cycle de vie des clés



# Transition d'état

Ces durées d'utilisation et de validité du chiffrement, combinées à d'autres fonctions du KMS, définissent une transition d'état pour les clés comme l'illustre la [FIGURE 1-3](#). Dans ce diagramme, les états et les transitions affichés en bleu sont définis par la spécification NIST 800-57.

FIGURE 1-3 Diagramme des transitions d'état



## États et transitions disponibles dans le logiciel KMS

Dans la [FIGURE 1-3](#), les états et les transitions signalés en rouge sont ajoutés par KMS. Lors de l'examen des clés dans KMS Manager, seul l'état interne est indiqué. Les états disponibles dans le logiciel KMS sont présentés ci-dessous.

### Préactivation

La clé a été générée, mais n'est pas encore disponible à des fins d'utilisation. Dans l'état préactivé, le logiciel KMS ajoute deux états détaillés supplémentaires, Generated (Généré) et Ready (Prêt).

#### *Generated (Généré)*

Une clé générée est une clé qui a été créée sur un KMA faisant partie d'un cluster. Elle reste générée tant qu'elle n'est pas répliquée sur au moins un autre KMA dans le cadre d'un cluster composé de plusieurs dispositifs de gestion des clés. Dans un cluster comprenant un seul KMA, vous devez enregistrer une clé dans au moins une sauvegarde pour pouvoir quitter l'état Generated (Généré).

#### *Ready (Prêt)*

Une clé prête est une clé qui a été protégée contre la perte grâce à la réplication ou à une sauvegarde. Une clé définie sur cet état est disponible pour l'assignation. La transition vers l'état Replicated (Répliqué) survient lors de la réplication ou (dans le cas d'un cluster comprenant un seul KMA) de la sauvegarde.

### Active (Actif)

Il est possible d'utiliser la clé en vue de protéger des informations (c.-à-d., de les chiffrer) ou de traiter des informations protégées au préalable (c.-à-d., de les déchiffrer). D'après NIST, une clé active peut servir exclusivement à des fins de protection, de traitement ou de protection et de traitement. En outre, l'organisme de normalisation indique clairement que dans le cas des clés de chiffrement de données symétriques, une clé peut être utilisée pendant une période spécifique pour protéger et traiter des informations, mais qu'une fois ce laps de temps écoulé, la clé peut uniquement servir à des fins de traitement.

L'état actif disponible dans le logiciel KMS comprend deux sous-états. Ces états sont décrits par le NIST, mais ils ne sont pas spécifiquement identifiés en tant qu'états.

#### *Protect-and-process (Protection et traitement)*

Une clé définie dans cet état peut servir à des fins de chiffrement et de déchiffrement. Cet état est appliqué aux clés lors de leur assignation. L'assignation se produit suite à la demande de création d'une nouvelle clé par un agent de chiffrement.

### *Process only (Traitement seul)*

Une clé définie dans cet état permet de déchiffrer des données, mais pas d'en chiffrer. Lorsqu'un agent détecte l'absence de clés définies sur l'état de protection et traitement (par ex., pour une unité de données spécifique en cours de lecture ou d'écriture), il devrait créer une nouvelle clé. Les clés passent de l'état de protection et traitement à l'état de traitement seul lorsque la période de chiffrement arrive à échéance.

### Deactivated (Désactivé)

La durée de validité du chiffrement-clé de cette clé est dépassée mais celle-ci est peut-être encore nécessaire pour traiter (déchiffrer) des informations. Le NIST indique clairement que les clés définies dans cet état peuvent servir à traiter des données.

À strictement parler, les directives du NIST indiquent que si des clés post-opérationnelles (clés désactivées et comprimées comprises) doivent rester accessibles, il est préférable de les archiver. Il s'agit d'un processus de récupération des clés permettant de rappeler des clés à partir d'une archive afin de pouvoir les réutiliser ultérieurement.

Le logiciel KMS fournit des archives sous la forme de sauvegardes de KMA mais il ne peut pas rappeler une clé spécifique à partir d'une sauvegarde. Par conséquent, il conserve des clés d'étapes post-opérationnelles dans le cluster KMS et les fournit sur demande à partir d'un agent.

### Compromised (Compromis)

Les clés sont compromises lorsqu'elles sont fournies à une entité non autorisée ou détectées par celle-ci. Les clés compromises ne doivent pas servir à protéger des informations, mais elles peuvent être utilisées afin de traiter des informations.

### Destroyed (Détruit)

Les clés détruites n'existent plus. Cependant, des informations associées peuvent être conservées. Dans KMS 2.0, les données sur les clés provenant de clés détruites sont supprimées du cluster KMS. Les clés détruites ne sont plus délivrées à un agent.

---

**Remarque** – La seule façon de détruire une clé consiste à passer par l'IG ou l'API de gestion.

---

Les directives du NIST ne semblent pas préconiser de méthode de destruction de clés en fonction du temps.

Dans les états Destroyed (Détruit) et Destroyed and Compromised (Détruit et compromis), le logiciel KMS définit deux sous-états. Ces états sont définis, car KMS ne contrôle pas les sauvegardes qu'il crée. L'administrateur d'un client doit informer le système de gestion des clés en cas de destruction d'une sauvegarde. Ce n'est qu'une fois toutes les copies de sauvegarde détruites qu'une clé peut être considérée comme réellement détruite. Ces sous-états sont Icomplete (Non achevé) et Complete (Achévé).

### *Incomplete (non achevé)*

Il existe encore au moins une sauvegarde contenant la clé détruite. Dans ce sous-état, la clé ne se trouve dans aucun KMA du cluster KMS. Il est impossible de délivrer des clés situées dans cet état à des agents.

### *Complete (Achévé)*

Toutes les sauvegardes contenant la clé ont été détruites. La clé ne se trouve dans aucun KMA et dans aucune sauvegarde. À strictement parler, des sauvegardes contenant la clé peuvent néanmoins encore exister. Tout ce que le logiciel KMS sait est qu'il a été informé que l'ensemble des sauvegardes a été intégralement détruit. Il en va de la responsabilité de l'utilisateur de s'assurer que ces copies de sauvegarde ont bien été détruites.

Il est bon de noter à nouveau que la transition vers l'état de destruction se produit uniquement suite à l'exécution d'une commande d'administration. En outre, il se peut qu'une clé soit délivrée à un agent de chiffrement alors qu'elle se trouve en phase post-opérationnelle (états Deactivated et Compromised). Cette interprétation est conforme aux descriptions de la phase post-opérationnelle du NIST. Les directives du NIST indiquent qu'une clé post-opérationnelle doit être détruite lorsqu'elle « n'est plus requise ». Nous pensons que seul l'utilisateur est apte à déterminer cette condition. Ainsi, seule une entité externe peut lancer la transition vers l'état Destroyed.

### **Destroyed and Compromised (Détruit et compromis)**

Il s'agit du même état que Destroyed, à ceci près que la clé a été compromise avant ou après sa destruction.

## Utilisateurs et contrôle d'accès basé sur les rôles

KMS vous offre la possibilité de définir plusieurs utilisateurs, chacun doté d'un ID propre et d'une phrase de passe. Chaque utilisateur se voit attribuer un ou plusieurs rôles prédéfinis. Ces rôles sont les suivants :

- Security Officer (Responsable de la sécurité) : se charge de la configuration et de la gestion du système de gestion des clés (KMS).
- Operation (Opérateur) : se charge de la configuration des agents et des opérations quotidiennes.
- Compliance officer (responsable de la conformité) : définit les groupes de clés et contrôle l'accès des agents aux groupes de clés.
- Backup operator (Opérateur des sauvegardes) : se charge des opérations de sauvegarde.
- Auditor (Responsable des audits) : permet d'afficher les pistes de vérification du système.

Lors du processus de démarrage rapide (QuickStart), un responsable de la sécurité est défini. Une fois le démarrage rapide terminé, il est possible de définir des utilisateurs supplémentaires via l'IG de KMS Manager.

### Opérations autorisées par rôle

La liste des fonctions autorisées par rôle est présentée dans le [TABLEAU 1-1, page 14](#).

Dans l'IG et la console, seules les opérations autorisées sont affichées. Il est possible qu'une opération soit affichée, puis qu'elle échoue lors d'une tentative d'exécution. Cela peut arriver lorsque des rôles associés à un utilisateur sont supprimés entre le moment où les informations sont affichées et celui où l'opération est tentée.

Tous les rôles à l'exception de celui du responsable des audits sont nécessaires pour créer un système de chiffrement opérationnel. Il est possible de créer des utilisateurs distincts, chacun d'un rôle unique. Autre possibilité, plusieurs rôles sont assignés à un même utilisateur.

### Protection par quorum

KMS offre également une fonction de protection par quorum pour certaines opérations. Il est possible de définir un quorum de 10 utilisateurs au maximum. Un seuil compris entre un et le nombre d'utilisateurs du quorum est également spécifié. Ces informations sont appelées références fractionnées de clés. Ne confondez pas les ID utilisateur et les phrases de passe des ID utilisateur et phrases de passe servant à se connecter au système. Lors d'une tentative d'opération nécessitant l'approbation d'un quorum, un écran s'affiche pour permettre à chaque utilisateur du quorum de saisir son ID et sa phrase de passe. L'opération sera autorisée uniquement lorsque le nombre minimum d'ID utilisateur et de phrases de passe (le seuil) sera atteint.

## Unités de données, clés, groupes de clés et stratégies de clés

Les unités de données servent à représenter des données chiffrées par des agents. Pour les lecteurs de bande, une unité de données correspond à une cartouche de bande ; les unités de données sont toujours présentes. Il ne s'agit pas d'une condition requise fondamentale et les agents ultérieurs pourront fonctionner sans que des unités de données ne soient définies.

Les clés désignent les véritables valeurs de clés (données de clés) et les métadonnées associées.

Les stratégies de clés définissent les paramètres régissant les clés. Il s'agit notamment des paramètres de cycle de vie (période de chiffrement et période de cryptage) et d'exportation/importation (importation et exportation autorisées ou non.)

Les groupes de clés associent des clés et des stratégies de clés. Ils disposent d'une stratégie spécifique et sont assignés à des agents. Chaque agent est doté d'une liste de groupes de clés autorisés. Un agent peut uniquement récupérer les clés assignées à l'un des groupes de clés autorisés qui lui est assigné. Les agents disposent également d'un groupe de clés par défaut. Lorsqu'un agent crée une clé (plus particulièrement, lorsqu'il en assigne une à une unité de données), la clé est placée dans le groupe de clés par défaut de l'agent. Il existe une fonctionnalité permettant aux agents de contrôler les groupes de clés de manière plus sophistiquée. Cependant, les agents existants ne peuvent pas l'exploiter.

Pour que le système puisse fonctionner, assurez-vous qu'au moins une stratégie de clés et un groupe de clés sont définis. Le groupe de clés doit être assigné par défaut à tous les agents.

---

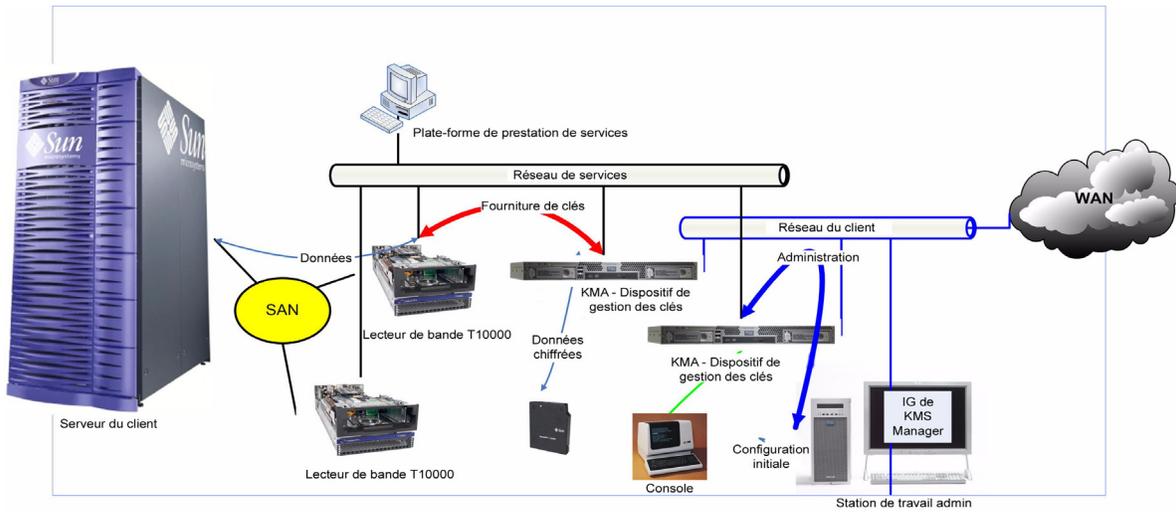
## Connexions TCP/IP et le KMA

Si un pare-feu est placé entre l'entité (indiquée à gauche) et le KMA, il doit autoriser l'entité à établir des connexions TCP/IP avec le KMA par le biais des ports suivants :

- Les communications KMS Manager/KMA nécessitent les ports 3331, 3332, 3333 et 3335.
- Les communications agent/KMA nécessitent les ports 3331, 3332, 3334 et 3335.
- Les communications KMA/KMA nécessitent les ports 3331, 3332 et 3336.

# KMS au sein du réseau

La **FIGURE 1-4** présente un déploiement standard de la solution KMS.



**FIGURE 1-4** Déploiement standard de la solution KMS

---

# Configuration logicielle requise de KMS Manager

Pour exécuter KMS Manager, vous devez disposer d'une station de travail fonctionnant sous Microsoft® Windows XP, Solaris 10 x86 Update 3 ou Solaris 10 x86 Update 4.

---

## Utilisation de l'aide en ligne

KMS Manager comprend une aide en ligne complète. Pour afficher la fenêtre d'aide sur n'importe quel écran de KMS Manager :

- cliquez sur le bouton **Help** (Aide) situé en haut du panneau de la fenêtre d'aide générale.

ou

- affichez un panneau soit en appuyant sur la touche **Tab** soit en cliquant n'importe où dans le panneau. Cliquez ensuite sur la touche **F1** pour afficher l'aide contextuelle.

---

## Contrôle d'accès basé sur les rôles

KMS définit les rôles suivants :

- **Security Officer (Responsable de la sécurité)** sécurité transfert.
- **Compliance Officer (Responsable de la conformité)** : gère les stratégies de clés et les groupes de clés, et détermine les agents et partenaires de transfert habilités à utiliser les groupes de clés.
- **Operator (Opérateur)** : gère les agents, les unités de données et les clés.
- **Backup Operator (Opérateur des sauvegardes)** : effectue les sauvegardes.
- **Auditor (Responsable des audits)** : affiche des informations sur le cluster KMS.

Un seul compte utilisateur KMA peut se voir assigner l'appartenance à un ou plusieurs rôles. Le KMA vérifie que l'entité de l'utilisateur ayant émis la requête est autorisé à exécuter une opération en fonction des rôles de l'utilisateur. Pour plus d'informations sur les rôles, reportez-vous à la section « [Connexion au KMA](#) », page 266.

## Opérations basées sur les rôles

Le **TABLEAU 1-1** affiche les opérations système autorisées pour chaque rôle d'utilisateur. Dans les sous-catégories de la colonne Rôles :

- **Oui** signifie que le rôle est habilité à effectuer l'opération.
- **Quorum** signifie que le rôle est habilité à effectuer l'opération sous réserve d'atteindre le quorum défini.
- **Vide** signifie que le rôle n'est pas habilité à effectuer l'opération.

**TABLEAU 1-1** Opérations système/Rôles d'utilisateur

Entité	Opération	Rôles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
Console						
	Se connecter	Oui	Oui	Oui	Oui	Oui
	Définir l'environnement linguistique du KMA	Oui				
	Définir l'adresse IP du KMA	Oui				
	Activer le support technique	Oui				
	Désactiver le support technique	Oui		Oui		
	Activer l'administrateur principal	Oui				
	Désactiver l'administrateur principal	Oui		Oui		
	Redémarrer le KMA			Oui		
	Arrêter le KMA			Oui		
	Consigner KMS dans le cluster	Quorum				
	Définir la phrase de passe de l'utilisateur	Oui				
	Réinitialiser le KMA	Oui				
	Mettre à zéro le KMA	Oui				
	Se déconnecter	Oui	Oui	Oui	Oui	Oui
Connexion						
	Se connecter	Oui	Oui	Oui	Oui	Oui
	Créer un profil	Oui	Oui	Oui	Oui	Oui
	Supprimer un profil	Oui	Oui	Oui	Oui	Oui
	Définir les paramètres de configuration	Oui	Oui	Oui	Oui	Oui
	Se déconnecter	Oui	Oui	Oui	Oui	Oui
Références fractionnées de clés						
	Lister	Oui				
	Modifier	Quorum				
Déverrouillage autonome						
	Lister	Oui				

**TABLEAU 1-1** Opérations système/Rôles d'utilisateur

Entité	Opération	Rôles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
	Modifier	Quorum				
Verrouiller/Déverrouiller le KMA						
	Lister le statut	Oui	Oui	Oui	Oui	Oui
	Verrouiller	Oui				
	Déverrouiller	Quorum				
Site						
	Créer	Oui				
	Lister	Oui		Oui		
	Modifier	Oui				
	Supprimer	Oui				
Paramètres de sécurité						
	Lister	Oui	Oui	Oui	Oui	Oui
	Modifier	Oui				
KMA						
	Créer	Oui				
	Lister	Oui		Oui		
	Modifier	Oui				
	Supprimer	Oui				
Utilisateur						
	Créer	Oui				
	Lister	Oui				
	Modifier	Oui				
	Modifier la phrase de passe	Oui				
	Supprimer	Oui				
Rôle						
	Lister	Oui				
Stratégie de clés						
	Créer		Oui			
	Lister		Oui			
	Modifier		Oui			
	Supprimer		Oui			

**TABLEAU 1-1** Opérations système/Rôles d'utilisateur

Entité	Opération	Rôles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
Groupe de clés						
	Créer		Oui			
	Lister		Oui	Oui		
	Lister les unités de données		Oui	Oui		
	Lister les agents		Oui	Oui		
	Modifier		Oui			
	Supprimer		Oui			
Agent						
	Créer			Oui		
	Lister		Oui	Oui		
	Modifier			Oui		
	Modifier la phrase de passe			Oui		
	Supprimer			Oui		
Assignation des agents/groupes de clés						
	Lister		Oui	Oui		
	Modifier		Oui			
Unité de données						
	Créer					
	Lister		Oui	Oui		
	Modifier			Oui		
	Modifier un groupe de clés		Oui			
	Supprimer					
Clés						
	Lister les clés des unités de données		Oui	Oui		
	Détruire			Oui		
	Compromettre		Oui			
Partenaires de transfert						
	Configurer	Quorum				
	Lister	Oui	Oui	Oui		
	Modifier	Quorum				
	Supprimer	Oui				
Clés de transfert						
	Lister	Oui				
	Mettre à jour	Oui				

**TABLEAU 1-1** Opérations système/Rôles d'utilisateur

Entité	Opération	Rôles				
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor
Assignations de groupes de clés pour les partenaires de transfert						
	Lister		Oui	Oui		
	Modifier		Oui			
Sauvegarde						
	Créer				Oui	
	Lister	Oui	Oui	Oui	Oui	
	Lister les sauvegardes avec clés détruites		Oui	Oui		
	Restaurer	Quorum				
	Confirmer les destructions				Oui	
Sauvegarde de sécurité principale						
	Créer	Oui				
Gestionnaire SNMP						
	Créer	Oui				
	Lister	Oui		Oui		
	Modifier	Oui				
	Supprimer	Oui				
Audit des événements						
	Afficher	Oui	Oui	Oui	Oui	Oui
	Afficher l'historique des agents		Oui	Oui		
	Afficher l'historique des unités de données		Oui	Oui		
	Afficher l'historique des clés d'unités de données		Oui	Oui		
Vidage système						
	Créer	Oui		Oui		
Heure système						
	Lister	Oui	Oui	Oui	Oui	Oui
	Modifier	Oui				
Serveur NTP						
	Lister	Oui	Oui	Oui	Oui	Oui
	Modifier	Oui				
Version du logiciel						
	Lister	Oui	Oui	Oui	Oui	Oui
	Mettre à niveau			Oui		

# Configuration et gestion du dispositif de gestion des clés (KMA)

Pour connaître les procédures d'installation et de configuration rapides de la solution KMS, reportez-vous au document *KMS 2.0 Installation and Service Manual*.

# Démarrage

---

Ce chapitre aborde les sujets suivants :

- démarrage du logiciel ELOM (Embedded Lights Out Manager) : ELOM établit une connexion à distance avec la console ;
- exécution du programme QuickStart : QuickStart est un utilitaire utilisé par un CSE pour configurer un nouveau KMA.

---

## Démarrage du logiciel ELOM (Embedded Light Out Manager)

Le système ELOM est équipé d'un processeur distinct de celui du serveur principal. Dès que le courant est mis (branché) et après une période de démarrage d'une à deux minutes, ELOM établit une connexion à distance avec la console, vous permettant d'exécuter des fonctions serveur telles que le programme *QuickStart*.

---

**Remarque** – Pour en savoir plus sur la configuration du serveur à l'aide des commandes de base d'ELOM, reportez-vous au document *KMA Installation and Service Manual*. Pour plus d'informations, consultez le document *Embedded Lights Out Manager Administration Guide*.

---

### Connexion au KMA

Connectez-vous au KMA via Embedded Lights Out Manager par l'une des méthodes suivantes :

- la connexion réseau (interface LAN 1 NET MGT d'ELOM), méthode conseillée ou
- le clavier et le moniteur reliés aux KMA.



**Les bloqueurs de fenêtres contextuelles** bloquent le lancement de Windows dans les procédures suivantes. Désactivez les bloqueurs de fenêtres contextuelles avant de commencer.

Si la fenêtre s'affiche non accompagnée d'une fenêtre de console, cela signifie que le navigateur Web ou la version Java dont vous disposez n'est pas compatible avec ELOM. Installez les dernières mises à niveau du navigateur et de Java. Reportez-vous au [TABLEAU 2-1](#) pour obtenir la liste des versions compatibles.

**TABLEAU 2-1** Navigateurs Web et versions Java compatibles

Système d'exploitation client	Environnement d'exécution Java (Java Web Start inclus)	Navigateurs Web
<ul style="list-style-type: none"> <li>■ Microsoft Windows XP Professionnel</li> </ul>	JRE 1.5 (Java 5.0 Update 7 ou version ultérieure)	<ul style="list-style-type: none"> <li>■ Internet Explorer 6.0 (ou version ultérieure) et Mozilla 1.7.5 (ou version ultérieure)</li> <li>■ Mozilla Firefox 1.0</li> </ul>
<ul style="list-style-type: none"> <li>■ Red Hat Linux 3.0 et 4.0</li> </ul>		<ul style="list-style-type: none"> <li>■ Mozilla 1.7.5 ou version ultérieure</li> <li>■ Mozilla Firefox 1.0</li> </ul>
<ul style="list-style-type: none"> <li>■ Solaris 9</li> <li>■ Solaris 10</li> <li>■ SUSE Linux 9.2</li> </ul>		<ul style="list-style-type: none"> <li>■ Mozilla 1.7.5</li> </ul>
Vous pouvez télécharger l'environnement d'exécution Java 1.5 sur : <a href="http://java.com">http://java.com</a> La version actuelle du guide d'ELOM se trouve à l'adresse : <a href="http://dlc.sun.com/">http://dlc.sun.com/</a> La documentation du serveur Sun Fire X2100 M2 est disponible à l'adresse : <a href="http://docs.sun.com/app/docs/coll/x2100m2">http://docs.sun.com/app/docs/coll/x2100m2</a>		

## Utilisation d'une connexion réseau

1. Lancez un navigateur Web à partir d'une autre station de travail connectée au réseau.
2. Connectez-vous au logiciel ELOM du KMA via l'adresse IP ou le nom d'hôte du LAN 1 (NET MGT), l'adresse que vous venez de configurer.

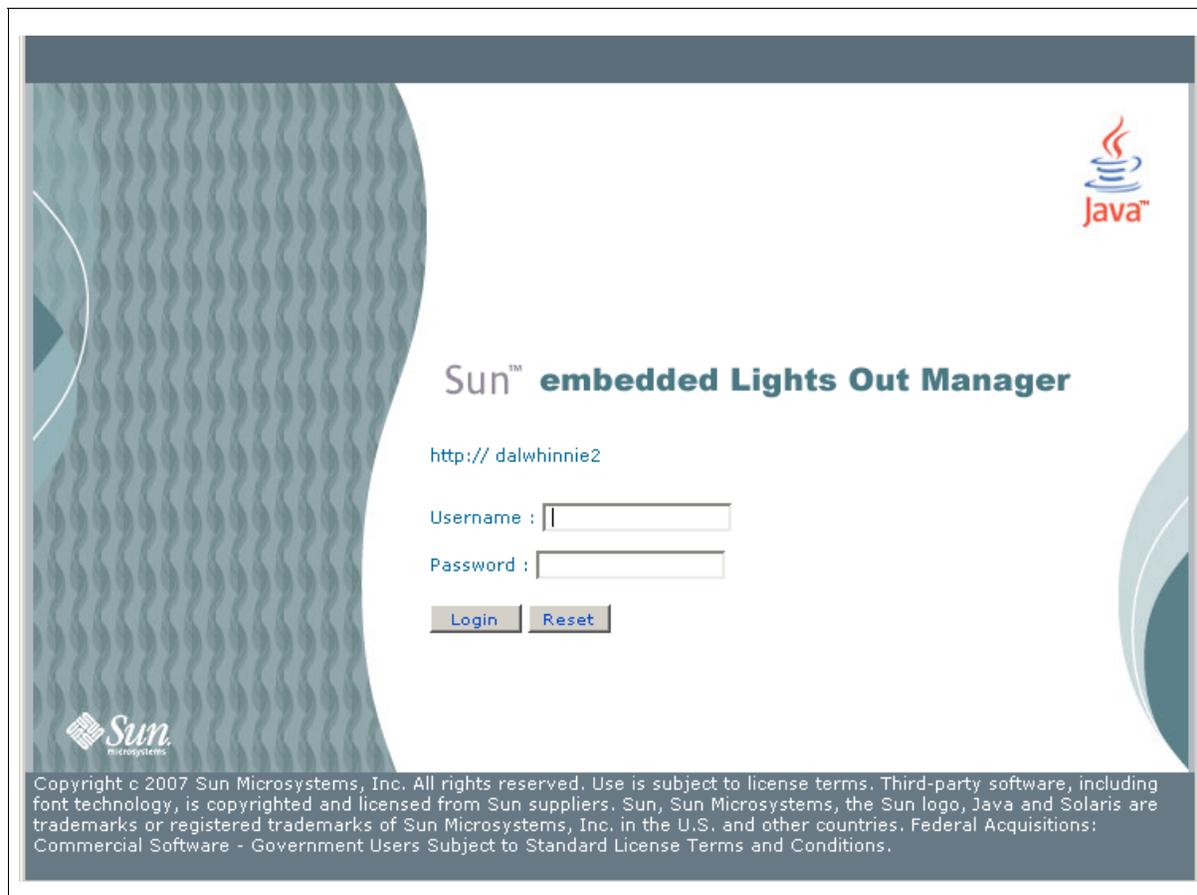
---

**Remarque** – Étant donné que le certificat d'ELOM ne correspondra pas au nom ou à l'adresse IP assigné(e), votre navigateur Web affichera plusieurs messages d'avertissement.

---

3. Cliquez sur OK ou sur Oui afin de contourner ces avertissements.  
Cela fait, l'invite de connexion d'ELOM s'affiche.

FIGURE 2-1 Écran de connexion d'ELOM



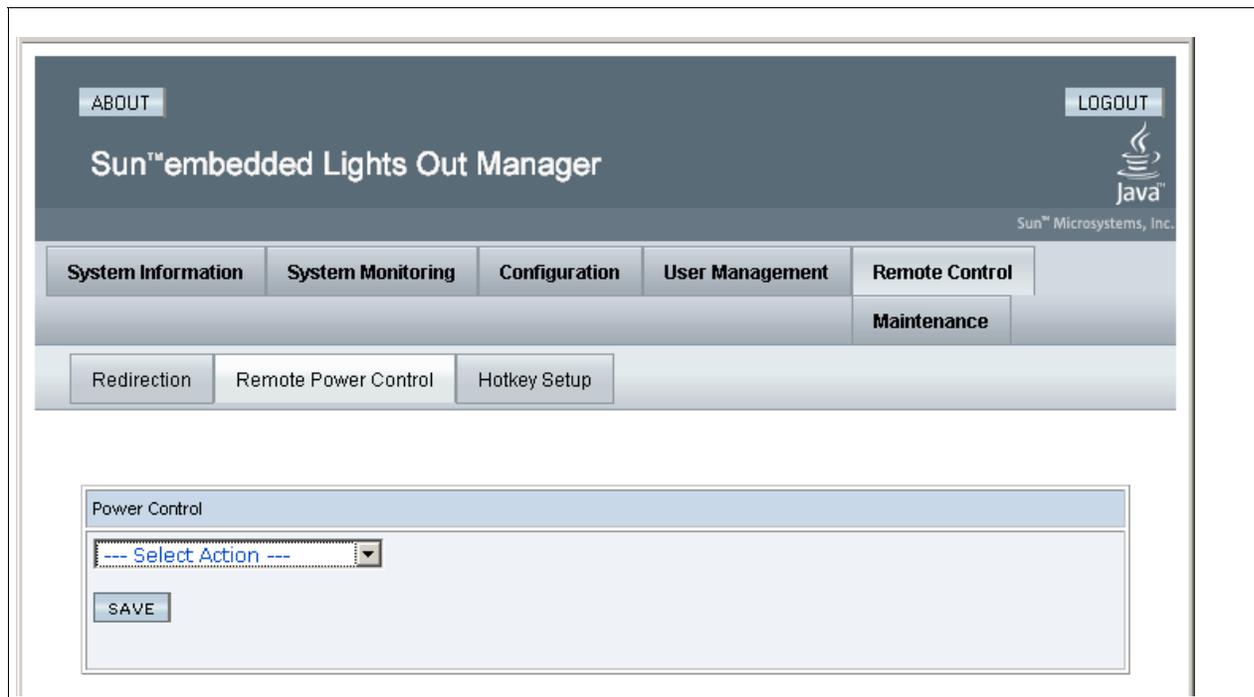
4. Connectez-vous en utilisant les informations suivantes :  
username = root  
Password = changeme

L'écran suivant est celui du gestionnaire. Si le serveur vient d'être branché et qu'il n'est pas encore sous tension, il n'aura pas terminé l'initialisation du système.

Les KMA sont configurés de manière à démarrer automatiquement lors de leur mise sous tension initiale. Ils doivent être initialisés à partir de l'invite de l'application QuickStart quelques minutes après leur mise sous tension.

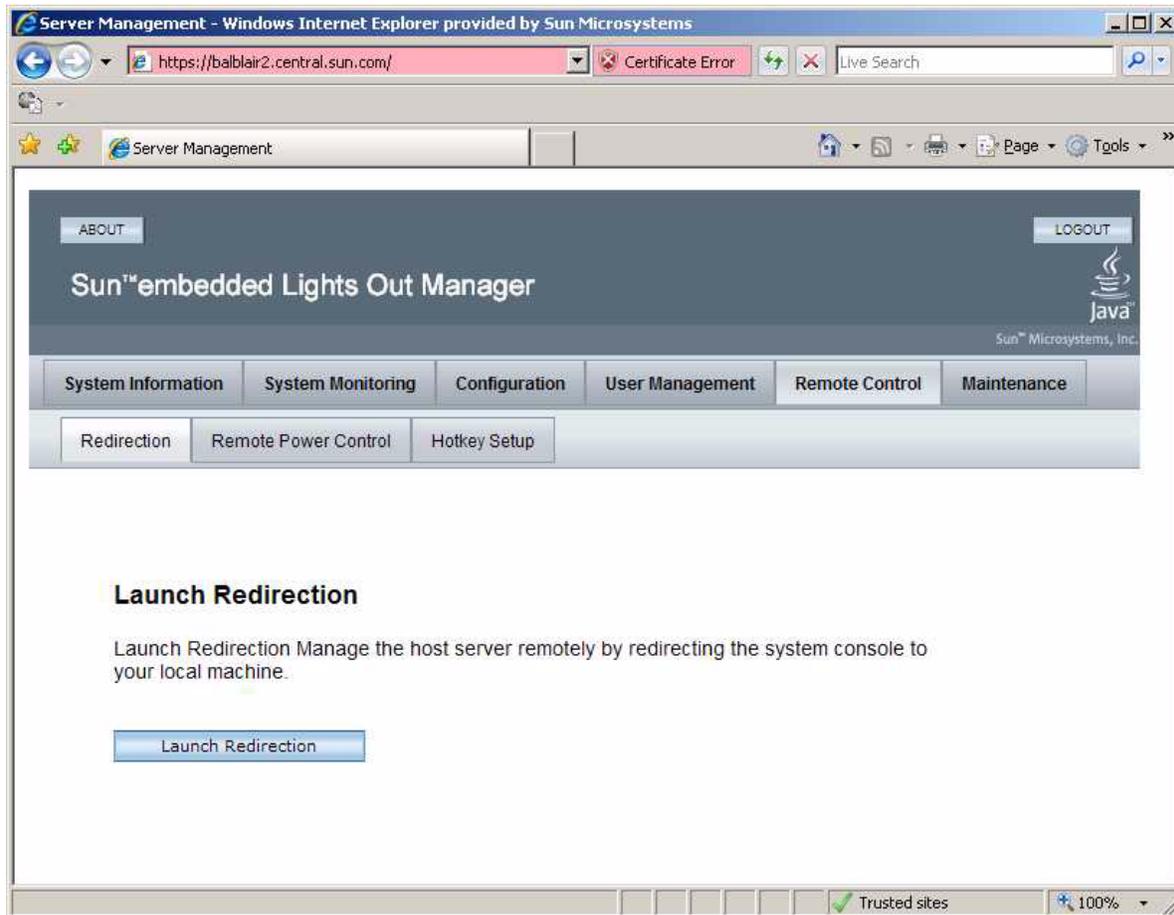
5. Vérifiez le statut de l'alimentation en cliquant sur l'onglet **System Monitoring** (Contrôle du système).  
Le statut de l'alimentation est indiqué dans le tableau.
6. Si l'option Power Status (Statut de l'alimentation) indique power off (Hors tension), cliquez sur l'onglet **Remote Control** (Contrôle à distance) situé à l'extrémité droite de la première rangée d'onglets.
7. Cliquez sur l'onglet **Remote Power Control** (Contrôle à distance de l'alimentation) disponible sur la deuxième rangée d'onglets.
8. Dans le menu déroulant Select Action (Sélectionner une action), choisissez **Power On** (Mettre sous tension), puis cliquez sur le bouton **Save** (Enregistrer).  
La mise sous tension du KMA commence. Ce processus prend quelques minutes, mais cela ne vous empêche nullement de poursuivre la configuration du KMA.

FIGURE 2-2 Contrôle de l'alimentation



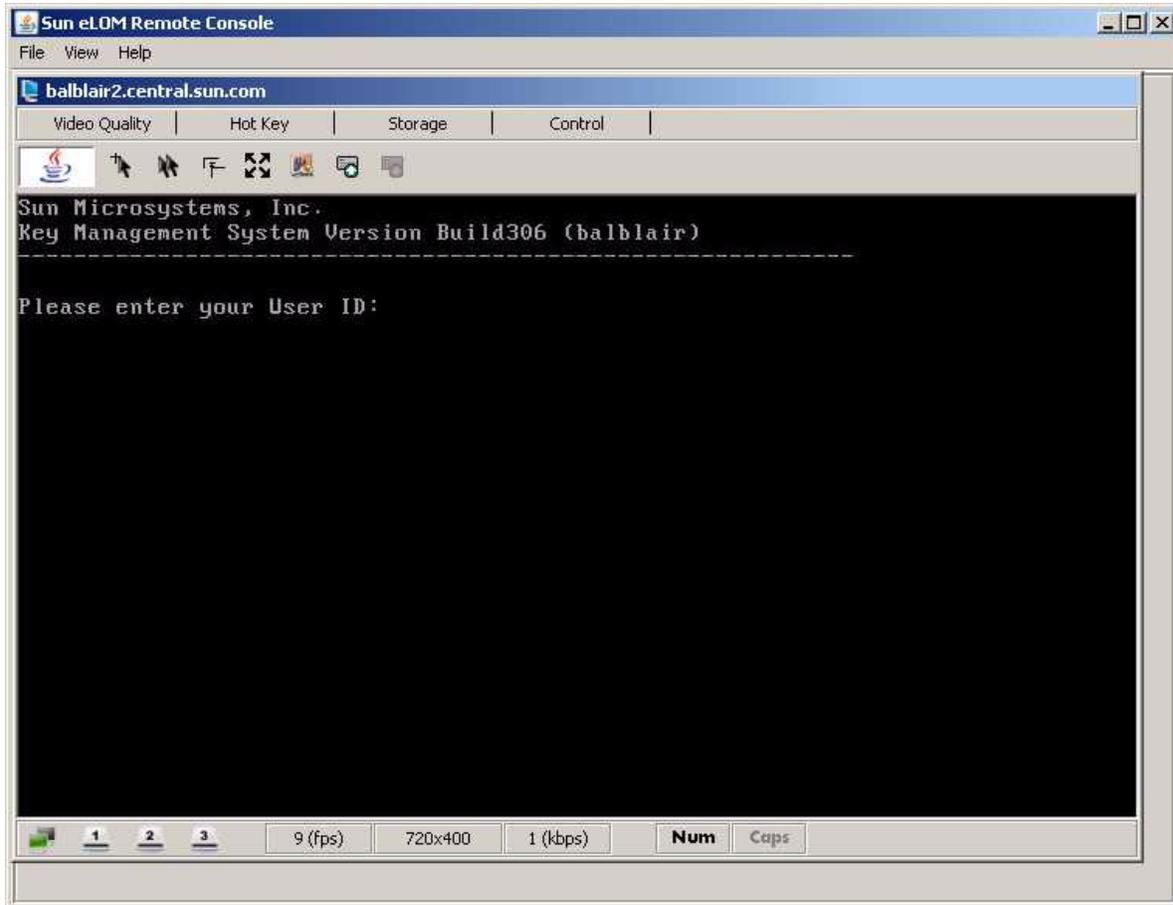
9. Cliquez sur l'onglet **Remote Control** (Contrôle à distance) disponible sur la première rangée d'onglets.
10. Cliquez sur l'onglet **Redirection** (Redirection) disponible sur la deuxième rangée d'onglets.

11. Cliquez sur le bouton **Launch Redirection** (Lancer la redirection).



L'écran de la console distante est alors ouvert dans une nouvelle fenêtre.

12. Un applet Java est téléchargé préalablement au lancement de la fenêtre de la console distante. Enregistrez le fichier javaRKVM.jnlp lorsque vous y êtes invité, puis ouvrez-le afin de lancer la console distante. Contournez les éventuels avertissements qui s'affichent à l'écran.



## Exécution du programme QuickStart

Lorsqu'un KMA se trouvant dans l'état par défaut défini en usine est mis sous tension, un mode spécial du menu de configuration appelé QuickStart est exécuté automatiquement. QuickStart collecte les informations de configuration minimales requises pour l'initialisation du KMA. Une fois le programme QuickStart exécuté jusqu'à son terme, il est impossible de le relancer. Le seul moyen d'accéder à nouveau au programme QuickStart consiste à réinitialiser le KMA selon son état par défaut défini en usine.

---

**Remarque** – Dans les exemples d'écrans suivants, les entrées en **gras** représentent les zones de réponse de l'utilisateur.

---

## Lancement de QuickStart

Pour exécuter le programme QuickStart :

Mettez le KMA sous tension. Lors de la première mise sous tension du KMA, QuickStart s'exécute, puis l'écran Welcome to QuickStart! (Bienvenue dans QuickStart) s'affiche.

```
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:
```

---

**Remarque** – Si l'utilisateur appuie sur les touches Ctrl+C, le programme QuickStart est réinitialisé et l'écran Welcome to QuickStart! (Bienvenue dans QuickStart) s'affiche.

---

## Définition de l'adresse IP

1. À l'invite `Press Enter to continue:` (Appuyez sur Entrée pour continuer), appuyez sur la touche <Entrée>. Les informations suivantes s'affichent.

```
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. À l'invite `Please enter the Management Network Hostname:` (Indiquez le nom de l'hôte réseau de gestion), saisissez le nom de l'hôte approprié, puis appuyez sur <Entrée>.
3. À l'invite `Do you want to use DHCP to configure the Management Network interface? [y/n]:` (Voulez-vous utiliser le protocole DHCP pour configurer l'interface réseau de gestion ?), tapez soit **n** (pour no) soit **y** (pour yes), puis appuyez sur <Entrée>. Si vous tapez **n**, passez à l'étape 4. Si vous choisissez **y**, passez à l'étape 6.

4. À l'invite `Please enter the Management Network IP Address:` (Saisissez l'adresse IP réseau de gestion), tapez l'adresse IP appropriée, puis appuyez sur `<Entrée>`.
5. À l'invite `Please enter the Management Network Subnet Mask:` (Saisissez l'adresse du masque de sous-réseau), tapez l'adresse appropriée (par exemple, `255.255.254.0`), puis appuyez sur `<Entrée>`.
6. À l'invite `Please enter the Service Network Hostname:` (Saisissez le nom de l'hôte réseau de service), tapez le nom de l'hôte approprié, puis appuyez sur `<Entrée>`.
7. À l'invite `Do you want to use DHCP to configure the Service Network interface? [y/n]:` (Voulez-vous utiliser le protocole DHCP pour configurer l'interface réseau de gestion ?), tapez soit `n` (pour no) soit `y` (pour yes), puis appuyez sur `<Entrée>`. Si vous tapez `n`, passez à l'étape 8. Si vous choisissez `y`, passez à l'étape 10.
8. À l'invite `Please enter the Service Network IP Address:` (Saisissez l'adresse IP réseau de service), tapez l'adresse IP appropriée, puis appuyez sur `<Entrée>`.
9. À l'invite `Please enter the Service Network Subnet Mask:` (Saisissez le masque de sous-réseau du réseau de service), tapez l'adresse du masque de sous-réseau appropriée (par exemple, `255.255.255.0`), puis appuyez sur `<Entrée>`.
10. À l'invite `Please enter the Gateway IP Address (optional but necessary if this KMA is to communicate with an entity on a different IP Subnet:` (Saisissez l'adresse IP de la passerelle (facultative mais obligatoire si ce KMA doit communiquer avec une entité située sur un sous-réseau IP différent)), tapez l'adresse IP appropriée, puis appuyez sur `<Entrée>`. Vous pouvez laisser cette entrée vide si le KMA n'est pas destiné à communiquer avec une entité se trouvant en dehors de son sous-réseau.
11. À l'invite `Please enter the Primary DNS Server IP Address (optional):` (Saisissez l'adresse IP du serveur DNS principal (facultatif)), tapez l'adresse IP appropriée, puis appuyez sur `<Entrée>`. Vous pouvez laisser cette entrée vide.
12. À l'invite `Please enter the DNS Domain:` (Saisissez le domaine DNS), indiquez le domaine DNS, puis appuyez sur `<Entrée>`.
13. Les informations suivantes s'affichent, indiquant que les paramètres réseau ont été appliqués. Cela peut prendre une ou deux minutes.

## Initialisation du KMA

1. Appuyez sur <Entrée> pour continuer. Les informations suivantes s'affichent.

```
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. À l'invite, saisissez un identificateur unique pour le KMA.

---

**Remarque** – Il est impossible de modifier un nom de KMA une fois qu'il a été défini à l'aide du programme QuickStart. La seule manière de le modifier consiste à réinitialiser le KMA selon son état par défaut défini en usine puis à réexécuter QuickStart.

---

3. À l'invite, saisissez une valeur pour la phrase de passe root (racine), en vous assurant qu'elle répond aux règles spécifiées précédemment.
4. À l'invite `Please re-enter the 'root' Passphrase:` (Ressaisissez la phrase de passe root), tapez la même phrase de passe qu'à l'[étape 3](#), puis appuyez sur <Entrée>.

## Configuration du cluster

1. À l'invite, appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que vous pouvez utiliser ce KMA pour créer un nouveau cluster, l'intégrer à un cluster existant ou restaurer un cluster à partir d'une copie de sauvegarde du KMA.

```
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. À l'invite, tapez **1**, **2** ou **3**, puis appuyez sur <Entrée>.

Si vous tapez 1, reportez-vous à la section « [Références de scission de clés](#) », page 32.

Si vous tapez 2, reportez-vous à la section « [Intégration à un cluster existant](#) », page 38.

Si vous tapez 3, reportez-vous à la section « [Restauration d'un cluster à partir d'une sauvegarde](#) », page 41.

## Références de scission de clés

Les ID utilisateur et les phrases de passe des références de scission de clés sont à saisir par le détenteur de ces informations. Si vous employez une personne pour collecter et saisir ces informations, vous allez à l'encontre de la raison d'être des références de scission de clés.

S'il s'avère peu pratique pour l'ensemble des membres des références de scission de clés de saisir ces informations à un moment donné, indiquez un jeu de références simplifié pour l'instant ; vous fournirez les références complètes ultérieurement dans le logiciel KMS Manager.

Cette méthode engendre cependant un risque de sécurité. Si une sauvegarde de sécurité principale est créée avec des références de scission de clés simplifiées, elle pourra servir à restaurer une sauvegarde.

1. À l'invite `Please enter your choice:` (Indiquez votre choix), tapez `1`.  
Les informations suivantes s'affichent.

```

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.

```

**Remarques :**

- Vous pourrez modifier ultérieurement les valeurs des options Key Split Size (Taille de la scission de la clé) et Key Split Threshold (Seuil de scission des clés) via KMS Manager.
- Afin de les protéger, les ID utilisateur et les phrases de passe doivent être exclusivement fournis par un utilisateur autorisé. Ces paramètres sont également modifiables après l'exécution du programme QuickStart.

2. À l'invite `Please enter the Key Split Size:` (Saisissez la taille de scission de la clé), indiquez le nombre de scissions de clés à générer, puis appuyez sur <Entrée>.
3. À l'invite `Please enter the Key Split Threshold:` (Saisissez le seuil de scission des clés), tapez le nombre de scission de clés requises pour obtenir un quorum, puis appuyez sur <Entrée>.
4. À l'invite `Please enter the Key Split User Name #1:` (Saisissez le premier nom d'utilisateur de scission de clé), tapez le nom d'utilisateur du premier utilisateur de scission de clé, puis appuyez sur <Entrée>.
5. À l'invite `Please enter Key Split Passphrase #1:` (Saisissez la 1ère phrase de passe de scission de clé, tapez la phrase de passe du premier utilisateur de scission de clé, puis appuyez sur <Entrée>.
6. À l'invite `Please re-enter Key Split Passphrase #1:` (Ressaisissez la 1ère phrase de passe de scission de clé), tapez la même phrase de passe que précédemment, puis appuyez sur <Entrée>.
7. Recommencez la procédure de l'étape 4 à l'étape 6 jusqu'à ce que tous les noms d'utilisateur et phrases de passe aient été saisis pour le nombre de scissions de clés sélectionné.

---

**Remarque** – Les noms d'utilisateur et phrases de passe de scissions de clés sont indépendants des autres comptes utilisateur établis pour l'administration des KMA.

---

## Références initiales de l'utilisateur responsable de la sécurité

1. À l'invite `Press Enter to continue:` (Appuyez sur Entrée pour continuer), appuyez sur la touche <Entrée>. Les informations suivantes s'affichent.

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.

---

**Remarque** – Ce compte utilisateur initial de responsable de la sécurité (Security Officer) sert à se connecter au KMA à l'aide de KMS Manager.

---

2. À l'invite, saisissez le nom d'utilisateur du responsable de la sécurité, puis appuyez sur <Entrée>. Les informations suivantes s'affichent.
3. À l'invite, tapez la phrase de passe du responsable de la sécurité, puis appuyez sur <Entrée>.
4. À l'invite `Please re-enter the Security Officer Passphrase:` (Ressaisissez la phrase de passe du responsable de la sécurité), indiquez à nouveau la même phrase de passe, puis appuyez sur <Entrée>.

---

**Important** – Tous les KMA disposent de leurs propres phrases de passe, indépendantes de celles assignées aux utilisateurs et aux agents. Le premier KMA d'un cluster se voit assigner une phrase de passe aléatoire. Si le certificat de ce KMA arrive à échéance et que vous souhaitez le récupérer à partir d'un autre KMA du même cluster, vous devez définir la phrase de passe sur une valeur connue à partir de KMS Manager. Pour plus d'informations sur les procédures, reportez-vous à la section « [Définition de la phrase de passe d'un KMA](#) », page 92.

---

## Préférence de déverrouillage autonome

---

**Attention** – Bien que cela s'avère plus commode et augmente la disponibilité du cluster KMS, l'activation du déverrouillage autonome engendre des risques de sécurité. Lorsque cette option est activée, un KMA hors tension conserve suffisamment d'informations pour pouvoir démarrer entièrement et commencer le déchiffrement des clés stockées.

Cela signifie par conséquent qu'un KMA volé peut très bien être mis sous tension par un pirate informatique qui est alors en mesure d'en extraire les clés. Bien qu'il ne soit pas facile d'extraire des clés, un utilisateur malveillant compétent est capable de vider toutes les clés d'un KMA. Aucune attaque cryptographique n'est nécessaire pour atteindre cet objectif.

Si l'option de déverrouillage autonome est désactivée, des attaques cryptographiques seront alors nécessaires pour extraire des clés d'un KMA volé.

Avant d'activer le déverrouillage autonome, étudiez soigneusement les risques de sécurité et d'attaques potentielles.

---

1. À l'invite `Press Enter to continue:` (Appuyez sur Entrée pour continuer), appuyez sur la touche <Entrée>. Les informations suivantes s'affichent.

```
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
```

---

**Remarque** – La fonction Autonomous Unlocking (Déverrouillage autonome) permet au KMA de basculer dans un état entièrement opérationnel après une réinitialisation à froid ou à chaud sans nécessiter la saisie d'un quorum de phrases de passe via KMS Manager. Vous pouvez ensuite modifier la configuration de cette option à partir de KMS Manager.

---

2. À l'invite, tapez `y` ou `n`, puis appuyez sur <Entrée>.

## Synchronisation horaire des KMA

Les KMA inclus dans un cluster **doivent** conserver leurs horloges synchronisées. En interne, tous les KMA utilisent le temps universel (UTC, coordinated universal time).

Vous pouvez également vous servir de KMS Manager pour régler les paramètres de la date et de l'heure sur les paramètres locaux.

```
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. Si un serveur NTP est disponible dans votre environnement réseau, à l'invite `Please enter the NTP Server Hostname or IP Address (optional):` (Saisissez le nom de l'hôte ou l'adresse IP du serveur NTP), indiquez le nom de l'hôte ou l'adresse IP approprié(e).
2. Si aucun serveur NTP n'est disponible, appuyez sur <Entrée>. Ensuite, à l'invite `Please enter the date and time for this KMA` (Saisissez la date et l'heure de ce KMA), indiquez la date et l'heure dans l'un des formats spécifiés ou appuyez sur <Entrée> pour utiliser les paramètres horaires affichés.
3. À l'invite, appuyez sur <Entrée>. L'initialisation du KMA est terminée.
4. Appuyez sur <Entrée> pour quitter. Le programme QuickStart se ferme ici et une invite de connexion s'affiche (voir la section « [Connexion au KMA](#) », page 266). Le KMA dispose à présent de la configuration système minimale requise pour communiquer avec KMS Manager.
5. L'étape suivante consiste à utiliser KMS Manager pour vous connecter au cluster. Pour plus d'informations à ce sujet, reportez-vous à la section « [Connexion au cluster](#) », page 71.

## Intégration à un cluster existant

---

**Important** – Avant d'effectuer cette tâche, le responsable de la sécurité doit se connecter au cluster KMS à l'aide de KMS Manager afin de créer un KMA. Reportez-vous à la section « [Création d'un KMA](#) », page 87.

Le nom du KMA spécifié lors du processus d'initialisation (voir la section « [Initialisation du KMA](#) », page 30) doit correspondre à celui que vous avez saisi au moment de la création du KMA.

---

Pour intégrer un KMA à un cluster existant :

1. Une fois le processus d'initialisation du KMA terminé (voir la section « [Initialisation du KMA](#) », page 30), appuyez sur <Entrée> à l'invite.

Les informations suivantes s'affichent, indiquant que vous pouvez utiliser ce KMA pour créer un nouveau cluster, l'intégrer à un cluster existant ou restaurer un cluster à partir d'une copie de sauvegarde du KMA.

```
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. À l'invite `Please enter your choice:` (Indiquez votre choix), tapez `2`.  
Les informations suivantes s'affichent.

```

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:

```

---

**Remarque** – Avant que ce nouveau KMA puisse communiquer avec un KMA existant du cluster, vous devez utiliser KMS Manager afin de créer une entrée correspondante dans la base de données de KMA existante. Pour plus d'informations à ce sujet, reportez-vous à la section « [Création d'un KMA](#) », page 87.

---

3. À l'invite, saisissez l'adresse réseau d'un KMA du cluster existant, puis appuyez sur <Entrée>.
4. À l'invite, saisissez la phrase de passe du KMA, puis appuyez sur <Entrée>.

5. Spécifiez le premier nom d'utilisateur de la scission de clé correspondant au premier KMA.
6. Tapez la phrase de passe de l'utilisateur de la scission de clé, puis appuyez sur <Entrée>.

---

**Important** – Indiquez soigneusement les noms d'utilisateur et phrases de passe des scissions de clés. Toute erreur de saisie entraîne l'échec de l'opération, signalé par un message d'erreur générique. Pour limiter les informations exposées à des attaques, aucune indication sur le nom d'utilisateur ou la phrase de passe incorrect(e) n'est fournie.

---

7. Recommencez l'[étape 5](#) et l'[étape 6](#) jusqu'à ce que vous ayez saisi un nombre suffisant de noms d'utilisateur et de phrases de passe de scissions de clés pour constituer un quorum.
8. À la prochaine invite `Please enter Key Split User Name` (Saisissez le nom d'utilisateur de scission de clé), appuyez sur <Entrée>. Laissez ce champ vide pour terminer.  
L'initialisation est terminée.
9. Appuyez sur <Entrée> pour quitter. Le programme QuickStart se ferme ici et une invite de connexion s'affiche (voir la section « [Connexion au KMA](#) », page 266). Le KMA dispose à présent de la configuration système minimale requise pour communiquer avec KMS Manager.
10. L'étape suivante consiste à utiliser KMS Manager pour vous connecter au cluster. Pour plus d'informations sur les procédures, reportez-vous à la section « [Connexion au cluster](#) », page 71.

## Restauration d'un cluster à partir d'une sauvegarde

Cette option vous permet de créer un compte Security Officer (Responsable de la sécurité) destiné à restaurer l'image de sauvegarde sur le KMA au moyen de KMS Manager. Vous pouvez utiliser une sauvegarde afin de restaurer la configuration d'un KMA dans le cas où ce dernier subirait une panne (disque dur endommagé, par exemple). Cependant, cela n'est généralement pas nécessaire, car un KMA restauré selon son état par défaut défini en usine peut immédiatement intégrer un cluster existant et construire sa propre base de données en recevant les mises à jour de réplication de ses pairs du cluster. La restauration d'un KMA à partir d'une sauvegarde s'avère néanmoins utile lorsque tous les KMA d'un cluster sont en panne.

---

**Remarque** – Vous devez disposer d'une sauvegarde. Pour connaître les procédures de création de copies de sauvegarde à l'aide de KMS Manager, reportez-vous à la section « [Création d'une sauvegarde](#) », page 259.

---

Pour restaurer une image de sauvegarde :

1. Une fois le processus d'initialisation du KMA terminé (voir la section « [Initialisation du KMA](#) », page 30), appuyez sur <Entrée> à l'invite.

Les informations suivantes s'affichent, indiquant que vous pouvez utiliser ce KMA pour créer un nouveau cluster, l'intégrer à un cluster existant ou restaurer un cluster à partir d'une copie de sauvegarde du KMA.

```
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. À l'invite `Please enter your choice:` (Indiquez votre choix), tapez **3**.  
Les informations suivantes s'affichent.

```
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. À l'invite, saisissez le nom d'utilisateur du responsable de la sécurité, puis appuyez sur `<Entrée>`.
4. À l'invite, tapez la phrase de passe du responsable de la sécurité, puis appuyez sur `<Entrée>`.

5. À l'invite `Please re-enter the Security Officer's Passphrase:` (Ressaisissez la phrase de passe du responsable de la sécurité), tapez la même phrase de passe qu'à l'étape 4, puis appuyez sur <Entrée>.

```

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. Si un serveur NTP est disponible dans votre environnement réseau, à l'invite `Please enter the NTP Server Hostname or IP Address (optional):` (Saisissez le nom de l'hôte ou l'adresse IP du serveur NTP (facultatif)), indiquez le nom de l'hôte ou l'adresse IP approprié(e).
7. Si aucun serveur NTP n'est disponible, appuyez sur <Entrée>. Ensuite, à l'invite `Please enter the date and time for this KMA` (Saisissez la date et l'heure de ce KMA), indiquez la date et l'heure dans l'un des formats spécifiés ou appuyez sur <Entrée> pour utiliser les paramètres horaires affichés.

Assurez-vous que la date et l'heure sont exactes. Les cycles de vie des clés reposent sur des intervalles temporaires, et les heures de création d'origine pour les clés sont contenues dans la sauvegarde. Il est essentiel de définir un paramètre horaire exact sur le KMA de remplacement afin de conserver les cycles de vie des clés attendus.

- À l'invite, appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant le terme de l'initialisation.

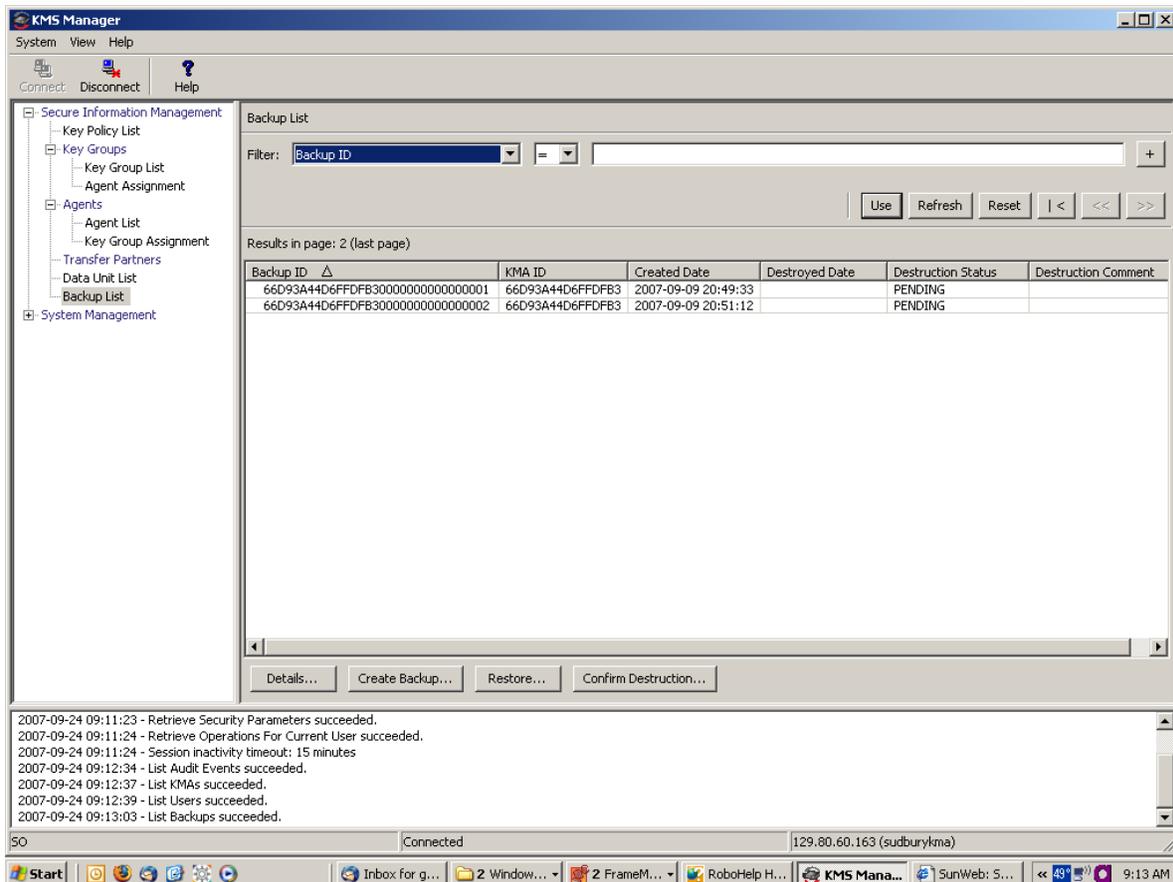
```
KMA Management System Version xxx
-----

KMA initialization complete!

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

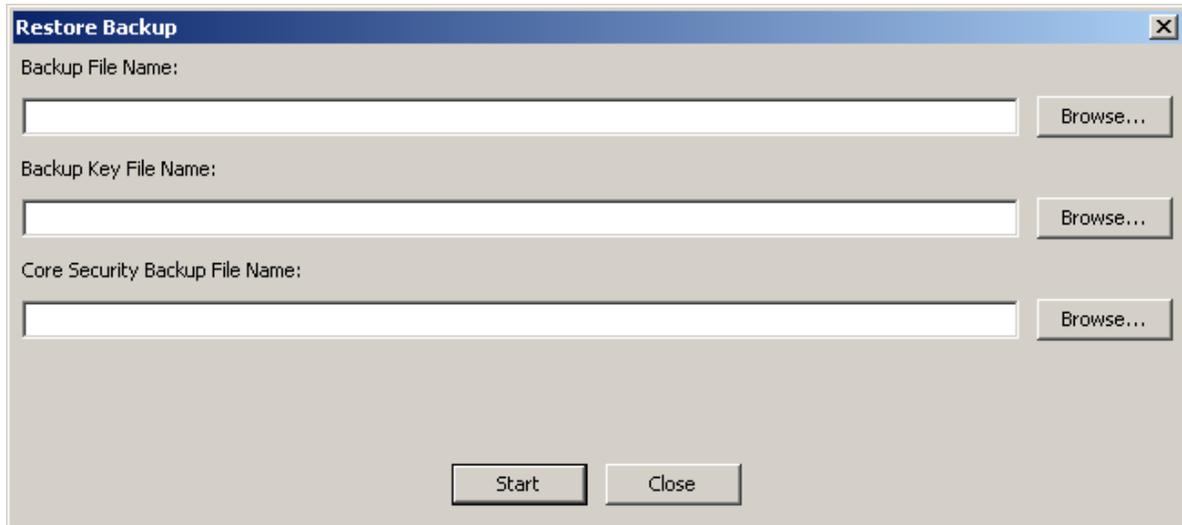
Press Enter to exit:
```

- Appuyez sur <Entrée> pour quitter. Le programme QuickStart se ferme ici et une invite de connexion s'affiche.
- Connectez-vous en tant que Security Officer (Responsable de la sécurité) sur KMS Manager et sélectionnez **Backup List** (Liste des sauvegardes). Dans l'écran Backup List (Liste des sauvegardes), cliquez sur le bouton **Restore** (Restaurer) afin de télécharger et de restaurer la sauvegarde sur le KMA.



11. Pour terminer l'opération de restauration, KMS Manager vous demande un fichier de sauvegarde correspondant au fichier de clés de sauvegarde, à un fichier de sauvegarde et au fichier de sauvegarde de sécurité principale.

Le fichier de clés de sauvegarde et le fichier de sauvegarde doivent correspondre alors que vous pouvez choisir n'importe quel fichier de sauvegarde de sécurité principale.



The image shows a dialog box titled "Restore Backup" with a close button (X) in the top right corner. The dialog contains three input fields, each with a "Browse..." button to its right:

- Backup File Name:
- Backup Key File Name:
- Core Security Backup File Name:

At the bottom of the dialog, there are two buttons: "Start" and "Close".

12. KMS Manager vous invite à ensuite à spécifier un quorum d'utilisateurs de scission de clés. Il doit s'agir des personnes dotées des références de scission de clés en vigueur lors de l'exécution de la sauvegarde de sécurité principale.

**Key Split Quorum Authentication**

To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials.

Split User 1:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 2:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 3:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 4:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 5:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 6:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 7:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 8:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 9:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 10:	<input type="text"/>	Passphrase:	<input type="text"/>

OK Cancel

Une fois la restauration terminée, les références de scission de clés appliquées lors de la sauvegarde (pas la sauvegarde de sécurité principale) sont rétablies.

---

**Important** – Indiquez soigneusement les noms d'utilisateur et phrases de passe des scissions de clés. Toute erreur de saisie entraîne l'échec du processus d'intégration à un cluster existant, signalé par un message d'erreur générique. Pour limiter les informations exposées à des attaques, aucune indication sur le nom d'utilisateur ou la phrase de passe incorrect(e) n'est fournie.

---

13. Une fois la restauration terminée, un nouveau cluster est créé.

## Utilisation de KMS Manager

---

Ce chapitre décrit le logiciel KMS Manager et présente les procédures suivantes :

- Installation du logiciel KMS Manager
- Appel de KMS Manager
- Désinstallation du logiciel KMS Manager

Il contient également une description succincte des menus et des volets de l'application.

### Présentation de KMS Manager

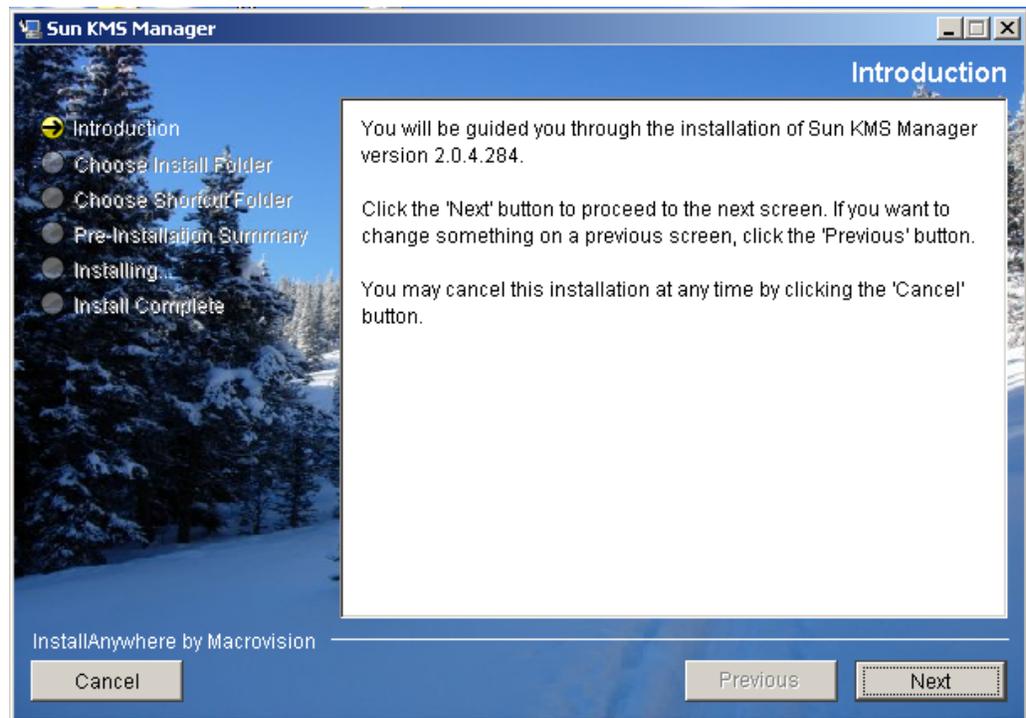
KMS Manager est une application jouant le rôle de client envers le KMA. Elle permet de configurer, de contrôler et de surveiller le KMA. Selon les rôles d'utilisateur assignés, les personnes sont autorisées à effectuer certaines tâches et pas d'autres.

# Installation du logiciel KMS Manager

Pour installer le logiciel KMS Manager :

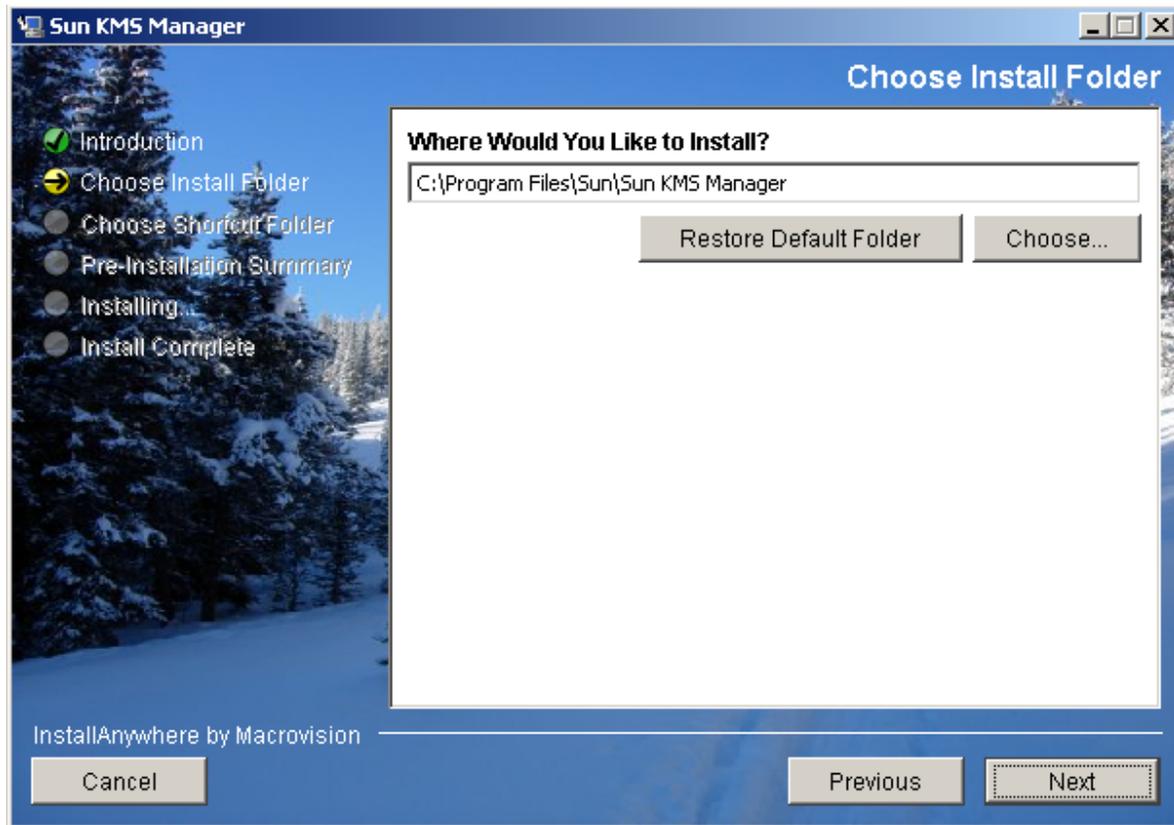
1. Rendez-vous sur le site Web du Centre des ressources client (CRC) de Sun StorageTek situé à l'adresse suivante :  
`http://www.support.storagetek.com/crc_home.html`
2. Connectez-vous au CRC et recherchez la zone intitulée Code Downloads (Téléchargement de codes). Cliquez sur le lien **KMS** afin de télécharger le code.
  - Sous Windows, double-cliquez sur l'exécutable **install.exe**.
  - Sous Solaris, ouvrez une fenêtre de shell et accédez au répertoire (via cd) dans lequel vous avez téléchargé le programme d'installation. À l'invite, tapez :  
`sh ./install.bin`

La fenêtre Introduction s'affiche.



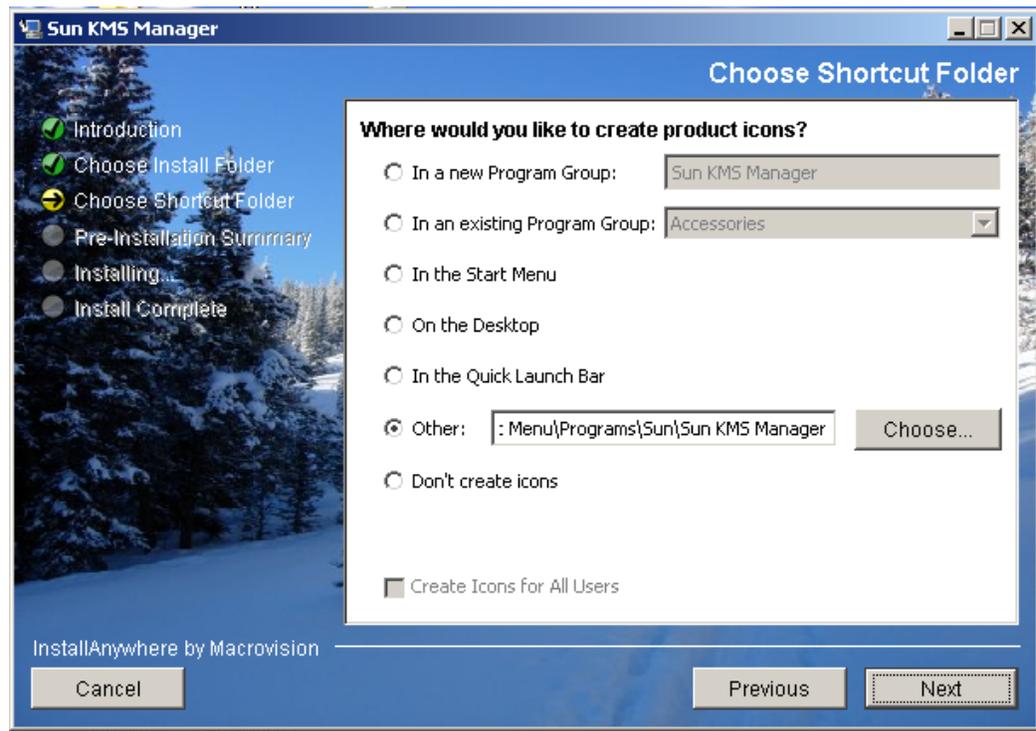
3. Cliquez sur Next (Suivant).

4. La fenêtre Choose Install Folder (Choix du dossier d'installation) s'affiche.



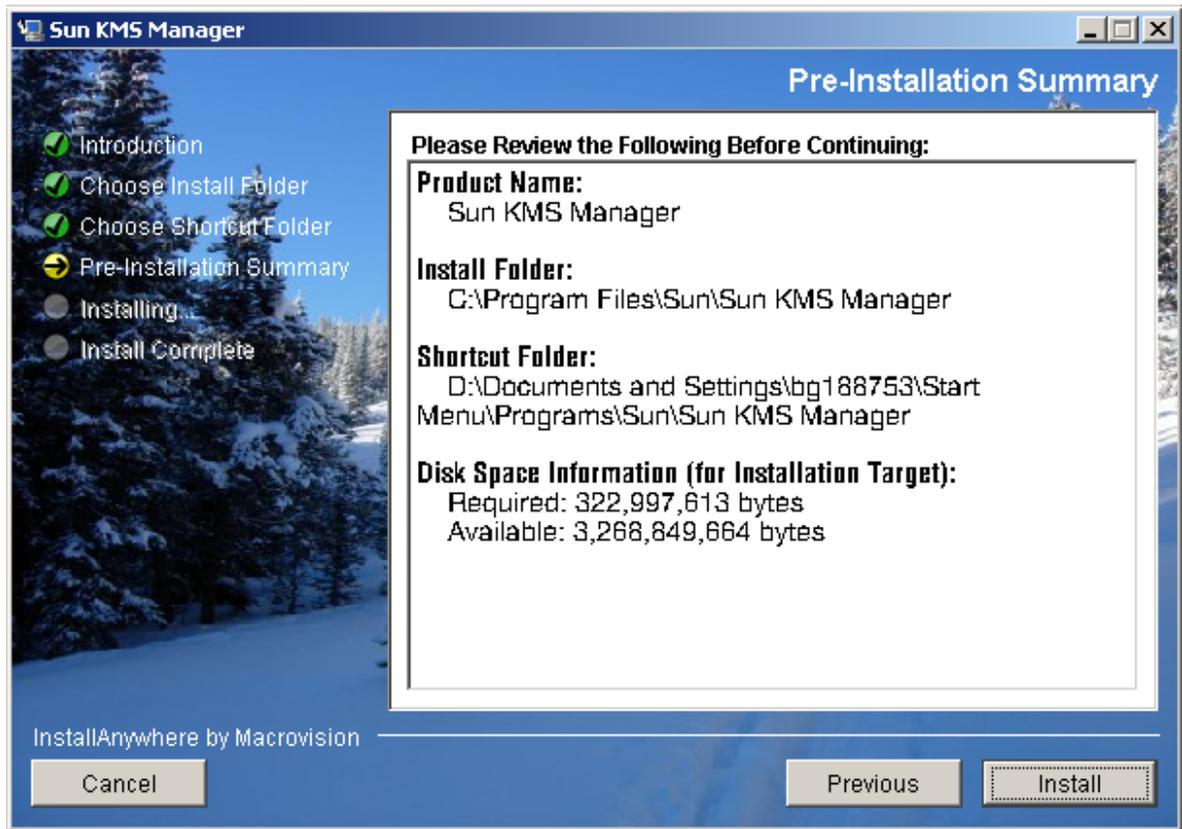
5. Pour sélectionner le dossier par défaut, cliquez sur Next (Suivant) ou indiquez un dossier d'installation personnel et choisissez Next (Suivant).

6. La fenêtre Choose Shortcut Folder (Choix du dossier des raccourcis) s'affiche, vous permettant de créer les icônes produit à l'emplacement de votre choix.

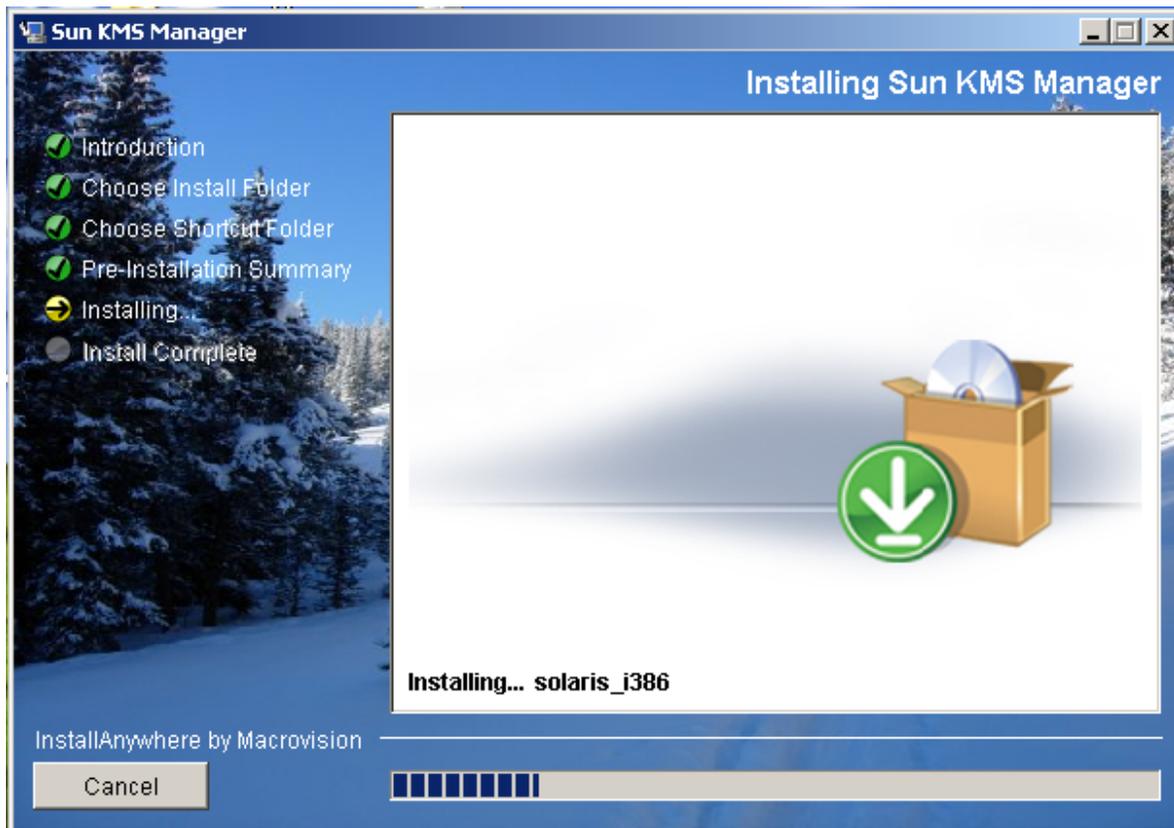


7. Cliquez sur Next (Suivant) une fois ce choix effectué.

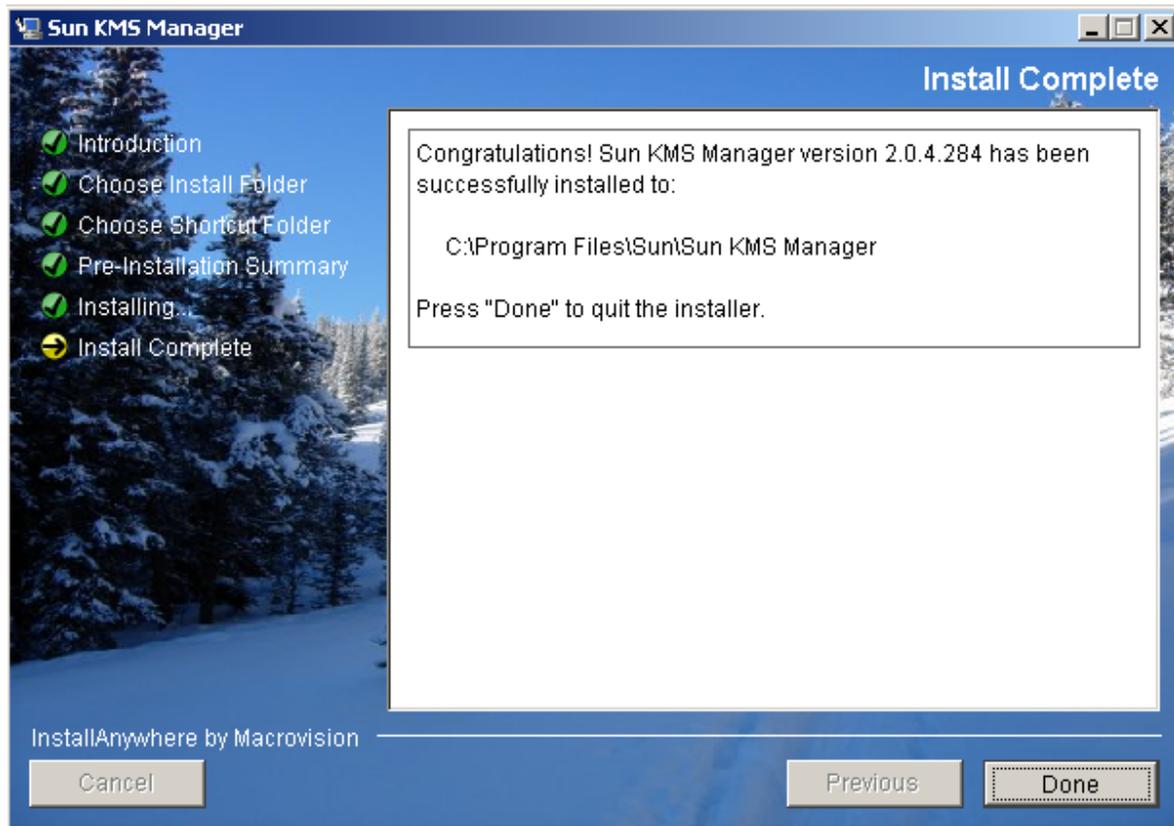
8. L'écran Pre-Installation Summary (Récapitulatif de la préinstallation) s'affiche.



9. Cliquez sur Install (Installer) afin d'installer KMS Manager ou choisissez Previous (Précédent) pour vérifier vos paramètres de configuration.



10. Le processus d'installation est à présent terminé. Cliquez sur Done (Terminer) pour quitter le programme.



# Appel de KMS Manager

Selon l'environnement, deux méthodes sont à votre disposition pour appeler KMS Manager :

- Démarrage sous Windows
- Démarrage sous Solaris

## Démarrage de KMS Manager sous Windows

Si vous avez spécifié la création d'un raccourci au moment de l'installation, double-cliquez dessus afin de lancer l'application KMS Manager.



Sinon, lancez l'Explorateur Windows, naviguez jusqu'au répertoire d'installation de KMS Manager, puis appelez l'exécutable KMS\_Manager.exe.

## Démarrage de KMS Manager sous Solaris

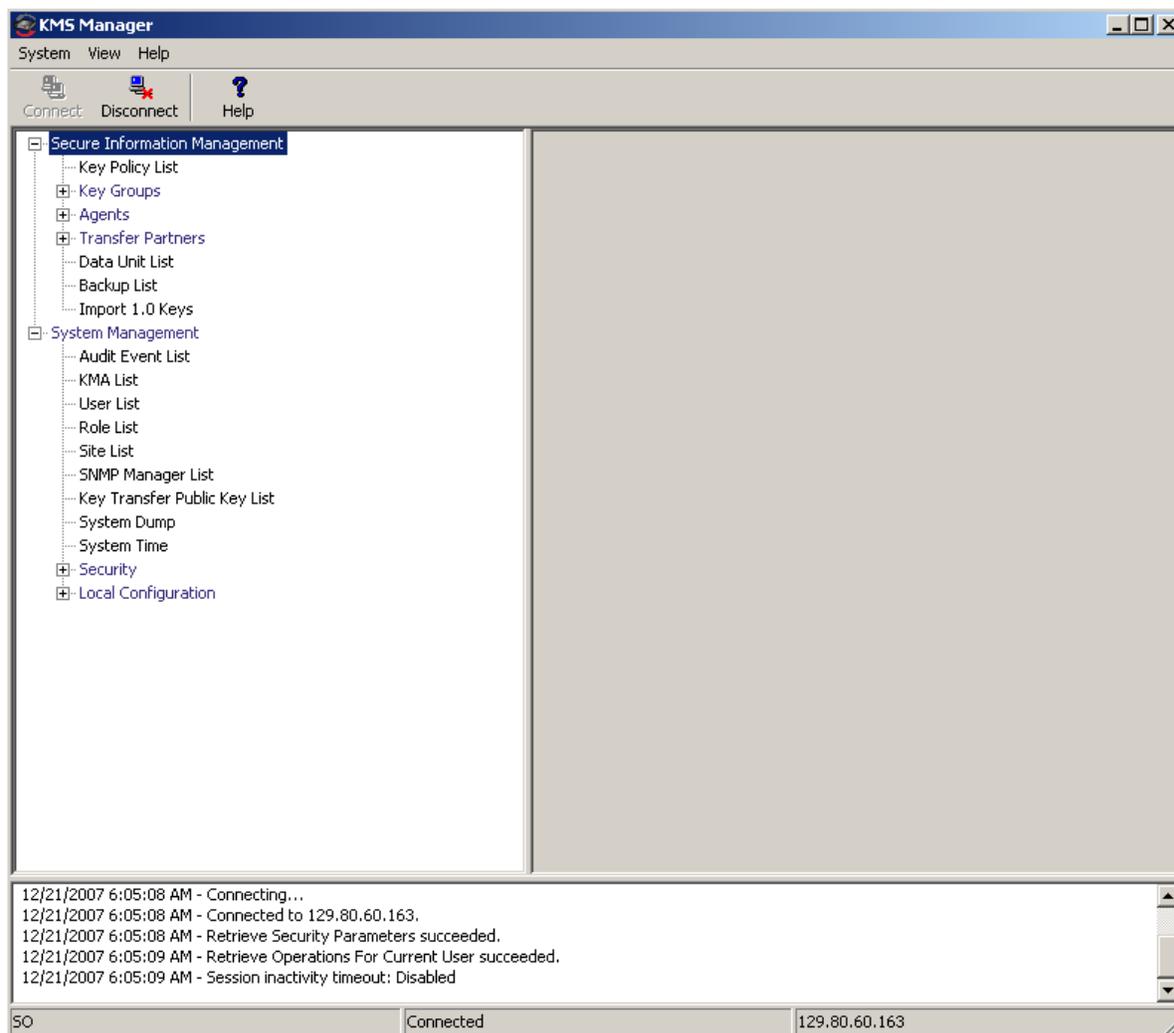
Tout comme sous Windows, vous pouvez indiquer au programme d'installation de créer un raccourci. Si, par exemple, vous avez créé ce raccourci dans le répertoire home, appelez-le à l'invite d'un shell en saisissant :

```
~/KMS_Manager
```

Sinon, naviguez jusqu'au répertoire d'installation de KMS Manager, puis appelez l'exécutable KMS\_Manager.exe.

# Présentation de l'IG de KMS Manager

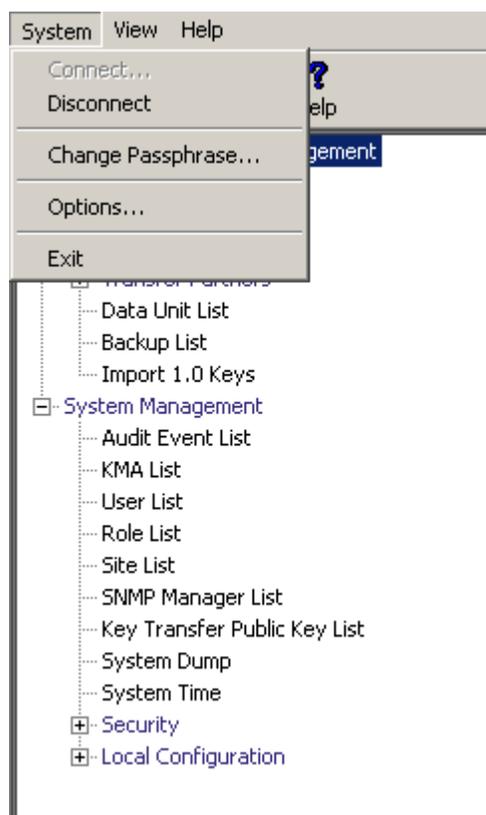
L'IG de KMS Manager est présentée ci-dessous à l'aide d'un exemple de menu.



L'IG de KMS Manager contient trois menus pratiques : System (Système), View (Affichage) et Help (Aide). Cliquez sur l'élément de barre d'actions approprié afin d'afficher un menu, puis sélectionnez une option de menu.

Des boutons de barre d'outils vous offrent des raccourcis vers plusieurs options de menu.

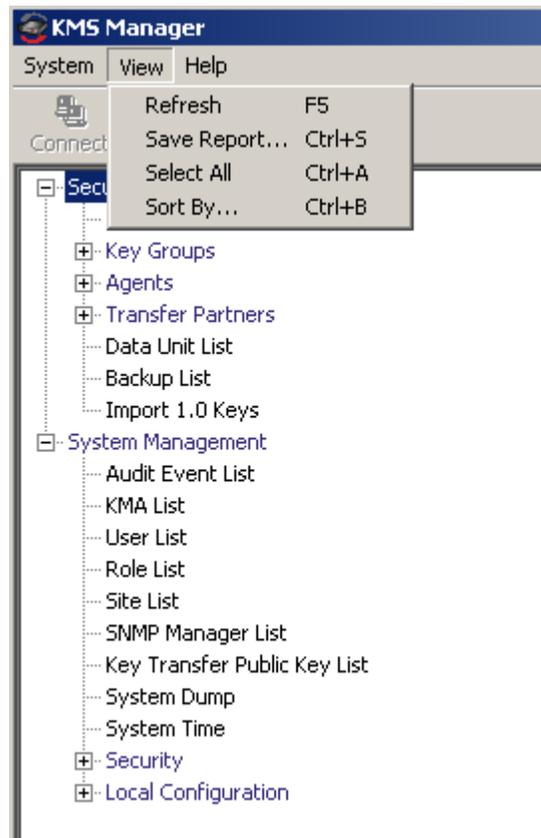
## Menu System (Système)



### Options du menu System (Système)

- **Connect** (Connexion) : permet d'afficher la boîte de dialogue Connect to Cluster (Connexion à un cluster) à partir de laquelle vous pouvez vous connecter à un cluster préexistant à l'aide d'un profile ou créer un nouveau profil de cluster.
- **Disconnect** (Déconnexion) : permet d'afficher la boîte de dialogue Disconnect from KMA (Déconnexion du KMA) à partir de laquelle vous pouvez vous déconnecter du KMA.
- **Change Passphrase** (Changer de phrase de passe) : permet d'afficher la boîte de dialogue Change passphrase à partir de laquelle vous pouvez modifier la phrase de passe.
- **Options** (Options) : permet d'afficher la boîte de dialogue Options dans laquelle vous pouvez spécifier divers paramètres de configuration.
- **Exit** (Quitter) : ferme l'IG de KMS Manager.

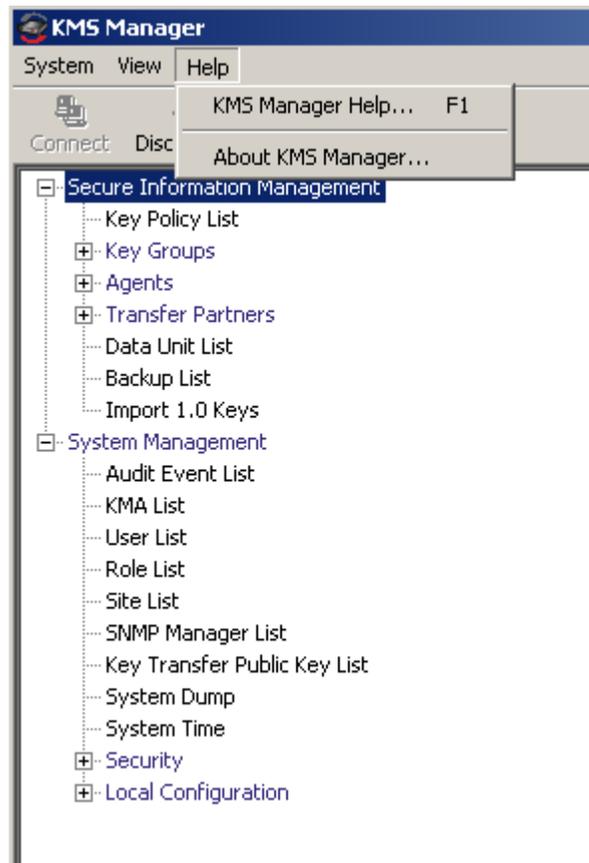
## Menu View (Affichage)



### *Options du menu View (Affichage)*

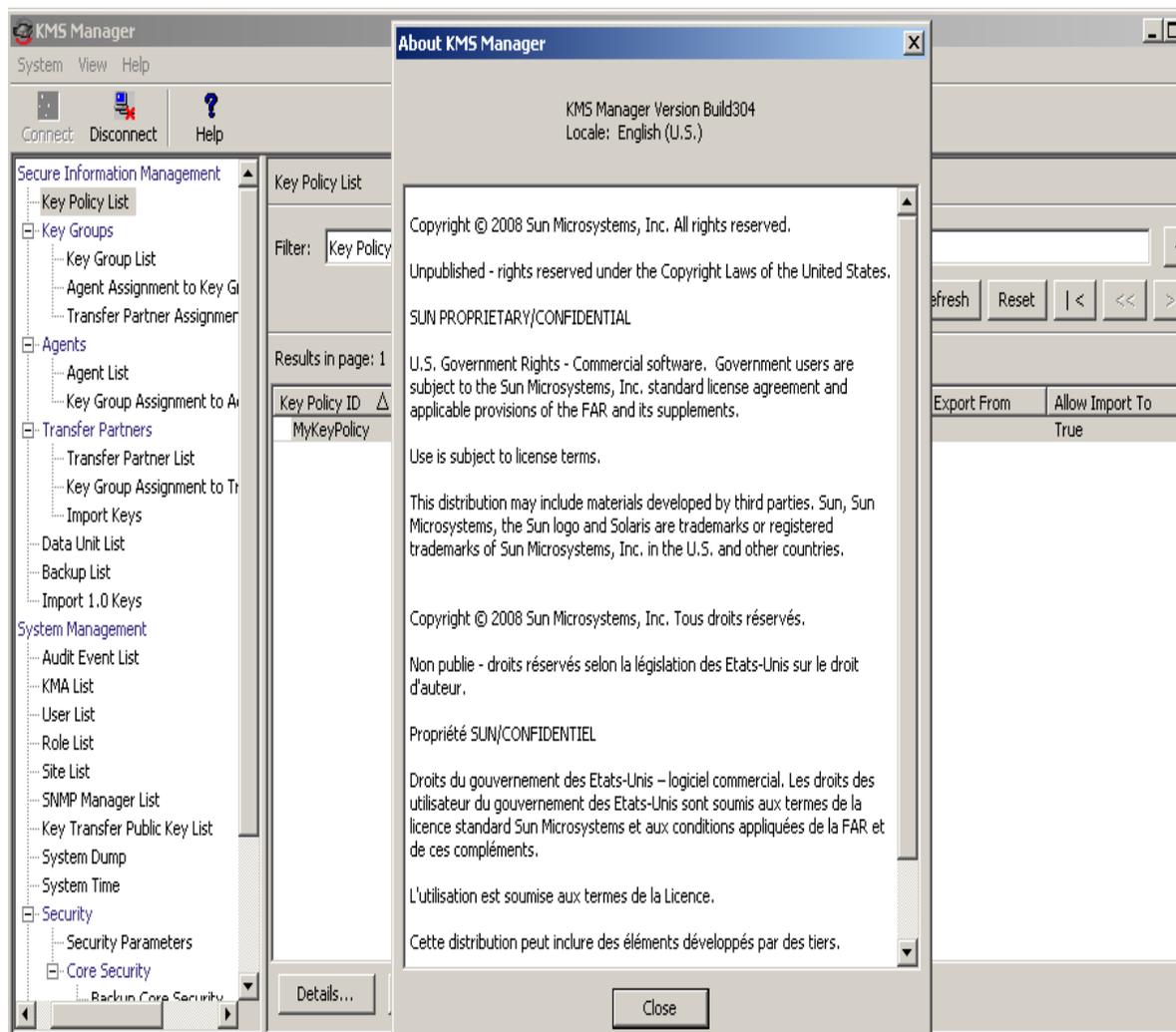
- **Refresh** (Actualiser) : actualise l'écran.
- **Save Report** (Enregistrer un rapport) : permet de télécharger le contenu de tout écran de liste dans un fichier texte situé sur le système exécutant KMS Manager.
- **Select All** (Tout sélectionner) : permet de sélectionner tous les éléments d'un écran de liste.
- **Sort By** (Trier par) : trie les éléments dans un écran de liste. Cette option équivaut à cliquer sur les en-têtes de colonnes dans une liste.

## Menu Help (Aide)



## Options du menu Help (Aide)

- **KMS Manager Help** (Aide de KMS Manager) : affiche l'index et le sommaire de l'aide en ligne relatifs à l'application KMS Manager.
- **About KMS Manager** (À propos de KMS Manager) : affiche des informations de version et de copyright relatives à l'application KMS Manager. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue.



## Boutons de barre d'outils

Le tableau ci-dessous décrit les boutons de barre d'outils disponibles dans KMS.

Bouton	Description
	Affiche la boîte de dialogue Connect to KMA (Connexion à un KMA) à partir de laquelle l'utilisateur peut se connecter à un KMA en sélectionnant un profil.
	Affiche la boîte de dialogue Disconnect from KMA (Déconnexion du KMA) à partir de laquelle l'utilisateur peut se déconnecter du KMA.
	Affiche l'index et le sommaire de l'aide en ligne de l'application.

## Raccourcis clavier

Les raccourcis clavier vous permettent de choisir des commandes en une seule étape. Les raccourcis suivants sont disponibles :

Coupe la sélection active.	Ctrl+X
Copie la sélection active.	Ctrl+C
Copie le contenu du Presse-papiers au point de sélection actif.	Ctrl+V
Affiche une boîte de dialogue permettant d'enregistrer un rapport sur un site local.	Ctrl+S

## Touches d'accès rapide aux menus

Les touches d'accès rapide aux menus sont prises en charge par toutes les options de menu. Maintenez la touche Alt enfoncée pour afficher les touches d'accès rapide.

## Utilisation de l'aide en ligne

L'aide en ligne comprend des informations complètes sur KMS. Son utilisation est simple. Les rubriques sont accessibles de différentes manières. Les opérations sont disponibles à partir de l'aide :

- Parcours du sommaire de l'aide
- Recherche de mots-clés
- Utilisation d'un index
- Navigation en arrière
- Impression de rubriques

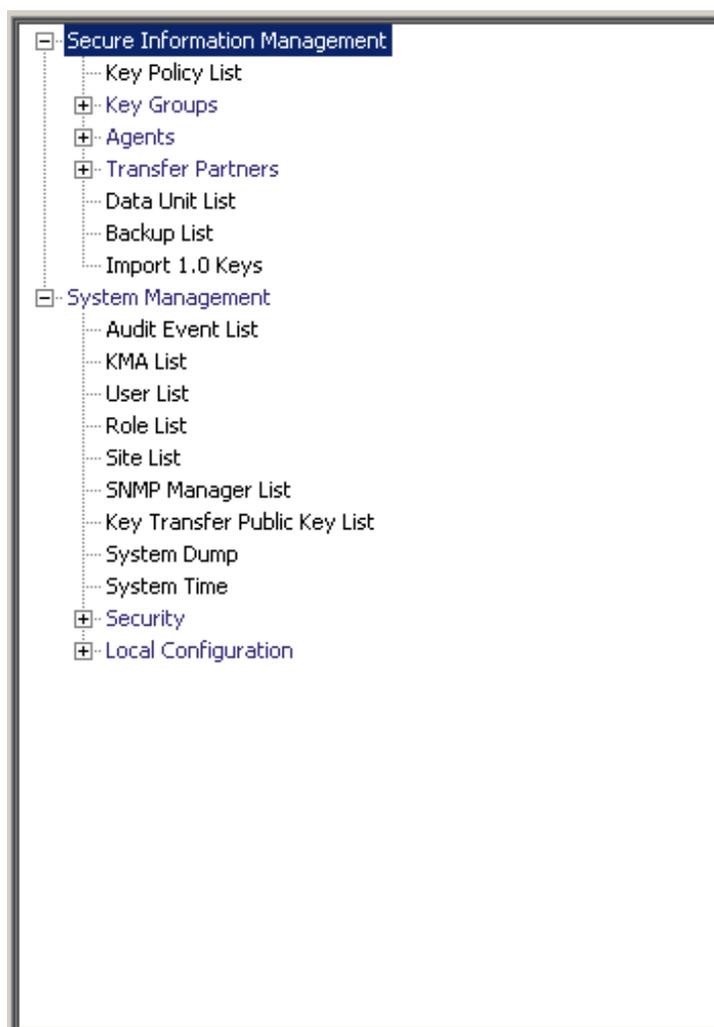
## Volets de l'IG de KMS Manager

L'IG de KMS Manager se divise en trois volets :

- Arborescence des opérations de gestion de KMS
- Détails des opérations de gestion de KMS
- Journal d'audit des sessions

### Arborescence des opérations de gestion de KMS

Le volet de l'arborescence des opérations de gestion de KMS, situé dans la partie gauche de l'écran, affiche toutes les fonctions opérationnelles du système de gestion des clés. Les options de ce volet varient en fonction des rôles qui vous sont assignés. L'exemple ci-dessous illustre les opérations autorisées pour un responsable de la sécurité.



## Volet des détails des opérations de gestion de KMS

Lorsqu'une opération est sélectionnée, le volet des détails des opérations de gestion de KMS, situé à droite du volet de l'arborescence des opérations, présente les composants requis pour exécuter cette opération. L'utilisateur peut appliquer des filtres aux éléments affichés dans les panneaux de listes. L'exemple ci-dessous affiche la liste des utilisateurs, suite à la sélection de l'option de menu User List (Liste des utilisateurs) dans le menu System Management (Gestion du système) du volet de l'arborescence des opérations.

The screenshot shows the KMS Manager application interface. The left pane displays a tree view with 'System Management' expanded and 'User List' selected. The main pane shows the 'User List' details, including a filter field set to 'User ID =', a table of users, and a status bar at the bottom.

Filter: User ID =

Use Refresh Reset | < << >> >>

Results in page: 8 (last page)

User ID	Description	Roles	Enabled	Failed Login Attempts
AUD	Test User	Auditor	True	0
All	Test User	Backup Operator, Compliance Officer, Operator, Security...	True	0
BO	test User	Backup Operator	True	0
CO	Test User	Compliance Officer	True	0
OP	Test User	Operator	True	0
SO		Backup Operator, Compliance Officer, Operator, Security...	True	0
nancy		Auditor	True	0
wally	night shift janitor	Security Officer	True	0

Details... Create... Delete

12/21/2007 6:05:08 AM - Retrieve Security Parameters succeeded.  
12/21/2007 6:05:09 AM - Retrieve Operations For Current User succeeded.  
12/21/2007 6:05:09 AM - Session inactivity timeout: Disabled  
12/21/2007 6:32:33 AM - List Key Policies succeeded.  
12/21/2007 6:39:46 AM - List Users succeeded.

SO Connected 129.80.60.163

## Volet du journal d'audit des sessions

Le volet du journal d'audit des sessions, situé sous les deux autres volets, propose une liste des événements de sessions les plus récents que vous pouvez faire défiler.

The screenshot displays the KMS Manager application window. The left-hand navigation pane shows a tree structure with 'System Management' expanded to 'User List'. The main area shows a 'User List' tab with a filter box set to 'User ID'. Below the filter, there are buttons for 'Use', 'Refresh', 'Reset', and navigation arrows. A table displays the following data:

User ID	Description	Roles	Enabled	Failed Login Attempts
AUD	Test User	Auditor	True	0
All	Test User	Backup Operator, Compliance Officer, Operator, Security...	True	0
BO	test User	Backup Operator	True	0
CO	Test User	Compliance Officer	True	0
OP	Test User	Operator	True	0
SO		Backup Operator, Compliance Officer, Operator, Security...	True	0
nancy		Auditor	True	0
wally	night shift janitor	Security Officer	True	0

At the bottom of the window, a log shows the following messages:

- 12/21/2007 6:05:08 AM - Connecting...
- 12/21/2007 6:05:08 AM - Connected to 129.80.60.163.
- 12/21/2007 6:05:08 AM - Retrieve Security Parameters succeeded.
- 12/21/2007 6:05:09 AM - Retrieve Operations For Current User succeeded.
- 12/21/2007 6:05:09 AM - Session inactivity timeout: Disabled
- 12/21/2007 6:32:33 AM - List Key Policies succeeded.

The status bar at the bottom indicates '50' on the left, 'Connected' in the center, and '129.80.60.163' on the right.

## Barre d'état

La barre d'état, située au bas de l'écran, comprend les champs suivants :

- **Nom de l'utilisateur** : affiche le nom de l'utilisateur actuellement connecté.  
Dans l'écran ci-dessous, il s'agit du responsable de sécurité : Security Officer (SO).
- **Statut de la connexion** : affiche l'état de la connexion active, ici **Connected** (Connecté).
- **Adresse IP KMA** : affiche l'adresse IP réseau de gestion et le nom du KMA cible.

Si aucune connexion n'est établie avec un KMA, les champs de statut sont vides.

The screenshot shows the KMS Manager application window. The left sidebar contains a tree view with categories like 'Secure Information Management' and 'System Management'. The 'User List' item is selected. The main area displays a table of users with columns for User ID, Description, Roles, Enabled, and Failed Login Attempts. Below the table are buttons for 'Details...', 'Create...', and 'Delete'. At the bottom, a status bar shows the user 'SO', the status 'Connected', and the IP address '129.80.60.163'. A log window at the bottom left shows system messages.

User ID	Description	Roles	Enabled	Failed Login Attempts
AUD	Test User	Auditor	True	0
All	Test User	Backup Operator, Compliance Officer, Operator, Security...	True	0
BO	test User	Backup Operator	True	0
CO	Test User	Compliance Officer	True	0
OP	Test User	Operator	True	0
SO		Backup Operator, Compliance Officer, Operator, Security...	True	0
nancy		Auditor	True	0
wally	night shift janitor	Security Officer	True	0

## Panneaux

Les différents écrans de KMS Manager comprennent des composants de panneaux communs. Ceux-ci font l'objet d'une description ci-dessous :

### **Title (Titre)**

Affiche le titre de l'écran.

### **Filter (Filtre)**

Permet de filtrer la base de données par clé spécifique. Il comprend les composants suivants :

**Table label** (Étiquette de table) : indique la table à laquelle le filtre s'applique.

**Boîte combinée Filter Attribute** (Attribut de filtre) : indique les champs à filtrer.

**Boîte combinée Filter Operator 1** (Opérateurs de filtrage 1) : indique les opérateurs de filtrage appliqués à la valeur de filtre 1. Les opérations de filtrage sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

**Contrôle Filter Value 1** (Valeur de filtre 1) : utilisé comme valeur unique ou comme valeur de départ de la plage de clés du filtre.

**Contrôle Filter Value 2** (Valeur de filtre 2) : utilisé comme valeur unique ou comme valeur de fin de la plage de clés du filtre.

**Bouton Use** (Utiliser) : applique le filtre à la liste affichée.

### **Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée. Il ne s'applique pas aux filtres sélectionnés depuis la dernière activation du bouton Use (Utiliser) ou Reset (Réinitialiser), et il ne modifie pas la page de la liste.

### **Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

### Results in Page (Résultats de la page)

Affiche le nombre d'éléments pouvant être affichés sur la page active. Ajoute la mention (last page) si vous avez atteint la dernière page de la liste. Le nombre maximum d'éléments affichés sur une page est défini par la valeur de l'option Query Page Size (Taille d'une page de requête) disponible dans la boîte de dialogue Options.

---

**Remarque** – Si le nombre d'enregistrements générés est supérieur à cette valeur, plusieurs pages sont affichées. Cliquez sur les boutons situés sous les filtres pour passer d'une page à l'autre.

---

### Sorting (Tri)

Cliquez sur un en-tête de colonne pour trier la liste selon ce champ. Si la sortie requiert plusieurs pages, les résultats complets sont triés, puis la page correspondante est retournée.

### Message

Affiche les messages liés aux requêtes effectuées dans la base de données. Ce paramètre fonctionne de pair avec la liste Database View (Vue de la base de données). Il comprend les composants suivants :

- Étiquette de texte statique : affiche des messages d'erreur. Exemple :  
`Result limit exceeded. 10,000 results returned. Use a filter to reduce the filter size.`

## Désinstallation du logiciel KMS Manager

Deux méthodes de désinstallation du logiciel KMS sont disponibles :

- Naviguez jusqu'au répertoire contenant le programme de désinstallation et lancez directement le fichier exécutable depuis cet emplacement.
- Sous Windows uniquement, lancez l'utilitaire Ajout/Suppression de programmes.

Dans les deux cas, la fenêtre Preparing Setup (Préparation à l'installation) s'affiche une fois la procédure terminée. Reportez-vous à la section « [Fin du processus de désinstallation](#) », page 69.

### Appel du fichier exécutable

Pour désinstaller le logiciel KMS Manager :

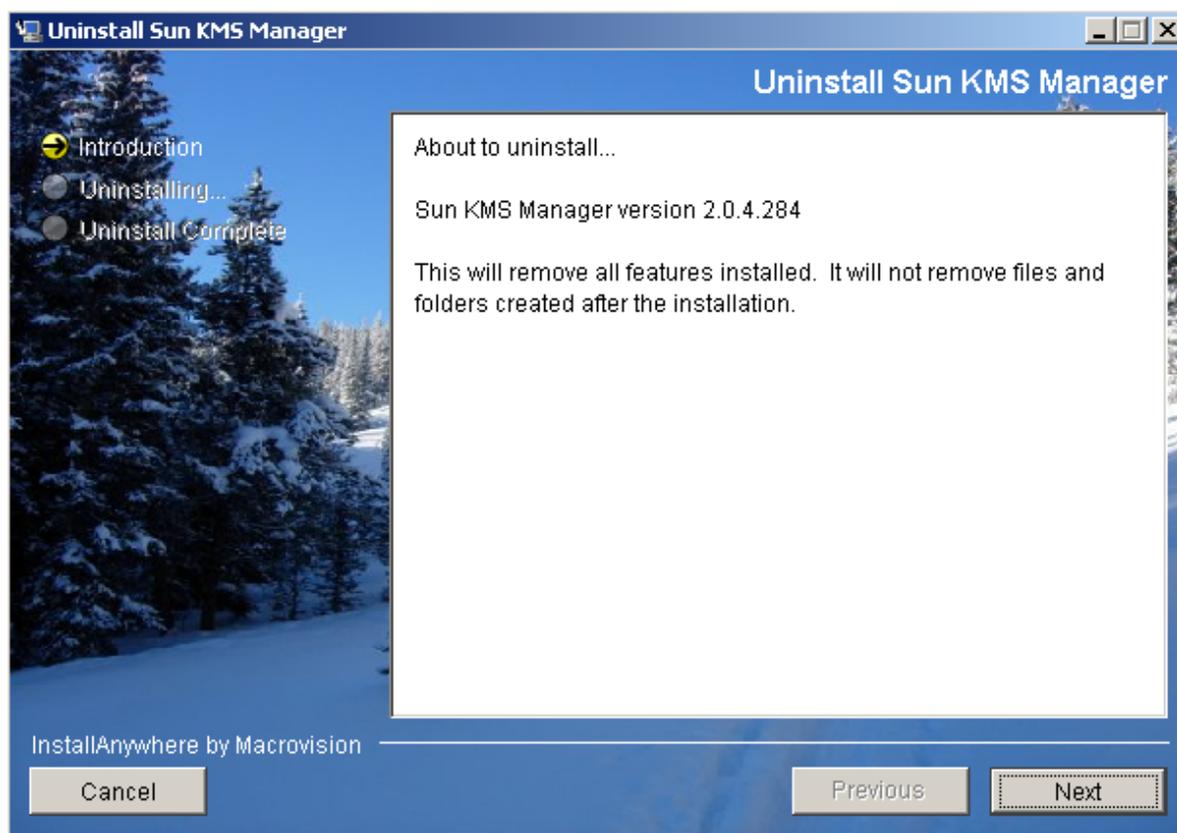
1. Naviguez jusqu'au répertoire Uninstall\_Sun KMS Manager, lequel se trouve dans le répertoire d'installation de KMS Manager.
2. Appelez l'exécutable Uninstall Sun KMS Manager (sous Windows) ou Uninstall\_Sun\_KMS\_Manager (sous Solaris) afin de lancer le processus de désinstallation.
3. La fenêtre Preparing Setup (Préparation à l'installation) s'affiche pendant que le programme d'installation/de désinstallation prépare l'opération.

### Appel de l'utilitaire Ajout/Suppression de programmes (Windows uniquement)

1. Choisissez **Démarrer**, puis **Paramètres**, **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**. La fenêtre Ajouter ou supprimer des programmes s'affiche. Faites défiler la liste (si le nom du logiciel n'est pas visible), sélectionnez Sun KMS Manager, puis cliquez sur le bouton Modifier/Supprimer.
2. La fenêtre Preparing Setup (Préparation à l'installation) s'affiche pendant que le programme d'installation/de désinstallation prépare l'opération.

## Fin du processus de désinstallation

La boîte de dialogue de désinstallation de KMS s'affiche, vous demandant de confirmer la suppression de l'application sélectionnée et de toutes les fonctions associées.



1. Cliquez sur Next (Suivant) pour continuer ou sur Cancel (Annuler) pour arrêter le processus et revenir à la fenêtre Ajouter ou supprimer des programmes (Windows) ou à l'invite de shell (Solaris).

---

**Remarque** – Vos profils de connexion ne seront pas supprimés.

---

2. Une fois le processus terminé, la fenêtre Uninstall Complete (Désinstallation terminée) s'affiche. Cliquez sur Finish (Terminer) pour fermer cette fenêtre. Fermez cette fenêtre afin de revenir à la fenêtre Ajouter ou supprimer des programmes (Windows) ou à l'invite de shell (Solaris).



## Utilisation du menu System (Système)

---

Ce chapitre fournit des instructions détaillées de connexion au KMA à l'aide de KMS Manager. Il présente par ailleurs les instructions d'utilisation des autres options du menu System (Système).

---

### Connexion au cluster

---

**Important** – Avant de vous connecter à un KMA, assurez-vous qu'au moins un profil de cluster existe et qu'un utilisateur est créé et activé sur le KMA.

---

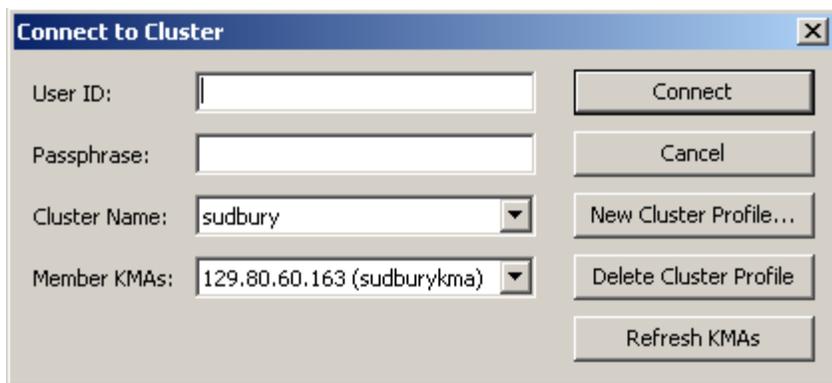
Cette section décrit les procédures de connexion au KMA à l'aide de KMS Manager. S'il s'agit de votre toute première connexion à un KMA, commencez par définir un profil de cluster. Lors des connexions ultérieures, vous pourrez ainsi vous en servir pour établir les connexions au KMA. KMS Manager se sert des informations sur le profil de cluster pour établir les communications avec un cluster (l'adresse IP du KMA).

---

### Création d'un profil de cluster

Pour créer un profil de cluster :

1. Dans le menu System (Système), choisissez Connect (Connecter) ou sur la barre d'outils, cliquez sur . La boîte de dialogue Connect to Cluster (Connexion à un cluster) s'affiche. Si vous possédez un profil préexistant, son nom et son adresse IP s'affichent dans les champs Cluster Name et IP Address.



2. Cliquez sur le bouton New Cluster Profile (Nouveau profil de cluster). La boîte de dialogue Create Cluster Profile (Création d'un profil de cluster) s'affiche.



3. Remplissez les champs des paramètres suivants :

**Cluster Name (Nom du cluster)**

Saisissez une valeur qui identifie de manière unique le nom du profil du cluster.

**Initial IP Address or Host Name (Adresse IP initiale ou nom de l'hôte)**

Indiquez l'adresse IP réseau de service ou le nom d'hôte du KMA initial de ce cluster auquel vous souhaitez vous connecter. Le choix du réseau de connexion varie en fonction du réseau auquel le système de l'ordinateur exécutant KMS Manager est relié.

---

**Remarque** – Il vous suffit de créer un seul profil de cluster, car il couvre la totalité du cluster et peut être utilisé par différentes personnes (utilisateurs de l'agent). La seule raison pouvant motiver la création d'un autre profil de cluster serait d'établir un second cluster ou le changement des adresses IP de tous les KMA du cluster actuel.

---

4. Cliquez sur OK. La boîte de dialogue Connect to Cluster (Connexion à un cluster) s'affiche en présentant les informations sur le profil du cluster que vous venez de créer.

5. Remplissez les champs des paramètres suivants, puis cliquez sur le bouton Connect (Se connecter) :

**User ID (ID utilisateur)**

Saisissez le nom de l'utilisateur qui se connectera au KMA spécifié ou, s'il s'agit de votre première connexion au KMA après l'exécution de l'assistant QuickStart initial, saisissez le nom du responsable de la sécurité créé dans QuickStart.

**Passphrase (Phrase de passe)**

Saisissez la phrase de passe associée à l'utilisateur sélectionné.

**Cluster Name (Nom du cluster)**

Sélectionnez le cluster auquel vous souhaitez vous connecter.

**Member KMAs (KMA membres)**

Sélectionnez le KMA auquel vous connecter dans ce cluster.

---

**Remarque** – Si un KMA a intégré le cluster après la dernière connexion au cluster de l'utilisateur, il ne figure pas dans la liste Member KMAs. Pour mettre à jour cette liste, saisissez le nom d'utilisateur et la phrase de passe, choisissez un profil de cluster et cliquez sur le bouton Refresh KMAs (Actualiser les KMA).

---

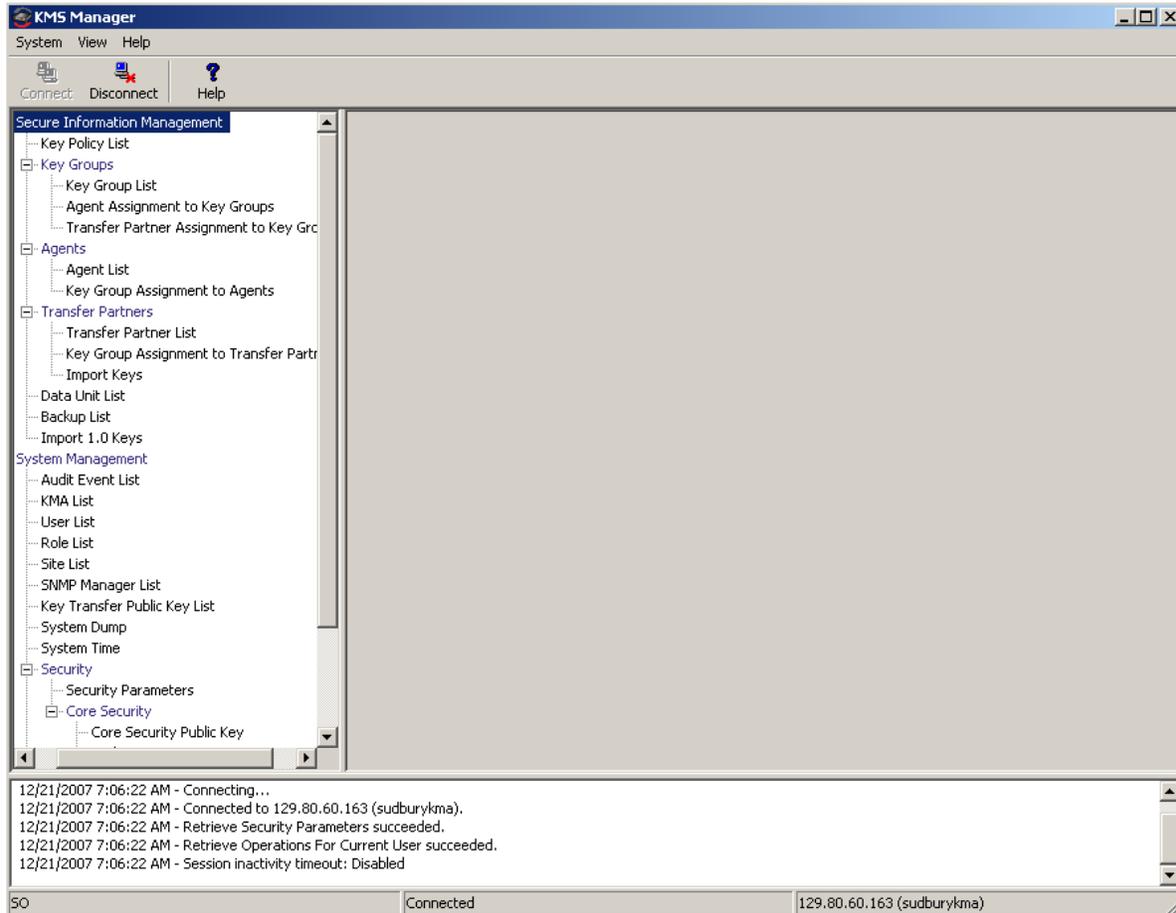


---

**Important** – Le KMA authentifie l'ID utilisateur et la phrase de passe. La liste des adresses IP de KMA retournée sert à remplir le profil du cluster. Elle est stockée sur l'hôte. La prochaine fois que l'utilisateur se connectera au KMA, il pourra saisir son nom d'utilisateur et sa phrase de passe, choisir un profil de cluster et sélectionner un KMA.

---

6. Si la connexion est établie, la barre d'état de l'IG de KMS Manager affiche le nom de l'utilisateur et son alias, le statut de la connexion au KMA (**Connected**) et l'adresse IP du KMA.



7. Vous pouvez à présent faire appel à KMS Manager pour effectuer diverses opérations. Les opérations possibles pour les différents rôles d'utilisateur sont décrites du [chapitre 5](#) au [chapitre 9](#).

---

**Remarque** – Les tâches disponibles dans le volet de l'arborescence des opérations de gestion de KMA varient selon le rôle assigné à l'utilisateur.

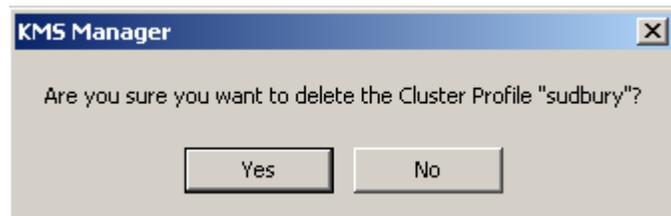
---

---

## Suppression d'un profil de cluster

Pour supprimer un profil de cluster :

1. Dans la boîte de dialogue Connect to Cluster (Connexion à un cluster), choisissez la flèche pointant vers le bas en regard du champ Cluster Name (Nom du cluster), mettez le profil à supprimer en surbrillance, puis cliquez sur le bouton Delete Cluster Profile (Supprimer le profil de cluster). La boîte de dialogue Delete Cluster Profile (Suppression du profil de cluster) s'affiche, vous demandant de confirmer la suppression du profil sélectionné.



2. Cliquez sur Yes (Oui) pour confirmer l'opération. Le profil de cluster est supprimé et vous revenez à la boîte de dialogue Connect to Cluster (Connexion à un cluster).

---

## Déconnexion d'un KMA

Pour vous déconnecter d'un KMA :

1. Dans le menu System (Système), choisissez **Disconnect** (Déconnexion) ou sur la barre d'outils, cliquez sur . Vous êtes instantanément déconnecté du KMA et du cluster KMS. Le volet du journal d'audit des sessions indique la date et l'heure de déconnexion du KMA.

---

## Modification de la phrase de passe

---

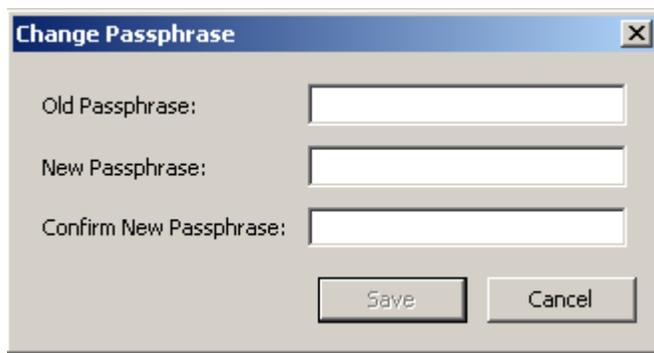
**Remarque** – L'option de menu de changement de mot de passe est uniquement activée si l'utilisateur est connecté à un KMA à l'aide d'un profil.

---

Cette fonction permet aux utilisateurs de modifier leurs phrases de passe personnelles. Elle n'invalide pas le certificat en vigueur de l'utilisateur.

Pour modifier la phrase de passe d'un utilisateur connecté :

1. Dans le menu System (Système), choisissez **Change Passphrase** (Changer de phrase de passe). La boîte de dialogue Change Passphrase (Changement de la phrase de passe) s'affiche.

The image shows a standard Windows-style dialog box titled "Change Passphrase". It has a blue title bar with a close button (X) on the right. The main area is light gray and contains three text input fields stacked vertically. The first is labeled "Old Passphrase:", the second "New Passphrase:", and the third "Confirm New Passphrase:". Below the input fields are two buttons: "Save" and "Cancel".

2. Remplissez les champs des paramètres suivants, puis cliquez sur OK :

**Old Passphrase (Ancienne phrase de passe)**

Saisissez l'ancienne phrase de passe de l'utilisateur.

**New Passphrase (Nouvelle phrase de passe)**

Saisissez la nouvelle phrase de passe de l'utilisateur.

**Confirm New Passphrase (Confirmer la nouvelle phrase de passe)**

Ressaisissez la même phrase de passe.

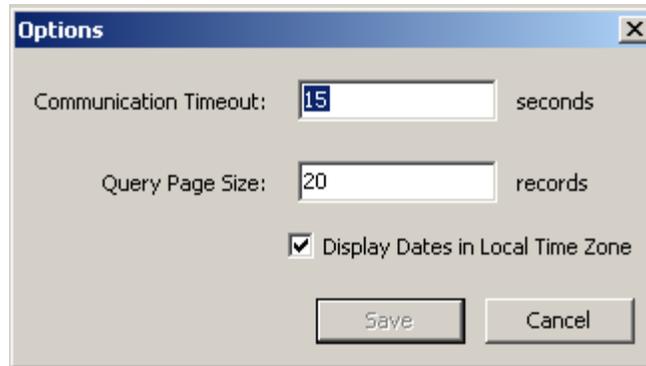
3. Le message suivant s'affiche dans le volet du journal d'audit des sessions, indiquant la date et l'heure de modification de la phrase de passe de l'utilisateur.

---

# Définition des paramètres de configuration

Pour spécifier les paramètres de configuration :

1. Dans le menu System (Système), choisissez Options. La boîte de dialogue Options s'affiche, indiquant les paramètres de configuration actuels.



2. Modifiez les paramètres suivants selon vos besoins, puis cliquez sur le bouton Save (Enregistrer) :

### **Communication Timeout (Délai de communication)**

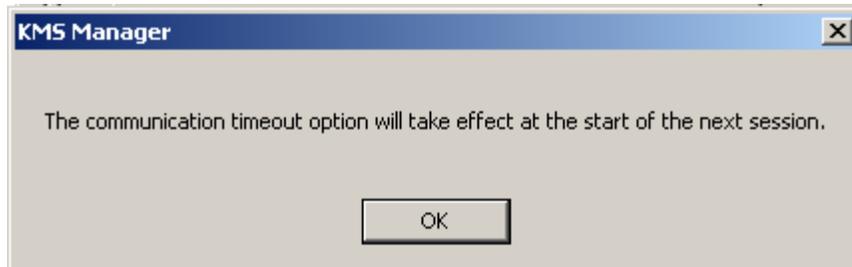
Saisissez un délai d'attente (en secondes) pendant l'établissement des communications avec le KMA connecté. Si le KMA ne répond pas dans l'intervalle de temps spécifié, KMS Manager abandonne la tentative de communication. La valeur minimale est de 1 tandis que la valeur maximale est de 60. La valeur par défaut est égale à 15.

### **Query Page Size (Taille d'une page de requête)**

Tapez le nombre maximum d'éléments à afficher sur un écran, dans une boîte de dialogue ou sur un onglet de boîte de dialogue présentant une liste d'éléments. La pagination permet de visualiser une liste dépassant la limite fixée par ce paramètre. La valeur minimale est de 1 tandis que la valeur maximale est de 1 000. La valeur par défaut est égale à 20.

**Display Dates in Local Time Zone (Afficher les dates selon le fuseau horaire local)**

Cochez cette case afin d'afficher toutes les dates et heures selon le fuseau horaire de la machine locale (c.-à-d., celle exécutant KMS Manager) plutôt qu'en temps universel (UTC). La valeur par défaut est sélectionnée. Le message de confirmation suivant s'affiche.



---

# Quitter KMS Manager

Pour quitter KMS Manager :

1. Dans le menu System (Système), choisissez **Exit** (Quitter) ou sur la barre de titre, cliquez sur . KMS Manager se ferme et vous revenez au bureau de Windows.
2. KMS Manager est immédiatement déconnecté et se ferme.



## Tâches du responsable de la sécurité

---

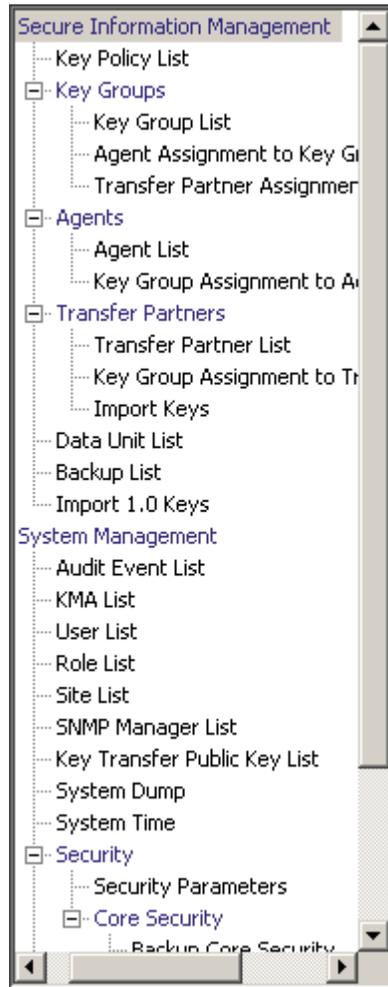
Un responsable de la sécurité (Security Officer) gère les paramètres de sécurité, les utilisateurs, les sites et les partenaires de transfert. Ce chapitre aborde les sujets suivants :

- Opérations qu'un utilisateur auquel le rôle de responsable de la sécurité a été assigné peut effectuer. Si plusieurs rôles vous ont été assignés, reportez-vous au chapitre pertinent pour des instructions sur les tâches associées à chaque rôle.
- Procédures d'activation et de désactivation d'un compte de support technique.

---

## Rôle Security Officer (Responsable de la sécurité)

En tant que responsable de la sécurité, vous pouvez gérer les entités (KMA, utilisateurs, sites et partenaires de transfert) de même que divers aspects de la sécurité du système.

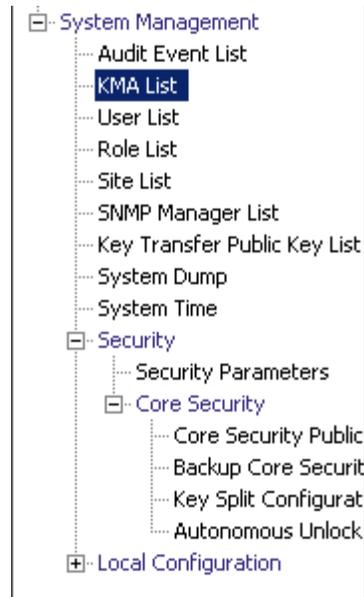


---

## Menu KMA List (Liste des KMA)

L'option de menu KMA List (Liste des KMA) vous permet d'effectuer les opérations suivantes :

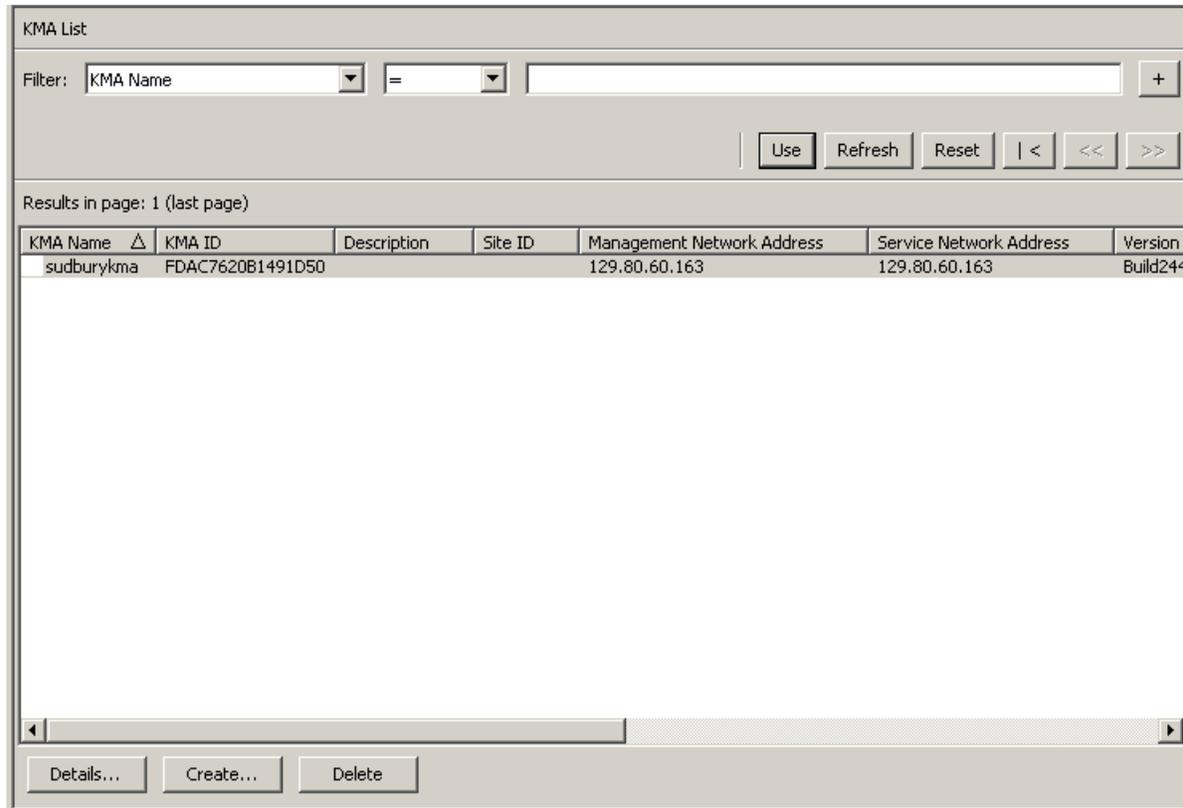
- Affichage des KMA
- Création d'un KMA
- Modification des informations d'un KMA
- Suppression d'un KMA



## Affichage des KMA

Pour afficher les KMA :

Dans le menu System Management (Gestion du système), sélectionnez KMA List (Liste des KMA). L'écran KMA List (Liste des KMA) s'affiche.



Vous pouvez également faire défiler la base de données et filtrer la liste des KMA selon l'un des critères suivants :

- KMA Name (Nom du KMA)
- KMA ID (ID du KMA)
- Description
- Site ID (ID du site)
- Management Network Address (Adresse réseau de gestion)
- Service Network Address (Adresse réseau de service)
- Version
- Failed Login Attempts (Tentatives de connexion ayant échoué)
- Responding (Répondant)
- Response Time (Temps de réponse)
- Replication Lag Size (Taille de latence de réplication)
- Key Pool Ready (Prêt pour le pool de clés)
- Enrolled (Inscrit)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour le KMA.

Les champs et leur description sont fournis ci-dessous :

#### **Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- KMA Name (Nom du KMA)
- Description
- Site ID (ID du site)
- Management Network Address (Adresse réseau de gestion)
- Service Network Address (Adresse réseau de service)
- Version
- Failed Login Attempts (Tentatives de connexion ayant échoué)
- Enrolled (Inscrit)

#### **Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

#### **Zone Filter Value 1 (Valeur de filtre 1)**

Saisissez une valeur dans le champ.

#### **Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer le filtre à la liste affichée.

#### **Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

#### **Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**KMA Name (Nom du KMA)**

Affiche l'identificateur fourni par l'utilisateur qui permet de différencier les KMA d'un cluster.

**KMA ID (ID du KMA)**

Affiche un identificateur unique généré par le système qui permet d'identifier le KMA.

**Description**

Décrit le KMA.

**Site ID (ID du site)**

Décrit le site auquel le KMA appartient.

**Management Network Address (Adresse réseau de gestion)**

Affiche l'adresse IP du KMA sur le réseau de gestion.

**Service Network Address (Adresse réseau de service)**

Affiche l'adresse réseau de service du KMA sur le réseau de gestion.

**Version**

Affiche le numéro de version du logiciel du KMA.

**Failed Login Attempts (Tentatives de connexion ayant échoué)**

Affiche le nombre de tentatives de connexions ayant échoué.

**Responding (Répondant)**

Indique que le KMA est en cours d'exécution. Les valeurs possibles sont True (Vrai) ou False (Faux).

**Response Time (Temps de réponse)**

Affiche le laps de temps (exprimé en millisecondes) que le KMA met à répondre à une requête.

**Replication Lag Size (Taille de latence de réplication)**

Affiche le nombre de mises à jour en attente de réplication.

**Key Pool Ready (Prêt pour le pool de clés)**

Affiche la proportion (en pourcentage) de clés prêtes non allouées.

**Enrolled (Inscrit)**

Indique si l'ajout ou la connexion du KMA au cluster a réussi. Les valeurs possibles sont True (Vrai) ou False (Faux).

Si vous souhaitez créer un KMA, cliquez sur le bouton Create (Créer). Pour plus d'informations, reportez-vous à la section « [Création d'un KMA](#) », page 87 ci-dessous.

Si vous souhaitez visualiser ou modifier les informations d'un KMA, mettez ce dernier en surbrillance dans la liste et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage/Modification des détails d'un KMA](#) », page 90.

Si vous souhaitez supprimer un KMA, cliquez sur le bouton Delete (Supprimer). Pour plus d'informations, reportez-vous à la section « [Suppression d'un KMA](#) », page 93.

## Création d'un KMA

Pour créer un KMA :

1. Dans l'écran KMA List (Liste des KMA), cliquez sur le bouton Create (Créer). La boîte de dialogue Create KMA (Création d'un KMA) s'affiche, l'onglet General (Général) étant activé.

2. Remplissez les champs des paramètres suivants :

### *Onglet General (Général)*

#### **KMA Name (Nom du KMA)**

Saisissez une valeur permettant d'identifier le KMA de manière unique dans un cluster. Cette valeur doit comprendre entre 1 et 64 caractères.

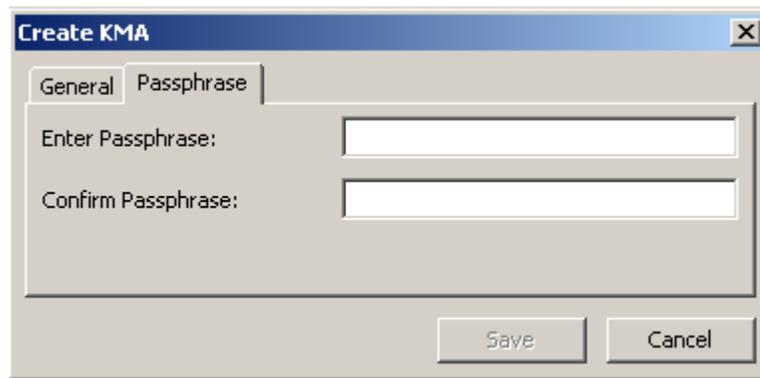
#### **Description**

Saisissez une valeur décrivant le KMA de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

#### **Site ID (ID du site)**

Cliquez sur la flèche pointant vers le bas et sélectionnez le site auquel le KMA appartient. Ce champ est facultatif.

3. Ouvrez l'onglet Passphrase (Phrase de passe).

The image shows a dialog box titled "Create KMA" with a close button (X) in the top right corner. It has two tabs: "General" and "Passphrase". The "Passphrase" tab is selected. Inside the dialog, there are two text input fields. The first is labeled "Enter Passphrase:" and the second is labeled "Confirm Passphrase:". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

4. Remplissez les champs des paramètres suivants, puis cliquez sur le bouton Save (Enregistrer).

#### Enter Passphrase (Saisissez la phrase de passe)

Tapez la phrase de passe associée à cet utilisateur. Une phrase de passe doit contenir entre 8 et 64 caractères. La valeur par défaut est égale à 8.

Conditions requises pour les phrases de passe :

- Une phrase de passe ne doit pas contenir le nom KMA de l'utilisateur.
- Une phrase de passe doit contenir trois des quatre classes de caractères : majuscule, minuscule, nombre ou caractère spécial.

Les caractères spéciaux suivants sont autorisés :

' ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } \ | ; : ' " < > , . / ?

- Les caractères de contrôle, tabulations et sauts de ligne compris, ne sont pas admis.

---

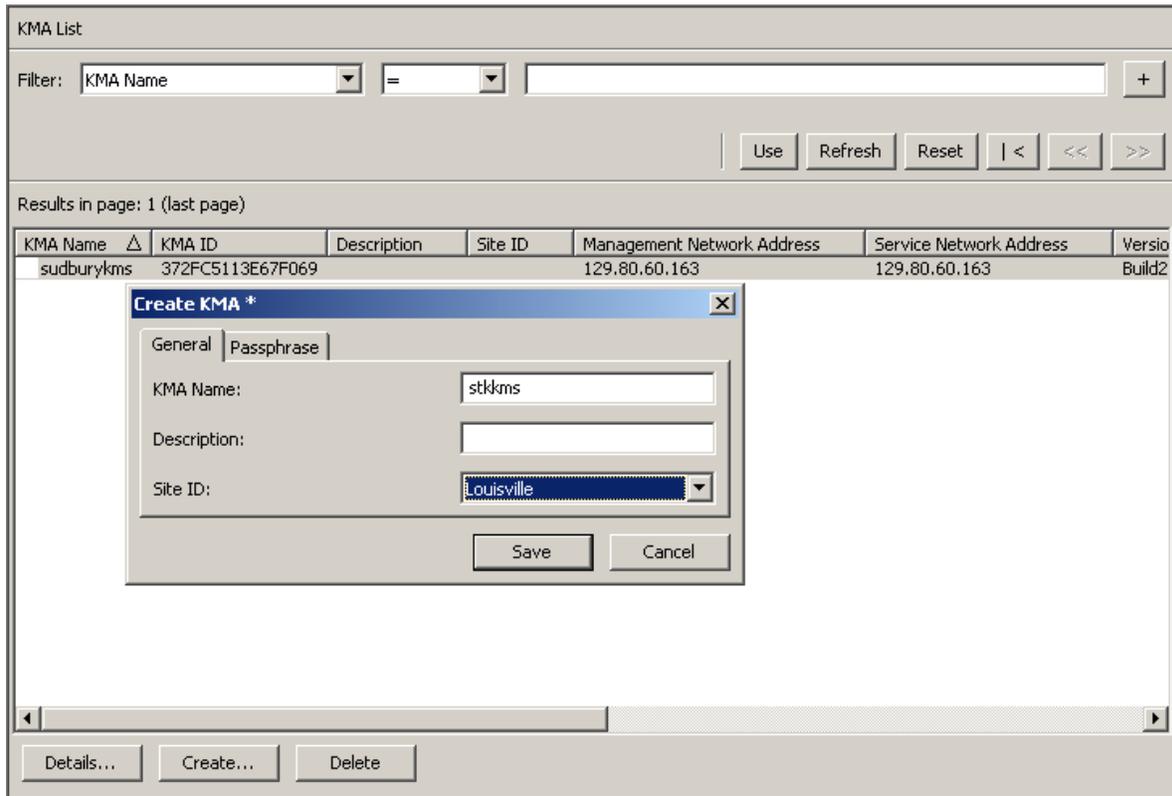
**Remarque** – Pour modifier la longueur minimale requise des phrases de passe, reportez-vous à la section « [Modification des paramètres de sécurité](#) », page 154.

---

#### Confirm Passphrase (Confirmer la phrase de passe)

Saisissez la même valeur que celle indiquée dans le champ de la phrase de passe.

5. L'enregistrement du KMA est ajouté à la base de données et l'entrée s'affiche dans l'écran KMA List (Liste des KMA).



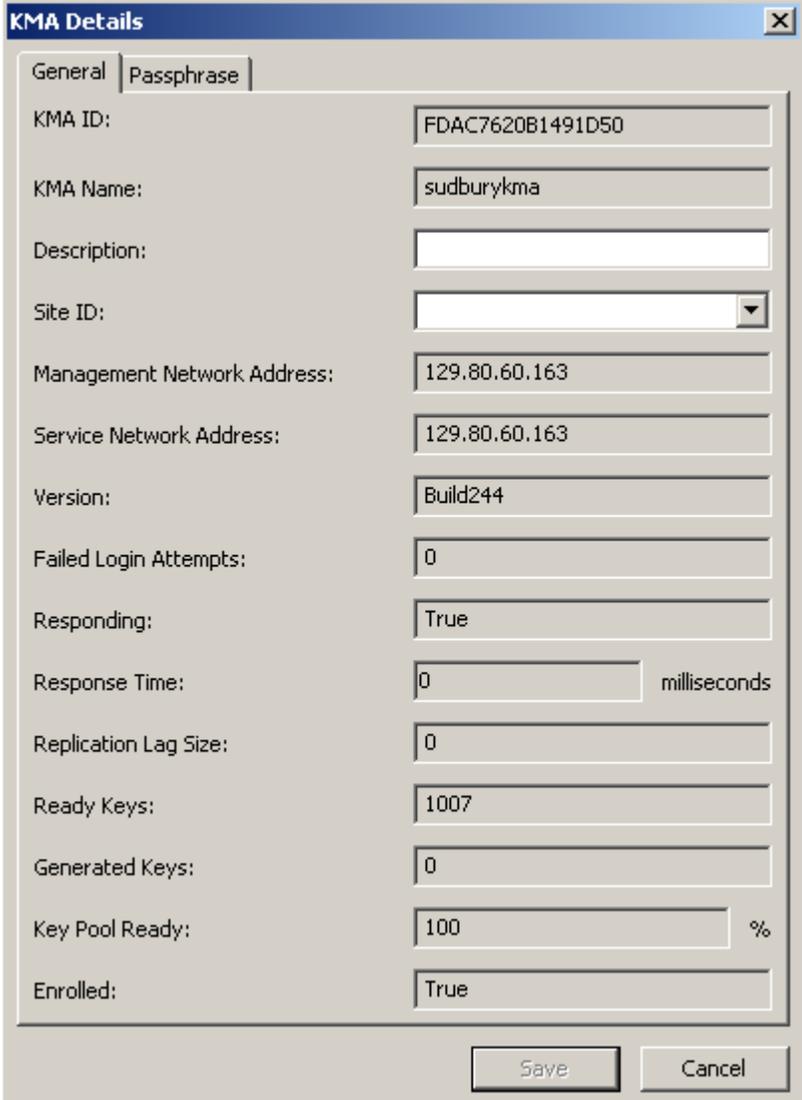
6. Exécutez à présent le programme QuickStart sur les KMAs que vous venez de créer afin de les intégrer au cluster. Pour connaître les procédures d'intégration à un cluster, reportez-vous à la section « [Intégration à un cluster existant](#) », page 38.

## Affichage/Modification des détails d'un KMA

**Remarque** – Si vous n'êtes pas responsable de la sécurité, tous les champs (y compris le bouton Save (Enregistrer)) sont désactivés lors de la visualisation des informations détaillées relatives à un KMA.

Pour modifier les informations détaillées d'un KMA :

1. Dans l'écran KMAs List (Liste des KMA), double-cliquez sur une entrée KMA pour laquelle vous souhaitez obtenir des informations détaillées ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). L'écran KMA Details (Détails du KMA) s'affiche.



The screenshot shows a dialog box titled "KMA Details" with two tabs: "General" and "Passphrase". The "General" tab is active, displaying the following fields:

KMA ID:	FDAC7620B1491D50
KMA Name:	sudburykma
Description:	
Site ID:	
Management Network Address:	129.80.60.163
Service Network Address:	129.80.60.163
Version:	Build244
Failed Login Attempts:	0
Responding:	True
Response Time:	0 milliseconds
Replication Lag Size:	0
Ready Keys:	1007
Generated Keys:	0
Key Pool Ready:	100 %
Enrolled:	True

At the bottom of the dialog box, there are two buttons: "Save" and "Cancel".

2. Sur l'onglet General (Général), modifiez les champs suivants :
  - Description
  - Site ID (ID de site)
3. Activez l'onglet Passphrase (Phrase de passe) et modifiez les paramètres suivants :
  - Enter Passphrase (Saisissez la phrase de passe)
  - Confirm Passphrase (ressaisissez la même phrase de passe).
4. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer).  
L'enregistrement KMA est modifié dans la base de données.

## Définition de la phrase de passe d'un KMA

---

**Remarque** – Vous avez la possibilité de modifier la phrase de passe d'un KMA à condition de ne pas être connecté au dispositif.

---

Lors de la création d'un cluster, une phrase de passe aléatoire est automatiquement assignée au KMA utilisé pour cette opération. Si le KMA doit récupérer le certificat d'une entité à partir d'un autre KMA du cluster car le sien a expiré, vous devez utiliser cette fonction afin de définir la phrase de passe sur une valeur connue.

Pour définir la phrase de passe d'un KMA :

1. Dans l'écran KMA List (Liste des KMA), double-cliquez sur l'entrée de KMA ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). La boîte de dialogue KMA Details (Détails du KMA) s'affiche, l'onglet General (Général) étant activé.
2. Activez l'onglet Passphrase (Phrase de passe) et modifiez les paramètres suivants :
  - Enter Passphrase (Saisissez la phrase de passe)
  - Confirm Passphrase (ressaisissez la même phrase de passe).
3. Cliquez sur le bouton Save (Enregistrer) pour sauvegarder vos modifications. L'entrée de base de données du KMA est modifiée.
4. À l'aide de la console, sur le KMA dont la phrase de passe a été modifiée, sélectionnez la fonction de connexion du KMA au cluster. Le KMA ne peut pas communiquer avec le cluster avant d'être à nouveau connecté.

## Suppression d'un KMA

---

**Important** – Avant de supprimer un KMA, mettez-le hors ligne au moyen de la fonction Shutdown KMA (Arrêter le KMA) de la console. Si cette opération échoue, le KMA continue à fonctionner en dehors du cluster et envoie des « informations obsolètes » aux agents et aux utilisateurs.

En général, cette commande ne sera utilisée que pour supprimer du cluster un KMA en panne. Toutefois, elle peut aussi servir à retirer un KMA mis hors service. Dans ce cas, il est néanmoins préférable d'utiliser la fonction Reset KMA (Réinitialiser le KMA) de la console avec l'option de mise à zéro. Cette fonction supprime le KMA du cluster et efface toutes les informations du disque du KMA mis hors service.

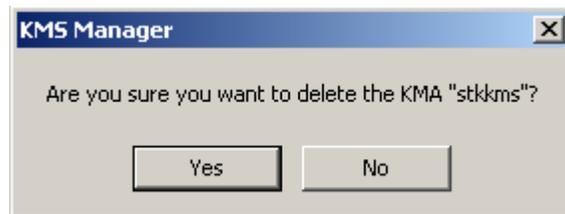
Si vous souhaitez réintégrer dans un cluster un KMA supprimé, vous devez réinitialiser le KMA selon son état par défaut défini en usine et sélectionner l'option 2 du programme QuickStart.

---

Cette option donne au responsable de la sécurité la possibilité de supprimer un KMA hors service.

Pour supprimer un KMA :

1. Dans l'écran KMAs List (Liste des KMA), mettez le KMA à supprimer en surbrillance et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue suivante s'affiche, vous demandant de confirmer la suppression du KMA sélectionné.



2. Cliquez sur Yes (Oui) pour confirmer l'opération. Le KMA sélectionné est supprimé et vous revenez à l'écran KMAs List (Liste des KMA). Le système efface également toutes les entrées associées au KMA et non utilisées par d'autres entités.

---

## Menu User List (Liste des utilisateurs)

L'option de menu User List (Liste des utilisateurs) vous permet d'effectuer les opérations suivantes :

- Affichage des utilisateurs
- Création d'un utilisateur
- Modification des informations sur un utilisateur existant
- Suppression d'un utilisateur existant



## Affichage des utilisateurs

Pour afficher les utilisateurs :

Dans le menu System Management (Gestion du système), sélectionnez **User List** (Liste des utilisateurs). L'écran User List (Liste des utilisateurs) s'affiche.

User ID	Description	Roles	Enabled	Failed Login Attempts
AUD	Test User	Auditor	True	0
All	Test User	Backup Operator, Compliance Officer, Operator, Security...	True	0
BO	test User	Backup Operator	True	0
CO	Test User	Compliance Officer	True	0
OP	Test User	Operator	True	0
SO		Backup Operator, Compliance Officer, Operator, Security...	True	0
nancy		Auditor	True	0
wally	night shift janitor	Security Officer	True	0

Vous pouvez également faire défiler la base de données et filtrer la liste des utilisateurs selon l'un des critères suivants :

- User ID (ID utilisateur)
- Description
- Roles (Rôles)
- Enabled (Activé)
- Failed Login Attempts (Tentatives de connexion ayant échoué)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour l'utilisateur.

Les champs et leur description sont fournis ci-dessous :

**Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- User ID (ID utilisateur)
- Description
- Enabled (Activé)
- Failed Login Attempts (Tentatives de connexion ayant échoué)

**Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

**Zone Filter Value 1 (Valeur de filtre 1)**

Saisissez une valeur dans le champ.

**Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer le filtre à la liste affichée.

**Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

**Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**User ID (ID utilisateur)**

Affiche un identificateur unique, communément appelé Nom d'utilisateur et permettant de différencier les utilisateurs d'un cluster.

**Description**

Décrit l'utilisateur.

**Roles (Rôles)**

Affiche la liste des rôles de sécurité associés à l'utilisateur. Les rôles permettent à l'utilisateur d'effectuer diverses opérations.

**Enabled (Activé)**

Indique le statut de l'utilisateur. Les valeurs possibles sont **True** (Vrai) ou **False** (Faux).

**Failed Login Attempts (Tentatives de connexion ayant échoué)**

Indique le nombre de tentatives de connexion ayant échoué.

Si vous souhaitez créer un utilisateur, cliquez sur le bouton Create (Créer). Pour plus d'informations, reportez-vous à la section « [Création d'un utilisateur](#) », page 98.

Si vous souhaitez modifier les informations d'un utilisateur, mettez ce dernier en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage/Modification des détails d'un utilisateur](#) », page 100.

Si vous souhaitez supprimer un utilisateur, cliquez sur le bouton Delete (Supprimer). Pour plus d'informations, reportez-vous à la section « [Suppression d'un utilisateur](#) », page 102.

Un responsable de la sécurité est habilité à définir la phrase de passe d'un utilisateur si celle-ci et/ou le certificat a été compromis(e). Pour connaître les procédures relatives à la définition de la phrase de passe d'un utilisateur, reportez-vous à la section « [Définition de la phrase de passe d'un utilisateur](#) », page 101.

Les utilisateurs peuvent également changer leur propre phrase de passe. Pour plus d'informations à ce sujet, reportez-vous à la section « [Modification de la phrase de passe](#) », page 76.

## Création d'un utilisateur

Pour créer un utilisateur :

1. Dans l'écran User List (Liste des utilisateurs), cliquez sur le bouton Create (Créer). La boîte de dialogue Create User (Création d'un utilisateur) s'affiche, l'onglet General (Général) étant activé.



The image shows a 'Create User' dialog box with a title bar containing a close button (X). It has two tabs: 'General' and 'Passphrase'. The 'General' tab is active. Inside the dialog, there are two text input fields: 'User ID:' and 'Description:'. Below these are five checkboxes under the heading 'Roles:': 'Auditor', 'Backup Operator', 'Compliance Officer', 'Operator', and 'Security Officer'. At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

2. Remplissez les champs des paramètres suivants :

### *Onglet General (Général)*

#### **User ID (ID utilisateur)**

Saisissez une valeur permettant d'identifier l'utilisateur de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

#### **Description**

Saisissez une valeur décrivant l'utilisateur de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

#### **Roles (Rôles)**

Cochez les cases situées en regard des rôles associés à l'utilisateur.

*Onglet Passphrase (Phrase de passe)*

3. Activez l'onglet Passphrase (Phrase de passe).

The image shows a 'Create User' dialog box with a 'Passphrase' tab selected. It contains two text input fields: 'Enter Passphrase:' and 'Confirm Passphrase:'. At the bottom, there are 'Save' and 'Cancel' buttons.

4. Remplissez les champs des paramètres suivants :

**Enter Passphrase (Saisissez la phrase de passe)**

Tapez la phrase de passe associée à cet utilisateur. La valeur minimale est de 8 tandis que la valeur maximale est de 64 caractères. La valeur par défaut est égale à 8.

Conditions requises pour les phrases de passe :

- Une phrase de passe ne doit pas contenir l'ID utilisateur de la personne.
- Une phrase de passe doit contenir trois des quatre classes de caractères : majuscule, minuscule, nombre ou caractère spécial.

Les caractères spéciaux suivants sont autorisés :

' ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } \ | ; : ' " < > , . / ?

- Les caractères de contrôle, tabulations et sauts de ligne compris, ne sont pas admis.

---

**Remarque** – Pour modifier la longueur minimale requise des phrases de passe, reportez-vous à la section « [Modification des paramètres de sécurité](#) », page 154.

---

**Confirm Passphrase (Confirmer la phrase de passe)**

Saisissez la même valeur que celle indiquée dans le champ de la phrase de passe.

5. Cliquez sur le bouton Save (Enregistrer). L'enregistrement de l'utilisateur est ajouté à la base de données. Le nouvel utilisateur s'affiche dans la User List (Liste des utilisateurs).

## Affichage/Modification des détails d'un utilisateur

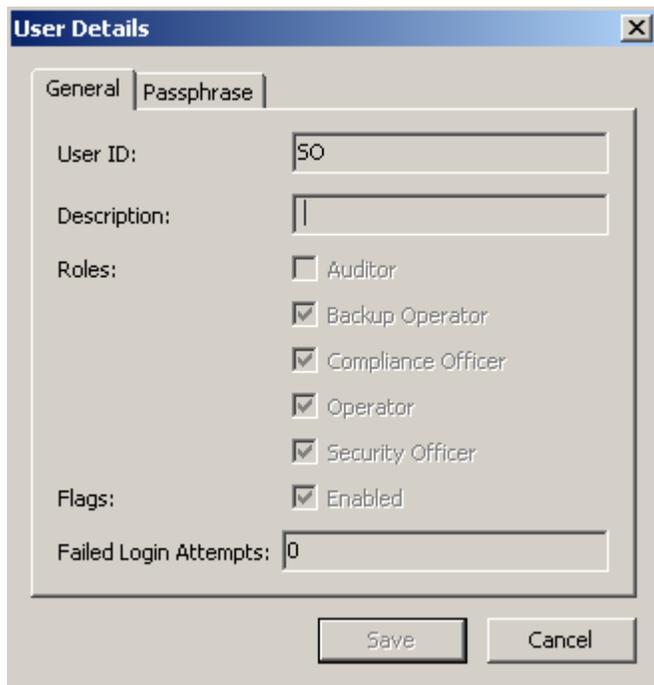
---

**Remarque** – Les responsables de la sécurité actuellement connectés ne peuvent pas modifier leurs enregistrements.

---

Pour modifier les informations de l'utilisateur :

1. Dans l'écran Users List (Liste des utilisateurs), double-cliquez sur un utilisateur pour lequel vous souhaitez obtenir des informations détaillées ou mettez en surbrillance un enregistrement utilisateur et cliquez sur le bouton Details (Détails). L'écran User Details (Détails de l'utilisateur) s'affiche, avec tous les champs (y compris le bouton Save (Enregistrer)) désactivés.



The screenshot shows a 'User Details' dialog box with the following fields and values:

- User ID: 50
- Description: |
- Roles:  Auditor,  Backup Operator,  Compliance Officer,  Operator,  Security Officer
- Flags:  Enabled
- Failed Login Attempts: 0

Buttons: Save, Cancel

2. Sur l'onglet General (Général), modifiez les paramètres suivants :

- User ID (ID utilisateur)
- Description
- Roles (Rôles)
- Flags - Enabled (Indicateurs - Activés)
- Failed Login Attempts (Tentatives de connexion ayant échoué)

Le champ Failed Login Attempts (Tentatives de connexion ayant échoué) affiche-le nombre de tentatives de connexions ayant échoué.

3. Activez l'onglet Passphrase (Phrase de passe) et modifiez les paramètres suivants :

- Enter Passphrase (Saisissez la phrase de passe)
- Confirm Passphrase (Confirmer la phrase de passe)

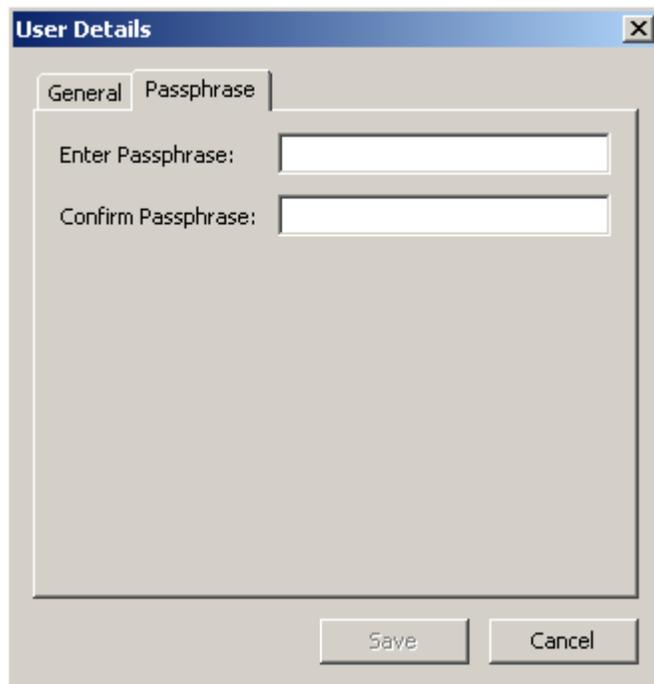
4. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer). L'enregistrement utilisateur est modifié dans la base de données.

## Définition de la phrase de passe d'un utilisateur

En tant que responsable de la sécurité, vous êtes habilité à définir la phrase de passe d'un utilisateur si celle-ci et/ou le certificat a été compromis(e). Un nouveau certificat est généré lorsque l'utilisateur se sert de la nouvelle phrase de passe pour se connecter au KMA.

Pour définir la phrase de passe d'un utilisateur :

1. Dans l'écran User List (Liste des utilisateurs), double-cliquez sur l'utilisateur dont vous souhaitez sélectionner la phrase de passe ou mettez l'utilisateur en surbrillance et cliquez sur le bouton Details (Détails).
2. L'écran User Details (Détails de l'utilisateur) s'affiche. Activez l'onglet Passphrase (Phrase de passe).



The image shows a dialog box titled "User Details" with a close button (X) in the top right corner. It has two tabs: "General" and "Passphrase". The "Passphrase" tab is selected. Inside the dialog, there are two text input fields. The first is labeled "Enter Passphrase:" and the second is labeled "Confirm Passphrase:". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

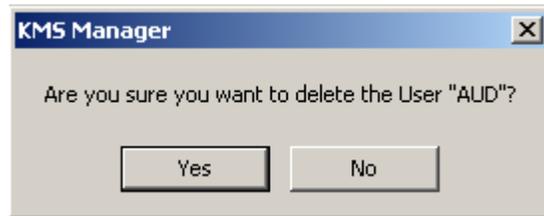
3. Dans le champ Enter Passphrase (Saisissez la phrase de passe), tapez la phrase de passe assignée par le responsable de la sécurité lors de la création du compte utilisateur.
4. Dans le champ Confirm Passphrase (Confirmer la phrase de passe), tapez la même valeur que celle indiquée à l'étape 3. La nouvelle phrase de passe associée à l'enregistrement utilisateur est enregistrée. Vous revenez à l'écran User List (Liste des utilisateurs).

## Suppression d'un utilisateur

Il est impossible à un utilisateur de se supprimer lui-même.

Pour supprimer un utilisateur :

1. Dans l'écran Users List (Liste des utilisateurs), sélectionnez l'utilisateur à supprimer et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue suivante s'affiche, vous demandant de confirmer la suppression de l'utilisateur sélectionné.



2. Cliquez sur Yes (Oui) pour supprimer l'utilisateur. L'utilisateur actuellement sélectionné est supprimé et vous revenez à l'écran User List (Liste des utilisateurs), où l'utilisateur supprimé ne figure plus dans la liste.

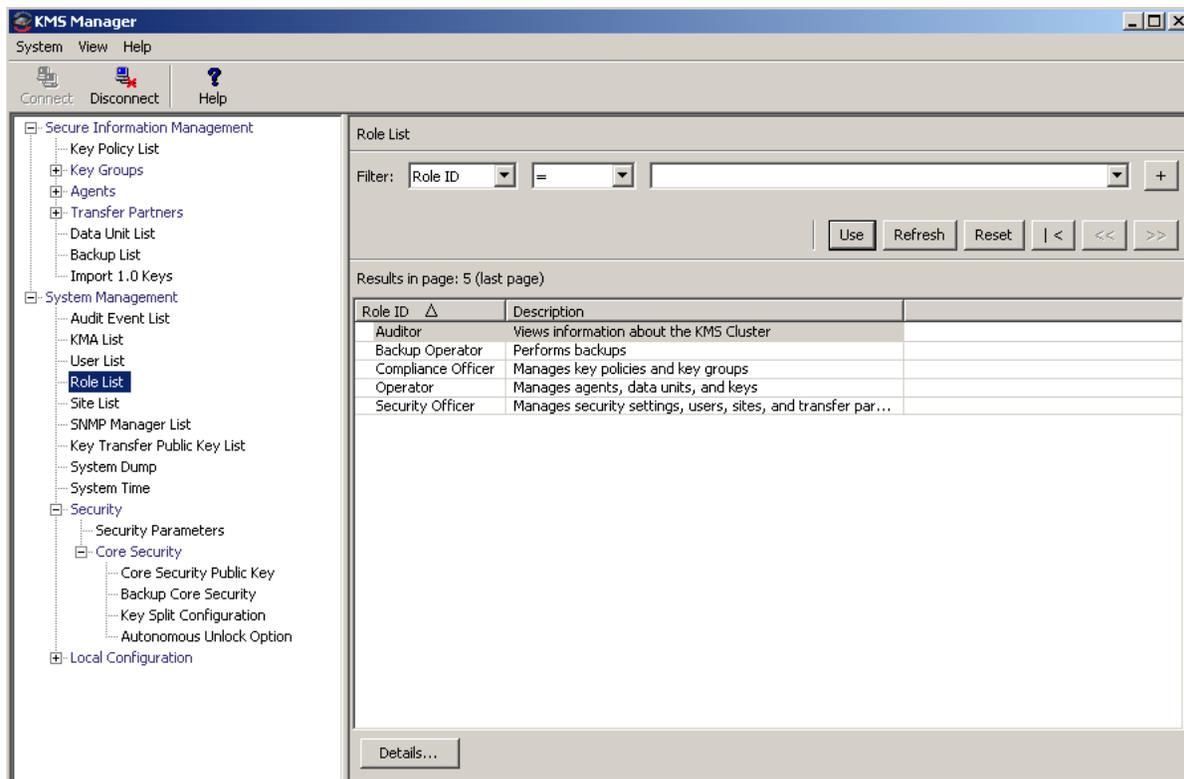
## Menu Role List (Liste des rôles)

L'option de menu Role List (Liste des rôles) vous donne également la possibilité d'afficher les rôles des utilisateurs. Les rôles sont des regroupements logiques fixes de diverses opérations système qu'un utilisateur est habilité à effectuer. Un utilisateur peut se voir assigner plusieurs rôles.

### Affichage des rôles

Pour afficher les rôles :

Dans le menu System Management (Gestion du système), sélectionnez **Role List** (Liste des rôles). L'écran Role List (Liste des rôles) s'affiche.



Vous pouvez également faire défiler la base de données et filtrer la liste des rôles selon l'un des critères suivants :

- Role ID (ID de rôle)
- Description

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée.

Les champs et leur description sont fournis ci-dessous :

**Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Role ID (ID de rôle)
- Description

**Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Vide
- Non vide

**Zone Filter Value 1 (Valeur de filtre 1)**

Saisissez une valeur dans le champ.

**Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

**Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**Role ID (ID de rôle)**

Affiche l'identificateur unique différenciant les rôles de sécurité les uns des autres.

**Description**

Décrit le rôle.

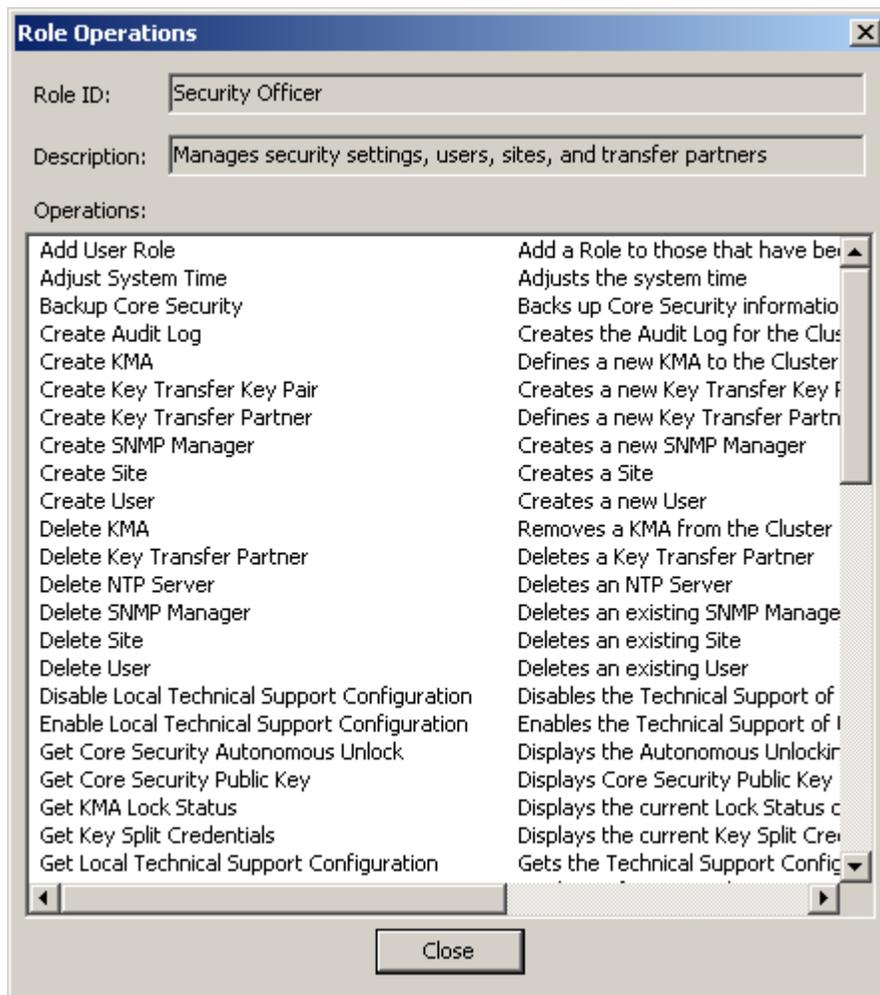
Pour obtenir plus d'informations sur un rôle, mettez une entrée de rôle en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage des opérations associées à un rôle](#) », page 105.

## Affichage des opérations associées à un rôle

La boîte de dialogue Role Operations (Opérations associées à un rôle) vous permet de visualiser un rôle et les opérations autorisées associées.

Pour afficher les opérations relatives à un rôle spécifique :

1. Dans l'écran Role List (Liste des rôles), mettez un rôle en surbrillance et cliquez sur le bouton Details (Détails). La boîte de dialogue Role Operations (Opérations associées à un rôle) s'affiche, indiquant les opérations associées au rôle sélectionné.



2. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue. Vous revenez à l'écran Role List (Liste des rôles).

---

## Menu Site List (Liste des sites)

Un site est un emplacement physique, comprenant au moins un KMA, auquel plusieurs agents (hôtes et cluster KMS) sont connectés. Les sites permettent aux agents de répondre aux équilibrages de charges ou aux échecs des KMA plus efficacement en se connectant à un autre KMA du site local plutôt qu'à un KMA distant.

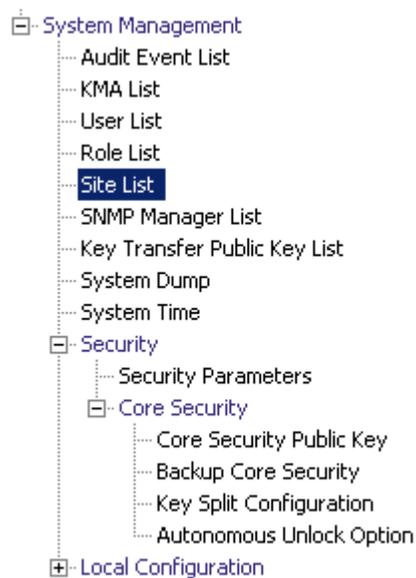
L'option de menu Site List (Liste des sites) vous permet d'effectuer les opérations suivantes :

- Affichage des sites
- Création d'un site
- Modification des informations d'un site
- Suppression d'un site

---

**Remarque** – Un opérateur peut uniquement afficher des sites. Un responsable de la sécurité peut gérer les sites.

---



## Affichage des sites

Pour afficher les sites :

Dans le menu System Management (Gestion du système), sélectionnez Site List (Liste des sites). L'écran Site List (Liste des sites) s'affiche.

Site ID	Description
LaBarge	This is a site in Wyoming
Louisville	another site
Sitenumba1	This is a site
Toronto	Yada is a site

Vous pouvez également faire défiler la base de données et filtrer la liste des sites selon l'un des critères suivants :

- Site ID (ID du site)
- Description

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour le site.

Les champs et leur description sont fournis ci-dessous :

### Filter (Filtre)

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Site ID (ID du site)
- Description

### **Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~

### **Zone Filter Value 1 (Valeur de filtre 1)**

Saisissez une valeur dans le champ.

### **Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer le filtre à la liste affichée.

### **Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

### **Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

### **Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

### **Site ID (ID du site)**

Permet d'identifier le site de manière unique.

### **Description**

Décrit le site.

Cliquez sur le bouton Create (Créer) pour créer un site. Pour plus d'informations, reportez-vous à la section « [Création d'un site](#) », page 110.

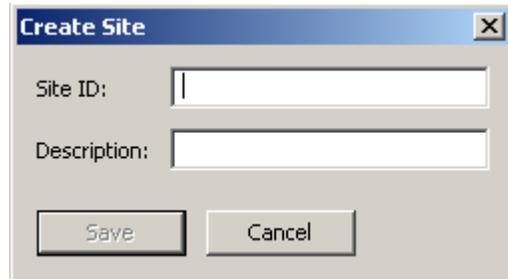
Si vous souhaitez visualiser ou modifier les informations d'un site, mettez ce dernier en surbrillance dans la liste et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage/Modification des détails d'un site](#) », page 112.

Cliquez sur le bouton Delete (Supprimer) pour supprimer le site sélectionné. Pour plus d'informations, reportez-vous à la section « [Suppression d'un site](#) », page 113.

## Création d'un site

Pour créer un site :

1. Dans l'écran Site List (Liste des sites), cliquez sur le bouton Create (Créer). La boîte de dialogue Create Site (Création d'un site) s'affiche.



2. Remplissez les champs des paramètres suivants :

### Site ID (ID du site)

Saisissez une valeur permettant d'identifier le site de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

### Description

Saisissez une valeur décrivant le site de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

Un exemple de boîte de dialogue remplie est présenté ci-dessous.



3. Cliquez sur le bouton Save (Enregistrer). Le nouveau site est enregistré et stocké dans la base de données. Il figure dans la liste des sites.

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

## Affichage/Modification des détails d'un site

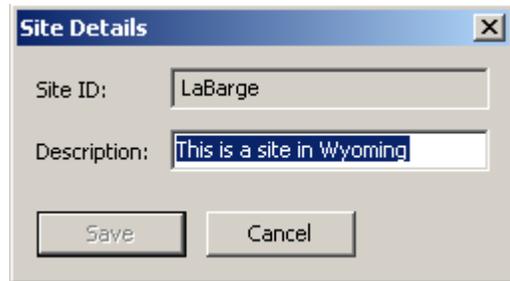
---

**Remarque** – Si vous n'êtes pas responsable de la sécurité, tous les champs (y compris le bouton Save (Enregistrer)) sont désactivés lors de la visualisation des informations détaillées relatives à un site.

---

Pour modifier les informations détaillées d'un site :

1. Dans l'écran Site List (Liste des sites), cliquez sur le bouton Details (Détails). La boîte de dialogue Site Details (Détails d'un site) s'affiche.



The screenshot shows a dialog box titled "Site Details". It has a close button in the top right corner. There are two text input fields: "Site ID" containing "LaBarge" and "Description" containing "This is a site in Wyoming". At the bottom, there are two buttons: "Save" and "Cancel".

2. Modifiez le champ Description et cliquez sur le bouton Save (Enregistrer). Les détails du site sont modifiés et stockés dans la base de données.

## Suppression d'un site

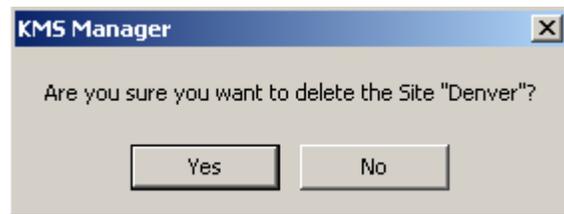
---

**Remarque** – Si le site est en cours d'utilisation, (c.-à-d., des agents ou KMA sont spécifiés comme étant sur le site), ces entités doivent d'abord être supprimées ou déplacées vers un autre site avant que vous puissiez le supprimer.

---

Pour supprimer un site :

1. Dans l'écran Site List (Liste des sites), mettez le site à supprimer en surbrillance et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue suivante s'affiche, vous invitant à confirmer vos actions.



2. Cliquez sur Yes (Oui) pour supprimer le site. Le site sélectionné est supprimé et vous revenez à l'écran Site List (Liste des sites).

---

## Menu SNMP Manager List (Liste des gestionnaires SNMP)

### Affichage des gestionnaires SNMP d'un KMA

Pour afficher les gestionnaires SNMP :

Dans le menu System Management (Gestion du système), sélectionnez SNMP Manager List (Liste des gestionnaires SNMP). L'écran SNMP Manager List (Liste des gestionnaires SNMP) s'affiche.

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

Vous pouvez également faire défiler la base de données et filtrer la liste des gestionnaires SNMP selon l'un des critères suivants :

- SNMP Manager ID (ID du gestionnaire SNMP)
- Description
- Network Address (Adresse réseau)
- Enabled (Activé)
- User Name (Nom d'utilisateur)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour le gestionnaire SNMP.

Les champs et leur description sont fournis ci-dessous :

#### **Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- SNMP Manager ID (ID du gestionnaire SNMP)
- Description
- Network Address (Adresse réseau)
- Enabled (Activé)
- User Name (Nom d'utilisateur)

#### **Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

#### **Zone Filter Value 1 (Valeur de filtre 1)**

Saisissez une valeur dans le champ.

#### **Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer le filtre à la liste affichée.

#### **Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

#### **Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**SNMP Manager ID (ID du gestionnaire SNMP)**

Affiche l'identificateur unique défini par l'utilisateur pour le gestionnaire SNMP.

**Description**

Affiche une description du gestionnaire SNMP. Ce champ est facultatif.

**Network Address (Adresse réseau)**

Affiche l'adresse réseau qui servira à envoyer un déROUTement SNMP.

**Enabled (Activé)**

Indique si ce gestionnaire SNMP est activé ou non.

**User Name (Nom d'utilisateur)**

Affiche le nom d'utilisateur qui servira à établir une connexion SNMPv3 de confiance sécurisée avec ce gestionnaire SNMP.

Cliquez sur le bouton Create (Créer) afin de définir un nouveau gestionnaire SNMP. Pour plus d'informations, reportez-vous à la section « [Création d'un nouveau gestionnaire SNMP](#) » ci-dessous.

Si vous souhaitez visualiser ou modifier les informations d'un gestionnaire SNMP, mettez l'entrée en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage/Modification des détails d'un gestionnaire SNMP](#) », page 119.

Cliquez sur le bouton Delete (Supprimer) afin de supprimer le gestionnaire SNMP sélectionné. Pour plus d'informations, reportez-vous à la section « [Suppression d'un gestionnaire SNMP](#) », page 120.

## Création d'un nouveau gestionnaire SNMP

1. Dans l'écran SNMP Managers List (Liste des gestionnaires SNMP), cliquez sur le bouton Create (Créer). La boîte de dialogue Create SNMP Manager (Création d'un gestionnaire SNMP) s'affiche.

The screenshot shows a dialog box titled "Create SNMP Manager". It contains the following fields and controls:

- SNMP Manager ID: [Text input field]
- Description: [Text input field]
- Network Address: [Text input field]
- Flags:  Enabled
- User Name: [Text input field]
- Passphrase: [Text input field]
- Confirm Passphrase: [Text input field]
- Buttons: Save, Cancel

2. Remplissez les champs des paramètres suivants :

### SNMP Manager ID (ID du gestionnaire SNMP)

Saisissez une valeur permettant d'identifier le gestionnaire SNMP de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

### Description

Saisissez une valeur décrivant le gestionnaire SNMP. Cette valeur doit comprendre entre 1 et 64 caractères.

### Network Address (Adresse réseau)

Tapez l'adresse réseau du gestionnaire SNMP.

### Flags - Enabled (Indicateurs - Activés)

Cochez cette case pour indiquer si la fonction SNMP est activée ou non.

### User Name (Nom d'utilisateur)

Tapez le nom d'utilisateur qui servira à authentifier le gestionnaire SNMP.

### Enter Passphrase (Saisissez la phrase de passe)

Tapez la phrase de passe qui servira à authentifier le gestionnaire SNMP.

**Confirm Passphrase (Confirmer la phrase de passe)**

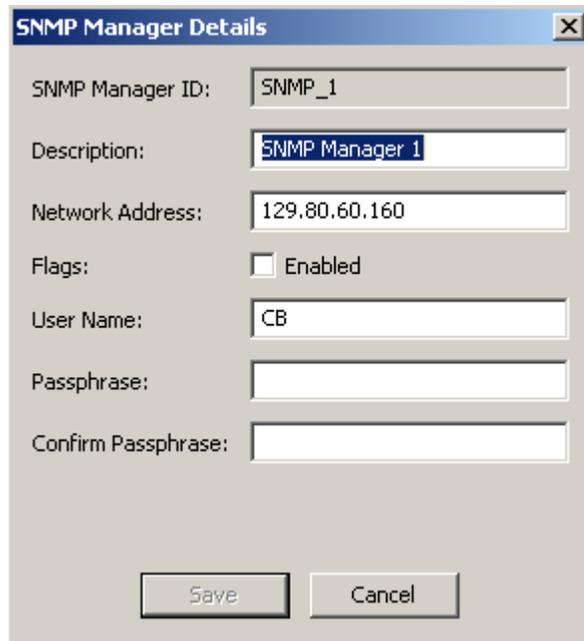
Saisissez la même phrase de passe que celle indiquée dans le champ Passphrase.

3. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer) afin d'enregistrer les informations. La nouvelle entrée SNMP Manager (Gestionnaire SNMP) et le profil associé sont stockés dans la base de données.

## Affichage/Modification des détails d'un gestionnaire SNMP

Pour afficher ou modifier les détails d'un gestionnaire SNMP :

1. Dans l'écran SNMP Managers List (Liste des gestionnaires SNMP), double-cliquez sur une entrée de gestionnaire SNMP pour laquelle vous souhaitez davantage d'informations et cliquez sur le bouton Détails (Détails). La boîte de dialogue SNMP Manager Details (Détails d'un gestionnaire SNMP) s'affiche.



The screenshot shows a dialog box titled "SNMP Manager Details". It contains the following fields and controls:

- SNMP Manager ID:
- Description:
- Network Address:
- Flags:  Enabled
- User Name:
- Passphrase:
- Confirm Passphrase:
- Buttons: Save, Cancel

2. Modifiez les paramètres selon les besoins.
3. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer) afin d'enregistrer les modifications.

---

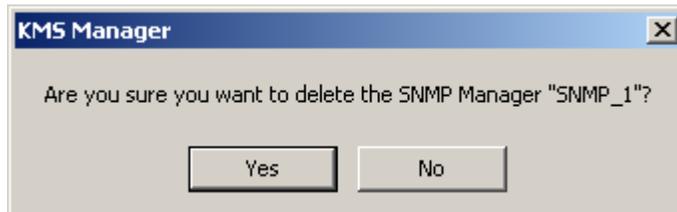
**Remarque** – Chaque fois que vous modifiez les détails d'un gestionnaire SNMP, vous devez à nouveau indiquer la phrase de passe.

---

## Suppression d'un gestionnaire SNMP

Pour supprimer un gestionnaire SNMP :

1. Dans l'écran SNMP Managers List (Liste des gestionnaires SNMP), mettez le gestionnaire SNMP à supprimer en surbrillance et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue de confirmation de la suppression du gestionnaire SNMP s'affiche.



2. Cliquez sur le bouton Yes (Oui) afin de supprimer le gestionnaire SNMP. Le gestionnaire SNMP sélectionné est supprimé et vous revenez à l'écran SNMP Managers List (Liste des gestionnaires SNMP).

---

# Transfert de clés

## Présentation

Le transfert de clés, également appelé partage de clés, permet aux clés et unités de données associées d'être échangées en toute sécurité entre partenaires. Il est obligatoire pour l'échange de supports chiffrés. Ce processus exige de la part des deux parties impliquées dans le transfert d'établir une paire de clés publique/privée et de fournir la clé publique à l'autre partie.

Chaque partie enregistre la clé publique de l'autre dans son propre cluster KMS. Une fois cette configuration initiale terminée, l'expéditeur utilise la fonction d'exportation de clés, laquelle lui permet de générer un fichier de transfert qu'il transmet au destinataire. Ce dernier utilise ensuite la fonction d'importation de clés afin d'importer les clés et les unités de données associées dans son cluster KMS.

Le fichier de transfert est signé au moyen de la clé privée de l'expéditeur et chiffré à l'aide de la clé publique du destinataire. Cela permet au destinataire de déchiffrer le fichier de transfert à l'aide de sa propre clé privée. Il peut ainsi vérifier que le fichier a bien été généré par l'expéditeur attendu au moyen de sa clé publique.

## Fonction Key Transfer Partners (Partenaires de transfert de clés)

La fonction Key Transfer Partners (Partenaires de transfert de clés) permet de déplacer des clés d'un cluster KMS vers un autre. En général, cette fonction sert à échanger des bandes entre entreprises ou au sein d'une entreprise si plusieurs clusters sont configurés en vue de traiter de nombreux sites.

Le processus de transfert de clés implique les étapes suivantes :

- Chaque cluster KMS configure l'autre comme partenaire de transfert. Cette procédure s'effectue généralement une seule fois.
- L'utilisateur exporte des clés d'un cluster KMS en vue de les importer dans l'autre. Cette étape peut se produire à de nombreuses reprises.

## Processus de transfert de clés

Dans le système de gestion des clés, vous devez effectuer un certain nombre de tâches dans un ordre précis. Comme ces tâches impliquent plusieurs rôles d'utilisateur, les procédures proprement dites sont décrites dans différents chapitres de ce guide.

### Configuration de partenaires de transfert de clés

Pour déplacer des clés, vous devez configurer un partenaire de transfert pour les deux clusters KMS participant à cette opération.

**Dans la procédure suivante, C1 désigne le premier cluster KMS et C2, le second.**

#### Administrateur de C1 (rôle Security Officer) :

1. Procurez-vous les informations de clé publique relatives à C1 (votre cluster). Pour ce faire, ouvrez le menu Key Transfer Public Key List (Liste des clés publiques de transfert). Reportez-vous aux sections « [Affichage de la liste de clés publiques de transfert](#) », page 137 et « [Affichage des informations détaillées sur les clés publiques de transfert](#) », page 140.
2. Copiez puis collez l'ID de clé publique et la clé publique dans un e-mail ou toute autre forme de communication convenue avec votre interlocuteur. Envoyez ces informations à l'administrateur de C2.

---

**Remarque** – La méthode de communication proprement dite doit être suffisamment sécurisée pour que C2 soit assuré de bien recevoir des informations provenant de C1. Un mécanisme, l'empreinte, permet d'empêcher la modification de ces informations en cours de transfert.

---

#### Administrateur de C2 (rôle Security Officer) :

3. Administrateur de C2 : saisissez les informations de clé publique de C1 dans le cluster KMS via le menu Transfer Partner List (Liste des partenaires de transfert). Reportez-vous à la section « [Menu Transfer Partner List \(Liste des partenaires de transfert\)](#) », page 126.
4. Cliquez sur le bouton Create (Créer). Indiquez le nom du partenaire de transfert, donnez une description et fournissez les coordonnées nécessaires. Déterminez l'utilisation future de ce partenaire. Reportez-vous à la section « [Création d'un partenaire de transfert](#) », page 130.
5. Activez l'onglet Public Keys (Clés publiques). Remplissez les champs Public Key ID (ID de clé publique) et Public Key (Clé publique) avec les informations que vous a fournies C1.

Une fois la clé publique indiquée, le système calcule l'empreinte. Il est préférable que les administrateurs de C1 et de C2 communiquent entre eux au moyen d'un autre mécanisme que celui utilisé pour le transfert de la clé proprement dite.

Les deux administrateurs doivent consulter leur KMS et vérifier la concordance de leurs empreintes respectives. Une incohérence indique que la clé a été endommagée ou modifiée lors du transfert.

6. Si l'empreinte est exacte, cliquez sur Save (Enregistrer). Le système demande un quorum. Cela s'explique par le fait que les opérations d'exportation de clés rendues possibles à ce stade pourraient servir à extraire des clés valables du cluster KMS. C1 est dorénavant configuré comme partenaire de transfert dans le cluster KMS C2.

**Administrateur de C2 (rôle Security Officer) :**

7. Recommencez l'étape 1 et l'étape 2, cette fois pour le cluster KMS C2.

**Administrateur de C1 (rôle Security Officer) :**

8. Recommencez la procédure de l'étape 3 à l'étape 6 afin d'ajouter la clé publique de C2 à C1.

**Administrateur de C1 (rôle Compliance Officer) :**

9. C1 doit configurer des groupes de clés pouvant être envoyés à C2. Reportez-vous à la section « [Affichage des assignations de groupes de clés](#) », page 208.

**Administrateur de C2 (rôle Compliance Officer) :**

10. C2 doit configurer des groupes de clés pouvant récupérer des clés à partir de C1. Reportez-vous à la section « [Affichage des assignations de groupes de clés](#) », page 208.
11. Sélectionnez le partenaire de transfert voulu.
12. Sélectionnez un ou plusieurs groupes de clés non autorisés, puis cliquez sur le bouton Move to (Déplacer vers)  afin de les ajouter à la liste des groupes de clés. Reportez-vous à la section « [Ajout d'un groupe de clés à un partenaire de transfert](#) », page 209.

## Exportation/Importation de clés

La procédure suivante sert à exporter des clés d'un cluster KMS afin de les importer dans un autre. Elle peut être effectuée à de nombreuses reprises.

**Dans la procédure suivante, C1 désigne le premier cluster KMS et C2, le second. Ces instructions ont pour objectif d'autoriser C2 à exporter des clés qui seront ensuite importées dans C1.**

### Administrateur de C2 (rôle Operator) :

1. Pour échanger des clés, affichez l'écran Data Unit List (Liste des unités de données). Reportez-vous à la section « [Affichage des unités de données](#) », page 241.
2. Sélectionnez une ou plusieurs unités de données (bandes) à envoyer de C2 vers C1. La balise externe (External Tag) correspond au code à barres des bandes.
3. Cliquez sur le bouton Export Keys (Exporter des clés) pour afficher la boîte de dialogue.
4. Sélectionnez le partenaire de transfert cible, choisissez le nom du fichier d'exportation des clés si nécessaire, puis cliquez sur Start (Commencer). Le fichier de transfert est créé.  
Seules les clés faisant partie des groupes de clés dont l'exportation vers C1 est autorisée sont effectivement exportées.
5. Envoyez le fichier de transfert à l'administrateur de C1 par e-mail ou toute autre forme ou méthode de communication convenue au préalable entre vous pour déplacer des fichiers.

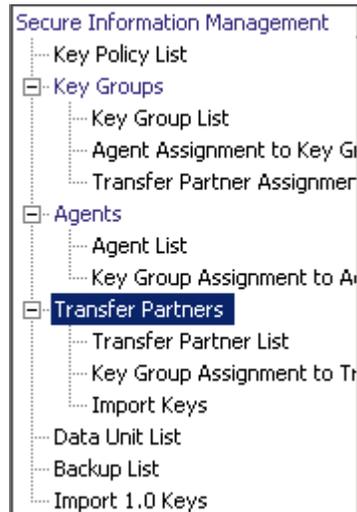
### Administrateur de C1 (rôle Operator) :

6. Ouvrez l'écran Import Keys (Importation de clés). Reportez-vous à la section « [Menu Import Keys \(Importer des clés\)](#) », page 238.
7. Indiquez le groupe de clés de destination vers lequel les clés seront importées, l'expéditeur (C2, dans le cas présent) ayant exporté ces clés et le nom du fichier de transfert des clés. Le groupe de clés sélectionné doit correspondre à un groupe de clés configuré pour recevoir des clés de la part de C2.
8. Cliquez sur Start (Commencer).

---

## Menu Transfer Partners (Partenaires de transfert)

La fonction Key Transfer Partners (Partenaires de transfert de clés) permet de déplacer des clés d'un cluster KMS vers un autre.



## Menu Transfer Partner List (Liste des partenaires de transfert)

Dans le menu Secure Information Management (Gestion des informations sécurisées), choisissez **Transfer Partner List (Liste des partenaires de transfert)**.

Transfer Partner List

Filter: Transfer Partner ID =

Use Refresh Reset | < << >>

Results in page: 1 (last page)

Transfer Partner ID	Description	Contact Information	Enabled	Allow Export To	Allow Import From	Public Key ID
mytp		Nancy	True	False	False	23F3156AA4

Details... Create... Delete

Vous pouvez également faire défiler la base de données et filtrer la liste des partenaires de transfert selon l'un des critères suivants :

- Transfer Partner ID (ID de partenaire de transfert)
- Description
- Contact Information (Coordonnées)
- Enabled (Activé)
- Allow Export To (Autoriser l'exportation vers)
- Allow Import From (Autoriser l'importation de)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour le partenaire de transfert.

Les champs et leur description sont fournis ci-dessous :

### Filter (Filtre)

Sélectionnez les options de filtrage afin de filtrer la liste des partenaires de transfert. Seuls les partenaires de transfert répondant à tous les critères de filtrage sont affichés.

**Boîte combinée Filter Attribute (Attribut de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez un attribut de filtrage. Les valeurs possibles sont les suivantes :

- Transfer Partner ID (ID du partenaire de transfert)
- Description
- Contact Information (Coordonnées)
- Enabled (Activé)
- Allow Export To (Autoriser l'exportation vers)
- Allow Import From (Autoriser l'importation de)

**Boîte combinée Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opération de filtrage à appliquer à l'attribut sélectionné. Cette option de filtrage est masquée pour certains attributs. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

**Zone de texte Filter Value (Valeur de filtre)**

Indiquez la valeur selon laquelle l'attribut sélectionné doit être trié. Cette option de filtrage est masquée pour certains attributs.

**Boîte combinée Filter Value (Valeur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez la valeur selon laquelle l'attribut sélectionné doit être filtré. Cette option de filtrage est masquée pour certains attributs.



Cliquez sur ce bouton pour ajouter d'autres filtres.



Cliquez sur ce bouton pour supprimer un filtre. Ce bouton est visible uniquement si plusieurs filtres sont affichés.

**Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer les filtres sélectionnés à la liste affichée et atteindre la première page.

**Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée. Il ne s'applique pas aux filtres sélectionnés depuis la dernière activation du bouton Use (Utiliser) ou Reset (Réinitialiser), et il ne modifie pas la page de la liste.

### **Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

### **Results in Page (Résultats de la page)**

Affiche le nombre d'éléments pouvant être affichés sur la page active. Ajoute la mention (last page) au nombre d'éléments si vous avez atteint la fin de la liste. Le nombre maximum d'éléments affichés sur une page est défini par la valeur de l'option Query Page Size (Taille d'une page de requête) disponible dans la boîte de dialogue Options.

### **Transfer Partner ID (ID du partenaire de transfert)**

Affiche l'identificateur unique qui différencie les partenaires de transfert les uns des autres. Cette valeur doit comprendre entre 1 et 64 caractères. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

### **Description**

Décrit le partenaire de transfert. Cette valeur doit comprendre entre 1 et 64 caractères. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

### **Contact Information (Coordonnées)**

Affiche les coordonnées du partenaire de transfert. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

### **Enabled (Activé)**

Indique si le partenaire de transfert est autorisé à partager des clés. Les valeurs possibles sont True (Vrai) ou False (Faux). Si ce champ est défini sur False (Faux), le partenaire ne peut pas partager de clés. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

### **Allow Export To (Autoriser l'exportation vers)**

Indique si le partenaire de transfert est autorisé à exporter des clés. Les valeurs possibles sont True (Vrai) ou False (Faux). Si ce champ est défini sur False, le partenaire de transfert ne peut pas exporter de clés. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

### **Allow Import From (Autoriser l'importation de)**

Indique si des clés peuvent être importées à partir de ce partenaire de transfert. Les valeurs possibles sont True (Vrai) ou False (Faux). Si ce champ est défini sur False, il est impossible d'importer des clés provenant de ce partenaire de transfert. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

**Public Key ID (ID de la clé publique)**

Affiche l'identificateur unique qui différencie les clés publiques les uns des autres. Cette valeur doit comprendre entre 1 et 64 caractères. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

**Public Key Fingerprint (Empreinte de la clé publique)**

Affiche l'empreinte (ou la valeur de hachage) de la clé publique.

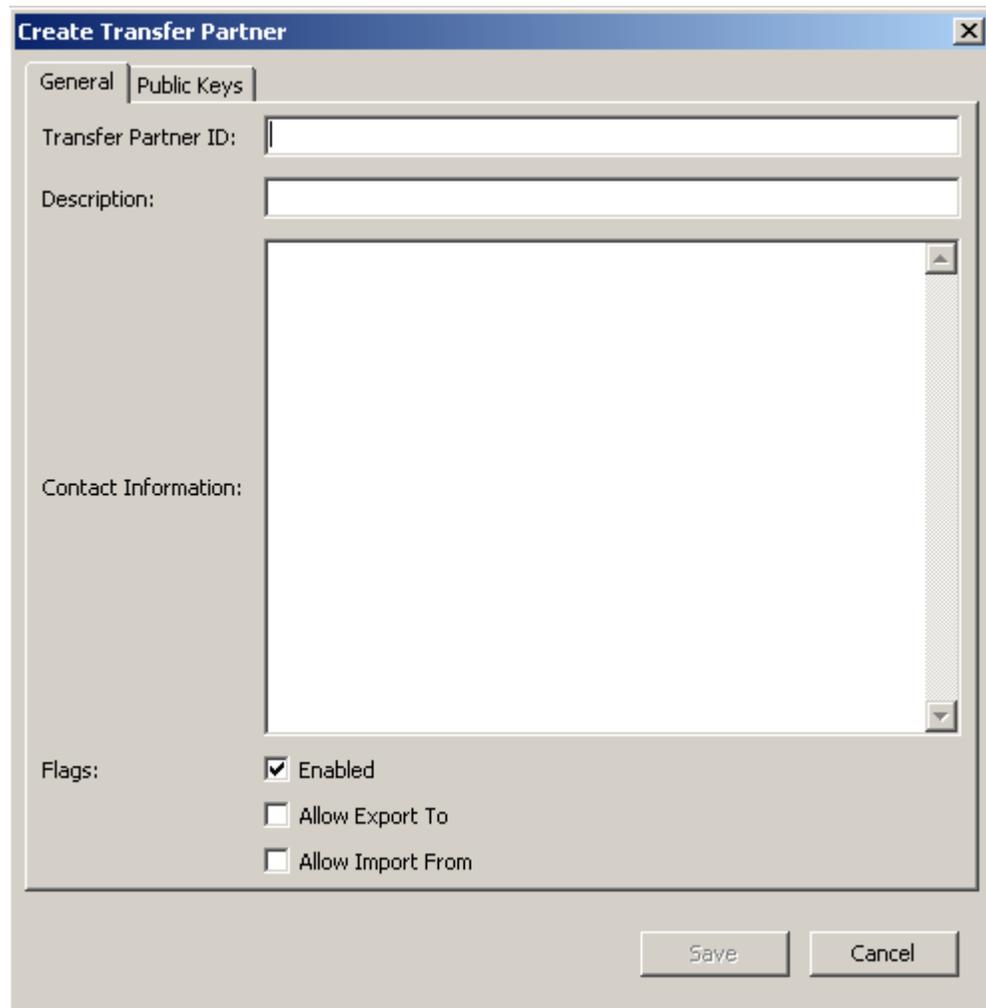
**Entry Date (Date de saisie)**

Affiche la date à laquelle la clé publique a été saisie dans le cluster KMS.

## Création d'un partenaire de transfert

Pour créer un partenaire de transfert :

1. Dans l'écran Transfer Partner List (Liste des partenaires de transfert), cliquez sur le bouton Create (Créer). La boîte de dialogue Create Transfer Partner (Création d'un partenaire de transfert) s'affiche, l'onglet General (Général) étant activé.



The screenshot shows a dialog box titled "Create Transfer Partner". It has two tabs: "General" and "Public Keys". The "General" tab is selected. The dialog contains the following fields and options:

- Transfer Partner ID:** A text input field.
- Description:** A text input field.
- Contact Information:** A large text area with a vertical scrollbar.
- Flags:** A section with three checkboxes:
  - Enabled
  - Allow Export To
  - Allow Import From

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

2. Remplissez les champs des paramètres suivants :

### *Onglet General (Général)*

#### **Transfer Partner ID (ID du partenaire de transfert)**

Identifie de manière unique le partenaire de transfert.

#### **Description**

Saisissez une valeur décrivant le partenaire de transfert de manière unique.  
Cette valeur doit comprendre entre 1 et 64 caractères. Ce champ peut rester vide.

**Contact Information (Coordonnées)**

Saisissez une valeur permettant d'identifier les coordonnées du partenaire de transfert. Ce champ peut rester vide.

**Flags - Enabled (Indicateurs - Activés)**

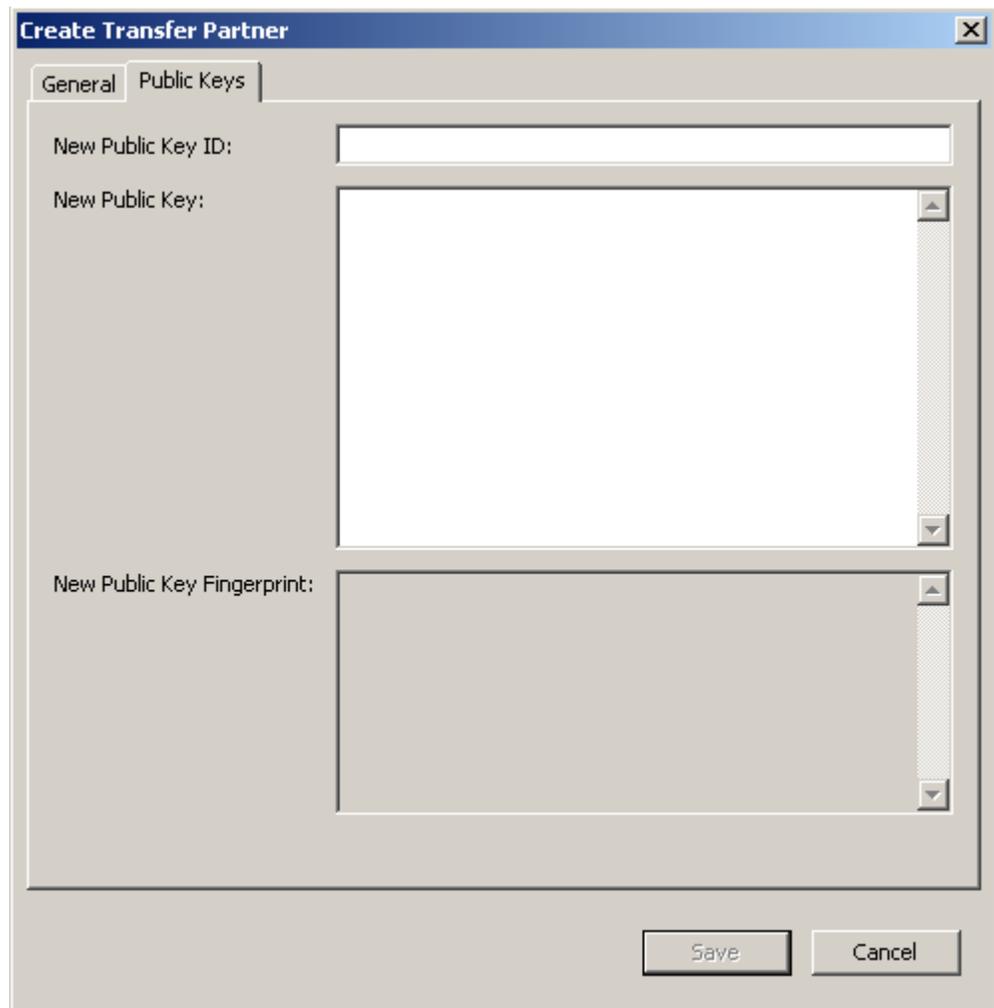
Cochez cette case pour autoriser ce partenaire de transfert à partager des clés. Si ce champ est désactivé, le partenaire de transfert ne peut pas partager de clés.

**Allow Export To (Autoriser l'exportation vers)**

Cochez cette case pour autoriser l'exportation de clés vers le partenaire de transfert. Si ce champ est désactivé, le partenaire de transfert ne sera pas disponible pour l'opération d'exportation.

**Allow Import From (Autoriser l'importation de)**

Cochez cette case pour indiquer si l'importation de clés à partir de ce partenaire de transfert est autorisée. Si ce champ est désactivé, il est impossible d'importer des clés provenant de ce partenaire de transfert.

**3. Activez l'onglet Public Keys (Clés publiques).**

The screenshot shows a dialog box titled "Create Transfer Partner" with a close button (X) in the top right corner. The dialog has two tabs: "General" and "Public Keys", with "Public Keys" currently selected. The "Public Keys" tab contains three input fields, each with a vertical scrollbar on the right side:

- "New Public Key ID:" followed by a single-line text input field.
- "New Public Key:" followed by a large multi-line text input area.
- "New Public Key Fingerprint:" followed by a large multi-line text input area.

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

*onglet Public Keys (Clés publiques)*

**New Public Key ID (Nouvel ID de clé publique)**

Saisissez l'ID de clé publique qui vous a été fourni par le partenaire de transfert.

**New Public Key (Nouvelle clé publique)**

Saisissez la clé publique qui vous a été fournie par le partenaire de transfert.

**New Public Key Fingerprint (Nouvelle empreinte de clé publique)**

Ce champ en lecture seule affiche l'empreinte (ou valeur de hachage) de la nouvelle clé publique. Vérifiez qu'elle correspond bien à celle du partenaire afin de vous assurer que la clé publique n'a pas été modifiée, accidentellement ou délibérément, lors de sa transmission.

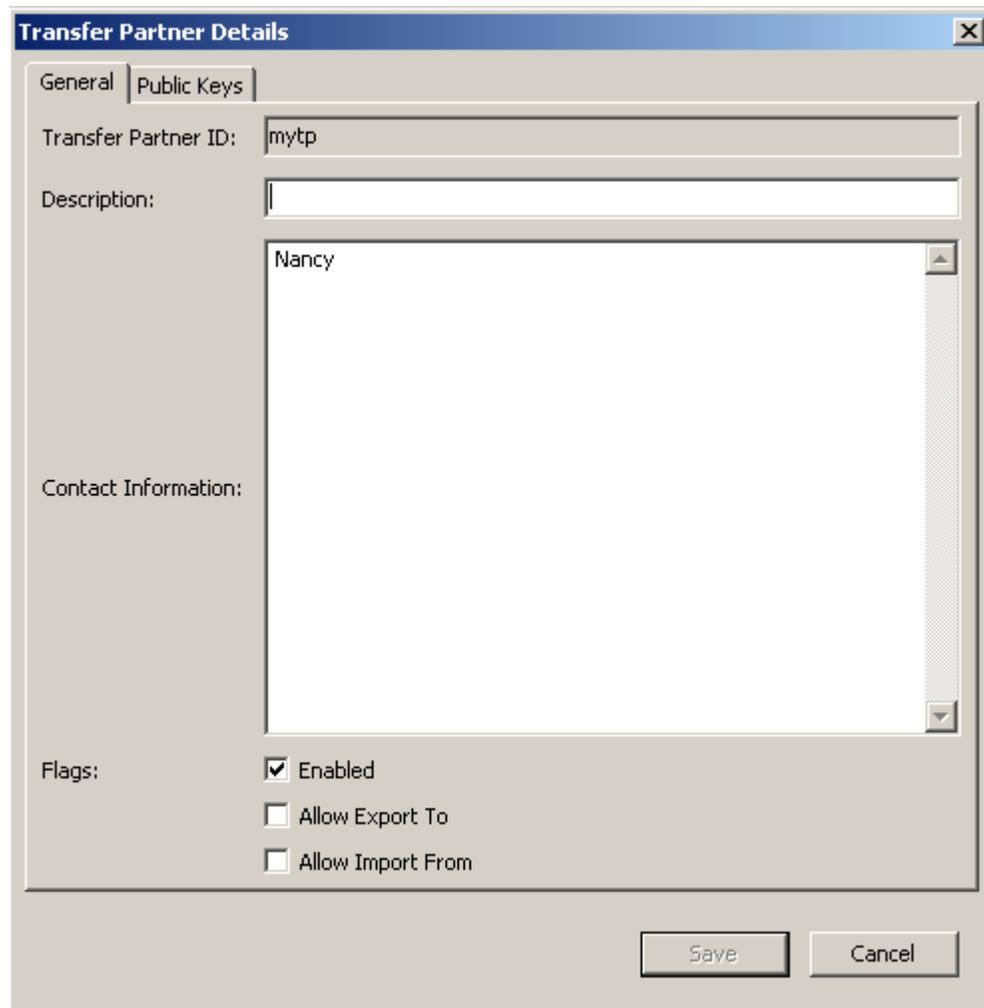
4. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer).

## Affichage/Modification des détails du partenaire de transfert

La boîte de dialogue Transfer Partner Details (Détails du partenaire de transfert) vous permet de visualiser des informations détaillées sur un partenaire de transfert spécifique.

Pour afficher ces informations :

1. Dans l'écran Transfer Partner List (Liste des partenaires de transfert), mettez un ID de partenaire en surbrillance et cliquez sur le bouton Details (Détails). La boîte de dialogue Transfer Partner Details (Détails du partenaire de transfert) s'affiche.



The screenshot shows a dialog box titled "Transfer Partner Details" with a close button (X) in the top right corner. The dialog has two tabs: "General" (selected) and "Public Keys".

Under the "General" tab, there are the following fields and controls:

- Transfer Partner ID:** A text box containing the value "mytp".
- Description:** A text box that is currently empty.
- Contact Information:** A large text area containing the name "Nancy".
- Flags:** A section with three checkboxes:
  - Enabled
  - Allow Export To
  - Allow Import From

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

### *Onglet General (Général)*

2. Sur l'onglet General (Général), modifiez les champs suivants :

- Description
- Contact Information (Coordonnées)
- Flags - Enabled (Indicateurs - Activés)
- Allow Export To (Autoriser l'exportation vers)
- Allow Import From (Autoriser l'importation de)

Le champ Transfer Partner ID (ID du partenaire de transfert) est en lecture seule.

3. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer).

L'enregistrement des partenaires de transfert est modifié dans la base de données.

4. Activez l'onglet Public Keys (Clés publiques).

**Transfer Partner Details \***

General Public Keys

New Public Key ID:

New Public Key:

New Public Key Fingerprint:

Existing Public Keys:

Public Key ID	Public Key
23F3156AA4864460DF9FB777F1AD7...	0201018EFD5E3DBEB972DD357B24815202302FF8f

Save Cancel

*Onglet Public Keys (Clés publiques)*

5. Sur l'onglet Public Keys (Clés publiques), vous pouvez modifier les champs suivants :

**New Public Key ID (Nouvel ID de clé publique)**

Saisissez l'ID de la nouvelle clé publique qui vous a été fourni par le partenaire de transfert.

**New Public Key (Nouvelle clé publique)**

Saisissez la nouvelle clé publique qui vous a été fournie par le partenaire de transfert.

**New Public Key Fingerprint (Nouvelle empreinte de clé publique)**

Ce champ en lecture seule affiche l'empreinte (ou valeur de hachage) de la nouvelle clé publique. Vérifiez cette clé auprès du partenaire de transfert source (l'expéditeur).

**Existing Public Keys (Clés publiques existantes)**

Cette liste affiche les clés publiques associées à ce partenaire.

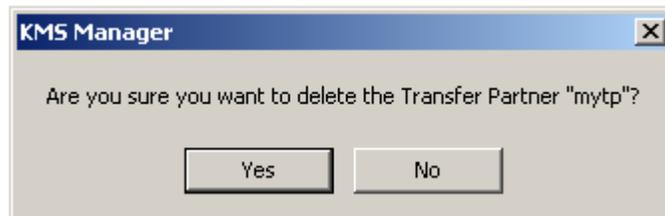
6. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer).

## Suppression d'un partenaire de transfert

Cette option donne la possibilité au responsable de la sécurité de supprimer un partenaire de transfert.

Pour supprimer un partenaire de transfert :

1. Dans l'écran Transfer Partner List (Liste des partenaires de transfert), mettez l'ID du partenaire de transfert à supprimer en surbrillance et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue Transfer Partner Confirm Delete (Confirmation de la suppression du partenaire de transfert) s'affiche.



2. Cliquez sur le bouton Yes (Oui) afin de supprimer le partenaire de transfert. Le partenaire de transfert sélectionné est supprimé et vous revenez à l'écran Transfer Partner List (Liste des partenaires de transfert).

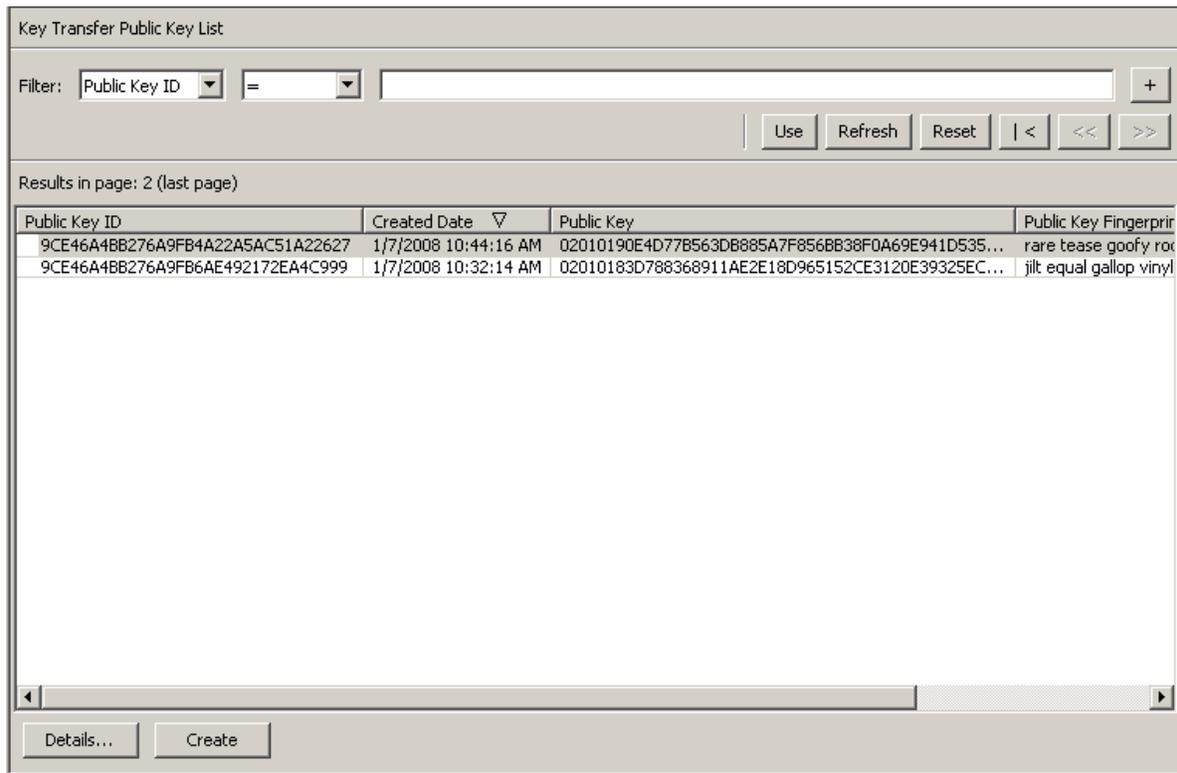
## Menu Key Transfer Public Key List (Liste des clés publiques de transfert de clés)

Pour partager des clés entre partenaires de transfert, les responsables de la sécurité doivent d'abord accéder aux informations de clés publiques correspondant à leur cluster KMS. Ce menu fournit des informations sur les clés publiques. La clé publique et l'ID correspondant affichés par cette commande doivent être transmis au partenaire de transfert.

### Affichage de la liste de clés publiques de transfert

Pour afficher la liste de clés publiques de transfert :

Dans le menu System Management (Gestion du système), choisissez Key Transfer Public Key List (Liste des clés publiques de transfert).



Vous pouvez également faire défiler la base de données et filtrer la liste des clés publiques de transfert selon l'un des critères suivants :

- Public Key ID (ID de la clé publique)
- Created Date (Date de création)
- Public Key (Clé publique)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée des clés publiques de transfert.

Les champs et leur description sont fournis ci-dessous :

**Filter (Filtre)**

Sélectionnez les options de filtrage afin de filtrer la liste des partenaires de transfert. Seuls les partenaires de transfert répondant à tous les critères de filtrage sont affichés.

**Boîte combinée Filter Attribute (Attribut de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez un attribut de filtrage. Les valeurs possibles sont les suivantes :

- Public Key ID (ID de la clé publique)
- Created Date (Date de création)
- Public Key (Clé publique)

**Boîte combinée Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opération de filtrage à appliquer à l'attribut sélectionné. Cette option de filtrage est masquée pour certains attributs. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

**Zone de texte Filter Value (Valeur de filtre)**

Indiquez la valeur selon laquelle l'attribut sélectionné doit être trié. Cette option de filtrage est masquée pour certains attributs.

**Boîte combinée Filter Value (Valeur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez la valeur selon laquelle l'attribut sélectionné doit être filtré. Cette option de filtrage est masquée pour certains attributs.

**Boîte combinée Filter Value (Valeur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez la valeur selon laquelle l'attribut sélectionné doit être filtré. Cette option de filtrage est masquée pour certains attributs.



Cliquez sur ce bouton pour ajouter d'autres filtres.



Cliquez sur ce bouton pour supprimer un filtre. Ce bouton est visible uniquement si plusieurs filtres sont affichés.

**Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer les filtres sélectionnés à la liste affichée et atteindre la première page.

**Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée. Il ne s'applique pas aux filtres sélectionnés depuis la dernière activation du bouton Use (Utiliser) ou Reset (Réinitialiser), et il ne modifie pas la page de la liste.

**Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'éléments pouvant être affichés sur la page active. Ajoute la mention (last page) au nombre d'éléments si vous avez atteint la fin de la liste. Le nombre maximum d'éléments affichés sur une page est défini par la valeur de l'option Query Page Size (Taille d'une page de requête) disponible dans la boîte de dialogue Options.

**Public Key ID (ID de clé publique)**

Affiche l'identificateur unique qui différencie les clés publiques les unes des autres. Cette valeur doit comprendre entre 1 et 64 caractères. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

**Created Date (Date de création)**

Affiche les date et heure de création de cette clé publique. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

La clé privée correspondant à la clé publique la plus récente est utilisée pour signer tous les fichiers de transfert de clés exportés.

**Public Key (Clé publique)**

Affiche la clé publique utilisée pour transférer des clés entre partenaires de transfert. Cette valeur est affichée en base 64. Cliquez sur le nom de cette colonne pour trier selon cet attribut.

**Public Key Fingerprint (Empreinte de la clé publique)**

Hachage de la clé publique. Cette valeur sert à vérifier que la clé publique a été transmise correctement et est affichée en base 64.

## Affichage des informations détaillées sur les clés publiques de transfert

Pour afficher l'écran Key Transfer Public Key Details, sélectionnez une clé publique, puis cliquez sur le bouton Details (Détails).



## Création d'une clé publique de transfert

Pour créer une clé publique de transfert, cliquez sur le bouton Create (Créer).

Une fois la clé créée, vous devez la fournir à tous les partenaires de transfert existants. Étant donné que les fichiers de transfert de clés créés après la définition de la nouvelle clé publique de transfert seront signés au moyen de cette nouvelle clé, les partenaires doivent en disposer avant d'importer les nouveaux fichiers de transfert de clés.

Key Transfer Public Key List

Filter: Public Key ID =  +

Use Refresh Reset | < << >> >

Results in page: 3 (last page)

Public Key ID	Created Date ▾	Public Key	Public Key Fingerprint
9CE46A4BB276A9FBE8FE99E7C3E203F8	1/15/2008 6:11:00 PM	020101CAD193962581A1DEE0E3EF3319084F2801A63F0...	selma flush equal all
9CE46A4BB276A9FB4A22A5AC51A22627	1/7/2008 10:44:16 AM	02010190E4D77B563DB885A7F856BB38F0A69E941D535...	rare tease goofy roc
9CE46A4BB276A9FB6AE492172EA4C999	1/7/2008 10:32:14 AM	02010183D788368911AE2E18D965152CE3120E39325EC...	jilt equal gallop vinyl

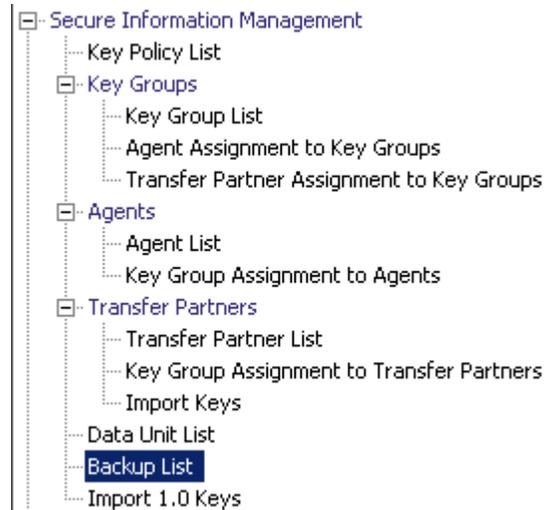
Details... Create

---

## Menu Backup List (Liste des sauvegardes)

L'option de menu Backup List (Liste des sauvegardes) permet au responsable de la sécurité d'effectuer les opérations suivantes :

- Afficher l'historique des sauvegardes
- Afficher les informations détaillées d'un fichier de sauvegarde
- Restaurer des sauvegardes



## Affichage de l'historique des fichiers de sauvegarde

Pour afficher l'historique des fichiers de sauvegarde :

Dans le menu Secure Information Management (Gestion des informations sécurisées), choisissez Backup List (Liste des sauvegardes). L'écran Backup List (Liste des sauvegardes) s'affiche.

Backup ID	KMA ID	Created Date	Destroyed Date	Destruction
FDAC7620B1491D50000000000000000001	FDAC7620B1491D50	12/4/2007 8:26:49 AM		PENDING
FDAC7620B1491D50000000000000000002	FDAC7620B1491D50	12/4/2007 8:30:18 AM		PENDING

Vous pouvez également faire défiler la base de données et filtrer les fichiers de sauvegarde selon l'un des critères suivants :

- Backup ID (ID de sauvegarde)
- KMA ID (ID du KMA)
- Created Date (Date de création)
- Destroyed Date (Date de destruction)
- Destruction Status (Statut de destruction)
- Destruction Comment (Commentaire sur la destruction)

Le bouton Use (Utiliser) applique le filtre à la liste affichée pour le fichier de sauvegarde.

Les champs et leur description sont fournis ci-dessous :

#### **Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Backup ID (ID de la sauvegarde)
- Created Date (Date de création)
- Destroyed Date (Date de destruction)
- Destruction Status (Statut de destruction)
- Destruction Comment (Commentaire sur la destruction)

#### **Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~

#### **Zone Filter Value 1 (Valeur de filtre 1)**

Si vous avez sélectionné un filtre de date, cliquez sur Set Date (Définir la date) afin de spécifier la date et l'heure de départ. La valeur s'affiche comme valeur de départ de la plage des clés de filtrage. Si vous avez sélectionné n'importe quel autre filtre, saisissez une valeur dans ce champ.

#### **Zone Filter Value 2 (Valeur de filtre 2)**

Si vous avez sélectionné un filtre de date, cliquez sur Set Date (Définir la date) afin de sélectionner une date et une heure de fin. La valeur s'affiche comme valeur de fin de la plage de clés de filtrage.

#### **Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer le filtre à la liste affichée.

#### **Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

#### **Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**Backup ID (ID de la sauvegarde)**

Affiche un identificateur unique généré par le système permettant de différencier les fichiers de sauvegarde les uns des autres.

**KMA ID (ID du KMA)**

Affiche le KMA pour lequel le fichier de sauvegarde a été généré.

**Created Date (Date de création)**

Affiche la date de création de la sauvegarde.

**Destroyed Date (Date de destruction)**

Affiche la date à laquelle la sauvegarde a été marquée comme ayant été détruite manuellement.

**Destruction Status (Statut de destruction)**

Indique le statut de la sauvegarde par rapport à sa destruction. Les valeurs possibles sont les suivantes :

**NONE (AUCUN)**

Le fichier de sauvegarde n'a pas été détruit et ne contient pas de clés d'unité de données détruites.

**PENDING (EN ATTENTE)**

Le fichier de sauvegarde n'a pas encore été détruit manuellement et contient des copies de clés d'unités de données détruites.

**DESTROYED (DÉTRUIT)**

Le fichier de sauvegarde a été détruit manuellement.

**Destruction Comment (Commentaire sur la destruction)**

Affiche des informations fournies par l'utilisateur concernant la destruction du fichier de sauvegarde.

**Details (Détails)**

Cliquez sur ce bouton afin d'afficher des informations plus détaillées sur une sauvegarde.

**Create Backup (Créer une sauvegarde)**

Cliquez sur ce bouton afin de créer une sauvegarde. Ce bouton n'est pas activé si vous êtes responsable de la sécurité.

**Restore (Restaurer)**

Cliquez sur ce bouton afin de restaurer une sauvegarde.

**Confirm destruction (Confirmer la destruction)**

Cliquez sur ce bouton afin de confirmer la destruction de la sauvegarde. Ce bouton n'est pas activé si vous êtes responsable de la sécurité.

Pour obtenir plus d'informations sur une sauvegarde, mettez celle-ci en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage d'informations détaillées sur une sauvegarde](#) », page 146.

Cliquez sur le bouton Restore (Restaurer) afin de restaurer la sauvegarde sélectionnée. Pour plus d'informations, reportez-vous à la section « [Restauration d'une sauvegarde](#) », page 148.

## Affichage d'informations détaillées sur une sauvegarde

La boîte de dialogue Backup Details (Détails de la sauvegarde) permet d'afficher des informations détaillées sur un fichier de sauvegarde.

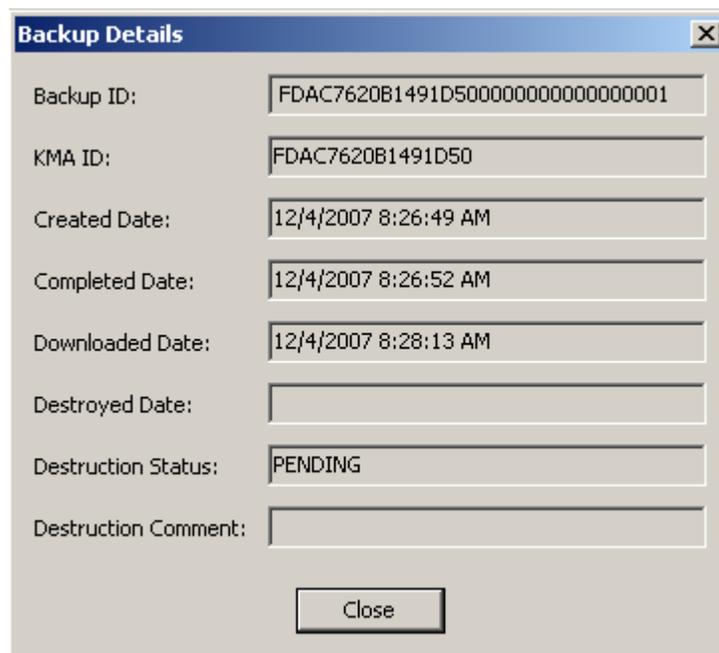
---

**Remarque** – Les fichiers de sauvegarde sont créés et restaurés sur le KMA.

---

Pour afficher des informations détaillées sur un fichier de sauvegarde :

1. Dans l'écran Backups List (Liste des sauvegardes), double-cliquez sur l'entrée de sauvegarde pour laquelle vous souhaitez obtenir des informations détaillées ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). La boîte de dialogue Backup Details (Détails de la sauvegarde) s'affiche en présentant tous les champs en lecture seule.



The screenshot shows a dialog box titled "Backup Details" with a close button in the top right corner. It contains several text input fields, each with a label to its left. The fields are: Backup ID (value: FDAC7620B1491D500000000000000001), KMA ID (value: FDAC7620B1491D50), Created Date (value: 12/4/2007 8:26:49 AM), Completed Date (value: 12/4/2007 8:26:52 AM), Downloaded Date (value: 12/4/2007 8:28:13 AM), Destroyed Date (empty), Destruction Status (value: PENDING), and Destruction Comment (empty). A "Close" button is located at the bottom center of the dialog box.

2. Les champs et leur description sont fournis ci-dessous :

### **Backup ID (ID de la sauvegarde)**

Affiche un identificateur unique généré par le système permettant de différencier les fichiers de sauvegarde les uns des autres.

**KMA ID (ID du KMA)**

Affiche le KMA sur lequel ce fichier de sauvegarde est généré.

**Created Date (Date de création)**

Affiche les date et heure de création du fichier de sauvegarde.

**Completed Date (Date de fin)**

Affiche les date et heure de fin du fichier de sauvegarde.

**Downloaded Date (Date de téléchargement)**

Affiche les date et heure de téléchargement du fichier de sauvegarde.

**Destroyed Date (Date de destruction)**

Affiche la date de destruction du fichier de sauvegarde.

**Destruction Status (Statut de destruction)**

Indique le statut de la sauvegarde par rapport à sa destruction.

**Destruction Comment (Commentaire sur la destruction)**

Affiche des informations fournies par l'utilisateur concernant la destruction du fichier de sauvegarde.

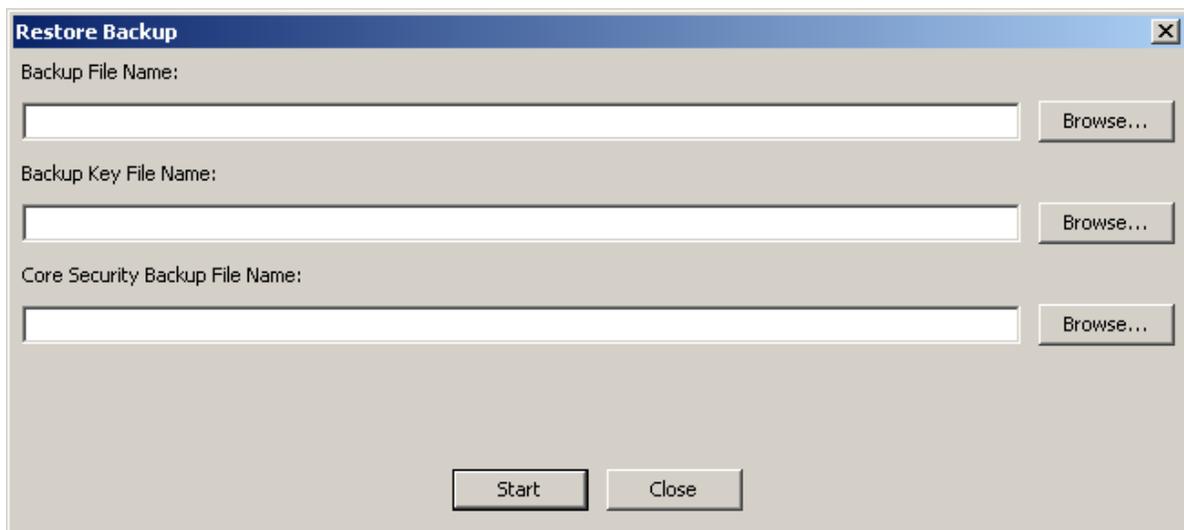
3. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue.

## Restauration d'une sauvegarde

Cette fonction permet à l'utilisateur de télécharger et de restaurer une sauvegarde composée d'un fichier de sauvegarde et d'un fichier de clés de sauvegarde sur le KMA. Avant de restaurer un fichier de sauvegarde sur un KMA, assurez-vous de bénéficier du quorum d'authentification requis.

Pour restaurer une sauvegarde :

1. Dans l'écran Backup List (Liste des sauvegardes), mettez la sauvegarde à restaurer en surbrillance et cliquez sur le bouton Restore (Restaurer). La boîte de dialogue Restore Backup (Restauration d'une sauvegarde) s'affiche.
2. Sélectionnez la sauvegarde de sécurité principale voulue, le fichier de clés de sauvegarde et le fichier de sauvegarde. Le fichier de clés de sauvegarde et la sauvegarde doivent correspondre. Autrement dit, ils doivent avoir été créés au même moment. La sauvegarde de sécurité principale peut être plus ancienne ou plus récente que ces deux fichiers. Il est possible d'utiliser n'importe quel fichier de sauvegarde de sécurité principale avec tout fichier de clés de sauvegarde et tout fichier de sauvegarde.
3. Cliquez sur le bouton Start (Commencer).



The image shows a Windows-style dialog box titled "Restore Backup". It has a blue title bar with a close button (X) on the right. The dialog contains three input fields, each with a "Browse..." button to its right:

- Backup File Name: [input field] [Browse...]
- Backup Key File Name: [input field] [Browse...]
- Core Security Backup File Name: [input field] [Browse...]

At the bottom of the dialog, there are two buttons: "Start" and "Close".

4. Une fois le processus de téléchargement terminé, la boîte de dialogue Restore Backup (Restauration d'une sauvegarde) vous en informe, puis la boîte de dialogue Key Split Quorum Authentication (Authentification par quorum de scission de clés) s'affiche. Le quorum doit saisir les noms d'utilisateur et phrases de passe correspondantes afin d'authentifier l'opération.

The image shows a dialog box titled "Key Split Quorum Authentication". It contains a message: "To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials." Below this message are ten rows, each with a "Split User" label and a "Passphrase" label, each followed by an empty text input field. At the bottom are "OK" and "Cancel" buttons.

5. Lorsque vous cliquez sur OK après avoir saisi les derniers nom d'utilisateur et phrase de passe, ceux-ci sont envoyés au KMA à des fins d'authentification. Si l'authentification réussit, la boîte de dialogue Key Split Quorum Authentication (Authentification par quorum de scission de clés) se ferme.

Les ID d'utilisateur et les phrases de passe, ainsi que le nombre requis (c.-à-d., le quorum) doivent correspondre aux identifiants de scission de clés en vigueur lors de la création de la sauvegarde de sécurité principale.

6. La boîte de dialogue Restore Backup (Restauration d'une sauvegarde) s'affiche, indiquant le statut du processus de restauration.
7. Les champs et leur description sont fournis ci-dessous :

**Backup File Name (Nom du fichier de sauvegarde)**

Nom du fichier de sauvegarde.

**Backup Wrapping Key File Name (Nom de fichier de la clé d'habillage de sauvegarde)**

Affiche le nom du fichier de clés de sauvegarde.

**Core Security Backup File Name (Nom du fichier de la sauvegarde de sécurité principale)**

Nom du fichier de sauvegarde contenant les informations sur les clés de la sécurité principale.

8. Une fois la restauration terminée, un message vous en informe. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue. La base de données et le magasin de clés sécurisé sont restaurés sur le KMA.

---

## Menu System Dump (Vidage système)

Le menu System Dump (Vidage système) crée un vidage système permettant de résoudre des problèmes et le télécharge dans un fichier compressé situé sur le système lorsque KMS Manager est en cours d'exécution. Le fichier téléchargé est enregistré dans un format compatible avec les utilitaires de compression.

---

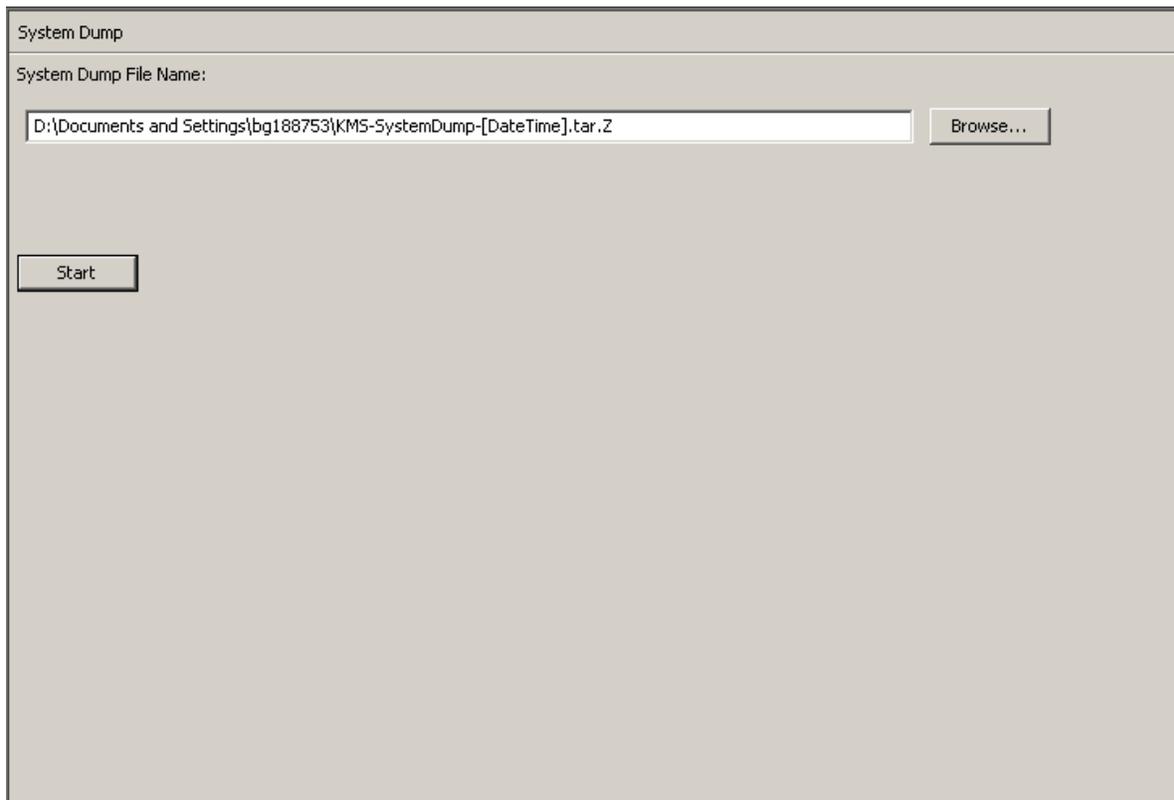
**Remarque** – Le vidage ne contient aucune information sur les clés permettant de déduire celles-ci.

---

### Création d'un vidage système

1. Pour créer un vidage système, dans le menu System Management (Gestion du système), choisissez System Dump (Vidage système). L'écran s'affiche, présentant un fichier \*.tar.Z généré automatiquement. Le cas échéant, cliquez sur Browse (Parcourir) afin de sélectionner un chemin de destination.
2. Cliquez sur le bouton Start (Commencer) pour commencer le téléchargement. Le système affiche en temps réel des messages indiquant la quantité d'informations de vidage système en cours de téléchargement et vous informe de la fin de l'opération.

3. Accédez au chemin de destination et ouvrez le fichier \*.tar.Z afin d'afficher les informations de vidage système.



Les champs et leur description sont fournis ci-dessous :

**File Name (Nom du fichier)**

Affiche un nom de fichier \*.tar.gz généré automatiquement.

**Browse (Parcourir)**

Cliquez sur ce bouton pour spécifier l'emplacement de ce fichier.

**Start (Commencer)**

Cliquez sur ce bouton pour lancer le processus de téléchargement.

---

## Menu Security Parameters (Paramètres de sécurité)

Le menu Security Parameters List (Liste des paramètres de sécurité) donne au responsable de la sécurité la possibilité de visualiser et de modifier les paramètres de sécurité du KMA.

### Récupération des paramètres de sécurité

Pour récupérer les paramètres de sécurité :

Dans le menu Security Parameters (Paramètres de sécurité), choisissez Security Parameters List (Liste des paramètres de sécurité). L'écran Security Parameters List (Liste des paramètres de sécurité) s'affiche en mode lecture seule.

Security Parameters	
Short Term Retention Audit Log Size Limit:	10,000
Short Term Retention Audit Log Lifetime:	7 Days
Medium Term Retention Audit Log Size Limit:	100,000
Medium Term Retention Audit Log Lifetime:	3 Months
Long Term Retention Audit Log Size Limit:	1,000,000
Long Term Retention Audit Log Lifetime:	2 Years
Login Attempt Limit:	5
Passphrase Minimum Length:	8
Management Session Inactivity Timeout:	Disabled

Modify...

Les champs et leur description sont fournis ci-dessous :

**Short Term Retention Audit Log Size Limit (Limite de la taille du journal d'audit de conservation à court terme)**

Affiche le nombre d'entrées du journal d'audit concernant les événements de type Erreur conservées avant leur troncation. La valeur par défaut est égale à 10 000. La valeur minimale est de 1 000 tandis que la valeur maximale est de 1 000 000.

**Short Term Retention Audit Log Lifetime (Durée de vie du journal d'audit de conservation à court terme)**

Affiche la durée de conservation (en jours) des entrées du journal d'audit à court terme avant leur troncation. La valeur par défaut est de 7 jours. La valeur minimale est de 7 jours et la valeur maximale de 24 855 jours.

**Medium Term Retention Audit Log Size Limit (Limite de la taille du journal d'audit de conservation à moyen terme)**

Affiche le nombre d'entrées du journal d'audit concernant les événements de type Erreur conservées avant leur troncation. La valeur par défaut est égale à 100 000. La valeur minimale est de 1 000 tandis que la valeur maximale est de 1 000 000.

**Medium Term Retention Audit Log Lifetime (Durée de vie du journal d'audit de conservation à moyen terme)**

Affiche la durée de conservation (en jours) des entrées du journal d'audit à moyen-terme avant leur troncation. La valeur par défaut est de 90 jours. La valeur minimale est de 7 jours et la valeur maximale de 24 855 jours.

**Long Term Retention Audit Log Size Limit (Limite de la taille du journal d'audit de conservation à long terme)**

Affiche le nombre d'entrées du journal d'audit de conservation à long terme conservées avant leur troncation. La valeur par défaut est égale à 1 000 000. La valeur minimale est de 1 000 tandis que la valeur maximale est de 1 000 000.

**Long Term Retention Audit Log Lifetime (Durée de vie du journal d'audit de conservation à long terme)**

Affiche la durée de conservation (en jours) des entrées du journal d'audit à long-terme avant leur troncation. La valeur par défaut est de 730 jours. La valeur minimale est de 7 jours et la valeur maximale de 24 855 jours.

**Login Attempt Limit (Nombre maximum de tentatives de connexion)**

Indique le nombre maximal d'échecs de tentatives de connexion avant la désactivation de l'entité. La valeur par défaut est égale à 5. La valeur minimale est de 1 tandis que la valeur maximale est de 1 000.

**Password Minimum Length (Longueur minimale de la phrase de passe)**

Affiche la longueur minimale de la phrase de passe. La valeur par défaut est de 8 caractères. La valeur minimale est de 8 tandis que la valeur maximale est de 64 caractères.

**Management Session Inactivity Timeout (Délai d'inactivité d'une session de gestion)**

Affiche la durée maximale (en minutes) qu'une session KMS Manager ou de console peut rester inactive avant d'être déconnectée automatiquement. La modification de cette valeur est sans effet sur les sessions déjà en cours. La valeur par défaut est égale à 15 minutes. La valeur minimale est de 0 (ce qui signifie qu'aucune valeur temporelle n'est utilisée) tandis que la valeur maximale est de 60 minutes.

Si vous souhaitez modifier les paramètres de sécurité, cliquez sur le bouton **Modify (Modifier)**. Pour plus d'informations, reportez-vous à la section « Modification des paramètres de sécurité » à la page 5-37.

## Modification des paramètres de sécurité

Pour modifier les paramètres de sécurité :

1. Dans l'écran Security Parameters List (Liste des paramètres de sécurité), cliquez sur le bouton Modify (Modifier). L'écran Modify Security Parameters (Modifier les paramètres de sécurité) s'affiche.

The screenshot shows a dialog box titled "Modify Security Parameters" with the following fields and values:

- Short Term Retention Audit Log Size Limit: 10,000
- Short Term Retention Audit Log Lifetime: 7 Day(s)
- Medium Term Retention Audit Log Size Limit: 100,000
- Medium Term Retention Audit Log Lifetime: 3 Month(s)
- Long Term Retention Audit Log Size Limit: 1,000,000
- Long Term Retention Audit Log Lifetime: 2 Year(s)
- Login Attempt Limit: 5
- Passphrase Minimum Length: 8
- Management Session Inactivity Timeout: 0 Minutes

Buttons: Save, Cancel

2. Modifiez les paramètres de sécurité selon vos besoins. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer). Les modifications sont enregistrées dans la base de données du KMA.

---

## Sécurité principale

L'élément essentiel du composant Core Security (Sécurité principale) correspond aux informations de clé racine. Il s'agit des données de clé générées au moment de l'initialisation du cluster. Les données de clé racine protègent la clé principale. La clé principale est une clé symétrique destinée à protéger les clés d'unités de données stockées sur le KMA.

La sécurité principale est protégée au moyen d'un modèle de scission de clé nécessitant un quorum d'utilisateurs défini dans les références de scission de clé en vue de fournir les noms d'utilisateur et phrases de passe de ces personnes pour déchiffrer les données de clé racine.

Ce mécanisme de sécurité implique deux états de fonctionnement pour le KMA : verrouillé et déverrouillé.

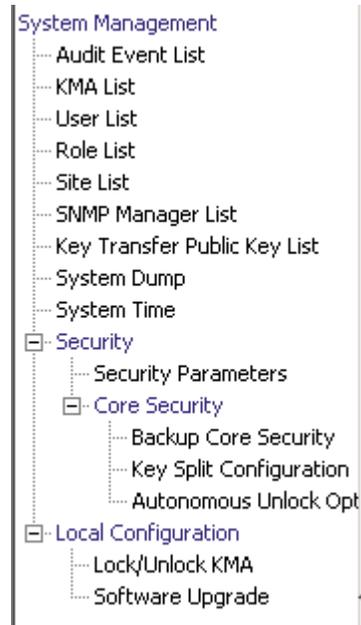
Un KMA verrouillé ne permet pas de déchiffrer les données de clé racine et, de ce fait, ne peut pas accéder aux clés des unités de données. En conséquence, le KMA n'est pas en mesure de répondre aux requêtes des agents en vue d'enregistrer de nouvelles unités de données ou de récupérer des clés d'unités de données existantes.

Un KMA déverrouillé est capable d'utiliser les données de clé racine afin d'accéder aux clés d'unités de données et de répondre aux requêtes des agents.

---

## Menu Core Security (Sécurité principale)

Le menu Core Security (Sécurité principale) propose les options suivantes :



Il permet au responsable de la sécurité d'effectuer les opérations suivantes :

- Création d'une sauvegarde de la sécurité principale
- Affichage/Modification des références de scission de clés
- Activation/Désactivation de l'option de déverrouillage autonome

## Backup Core Security (Sauvegarder la sécurité principale)

L'option Backup Core Security (Sauvegarder la sécurité principale) permet au responsable de la sécurité de sauvegarder les données de clés de la sécurité principale et de les télécharger dans un fichier situé sur le système local.

---

**Attention** – Veillez à protéger soigneusement les fichiers de sauvegarde de la sécurité principale. Comme le fichier de sauvegarde de la sécurité principale peut s'utiliser avec n'importe quelle paire de fichier de sauvegarde/fichier de clé de sauvegarde, même les anciennes versions peuvent s'avérer utiles.

---

### Création d'une sauvegarde de sécurité principale

Effectuez une nouvelle sauvegarde de la sécurité principale après chaque modification des références de scission de clés.

---

**Important** – Le responsable de la sécurité doit sauvegarder les données de clés de la sécurité principale avant de créer une sauvegarde. Reportez-vous à la section « [Création d'une sauvegarde](#) », page 259.

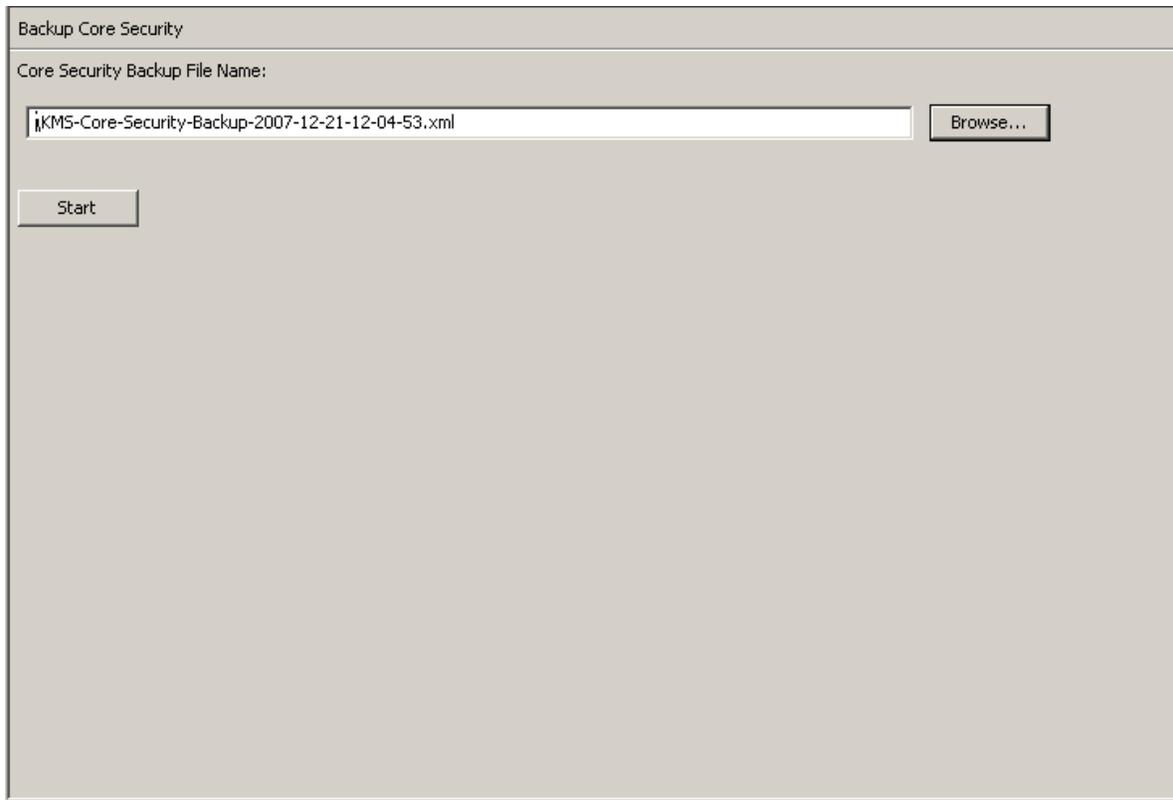
---

1. Dans le menu Core Security (Sécurité principale), choisissez Backup Core Security (Sauvegarder la sécurité principale). L'écran Backup Core Security (Sauvegarder la sécurité principale) s'affiche.

---

**Remarque** – Les noms des fichiers de sauvegarde sont générés automatiquement. Toutefois, vous pouvez les modifier et choisir le bouton Browse (Parcourir) afin de sélectionner le chemin de destination.

---



2. Cliquez sur le bouton Start (Commencer) afin de créer le fichier de sauvegarde de la sécurité principale et de le télécharger vers la destination définie par l'utilisateur.
3. Une fois la sauvegarde terminée, un message s'affiche à l'écran. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue.
4. Vous revenez à l'écran Backup Core Security (Sauvegarder la sécurité principale).

## Key Split Configuration (Configuration de scissions de clé)

L'option de menu Key Split Configuration (Configuration de scissions de clé) permet au responsable de la sécurité d'afficher et de modifier les références de scission de clés du KMA.

### Affichage de la configuration de scissions de clé

Pour afficher la configuration de scissions de clé :

1. Dans le menu Core Security (Sécurité principale), choisissez Key Split Configuration (Configuration de scissions de clé). L'écran Key Split Configuration (Configuration de scissions de clé) s'affiche.

Key Split Configuration

Key Split Number:  users

Threshold Number:  users

Split User 1:  Split User 2:

Split User 3:  Split User 4:

Split User 5:  Split User 6:

Split User 7:  Split User 8:

Split User 9:  Split User 10:

Les champs et leur description sont fournis ci-dessous :

#### **Key Split Number (Nombre de scissions de clé)**

Affiche le nombre de scissions de clé. La valeur maximale est de 10.

#### **Threshold Number (Seuil)**

Affiche le nombre d'utilisateurs requis pour l'authentification d'un quorum.

#### **Utilisateur de scission (1-10)**

Affiche le nom des utilisateurs de la scission existante.

Si vous souhaitez modifier les noms d'utilisateur, les phrases de passe ou le seuil d'une scission de clé, cliquez sur le bouton Modify (Modifier). Pour plus d'informations, reportez-vous à la section « [Modification de la configuration de scissions de clé](#) », page 161.

## Modification de la configuration de scissions de clé

Pour modifier la configuration de scissions de clé :

1. Dans l'écran Key Split Configuration (Configuration de scissions de clé), cliquez sur le bouton Modify (Modifier). La boîte de dialogue Modify Key Split Configuration (Modification de la configuration des scissions de clé) s'affiche.

2. Remplissez les champs des paramètres suivants, puis cliquez sur le bouton OK :

### Key Split Number (Nombre de scissions de clé)

Saisissez une nouvelle valeur correspondant au nombre de scissions de clé. Le nombre maximal est de 10.

### Threshold Number (Seuil)

Indiquez une nouvelle valeur indiquant le nombre d'utilisateurs requis pour former un quorum.

### Split User (Utilisateur de la scission) x

Saisissez un nouveau nom d'utilisateur. Pour chaque utilisateur de la scission, renseignez les champs de la phrase de passe et de la confirmation de la phrase de passe.

---

**Remarque** – Le nombre de champs Split User activés varie en fonction de la valeur saisie dans le champ Key Split Number.

---

3. Cliquez sur le bouton Save (Enregistrer) une fois le dernier nom d'utilisateur et la dernière phrase de passe indiqués.
4. La boîte de dialogue Key Split Quorum Authentication (Authentification du quorum de scission de clés) s'affiche une fois les références de scission de clés spécifiées. Saisissez le nom d'utilisateur et la phrase de passe correspondant aux références de quorum existantes, puis cliquez sur OK. Cela nécessitait de définir de nouvelles références à l'étape 2 et à l'étape 3.

**Key Split Quorum Authentication**

To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials.

Split User 1:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 2:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 3:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 4:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 5:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 6:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 7:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 8:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 9:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 10:	<input type="text"/>	Passphrase:	<input type="text"/>

OK Cancel

5. Le système met à jour les anciennes informations de configuration dans la base de données. La nouvelle configuration s'affiche dans l'écran Key Split Credentials (Références de scission de clés).

---

**Remarque** – Les données de clés de sécurité principale sont à nouveau habillées au moyen des références de scission de clés mises à jour.

---

6. Créez une nouvelle sauvegarde de la sécurité principale (voir « [Création d'une sauvegarde de sécurité principale](#) », page 157).

---

**Remarque** – Détruisez tous les anciens fichiers de sauvegarde de sécurité principale afin de vous assurer que les anciennes références de scission de clés ne pourront pas être utilisées pour détruire une sauvegarde.

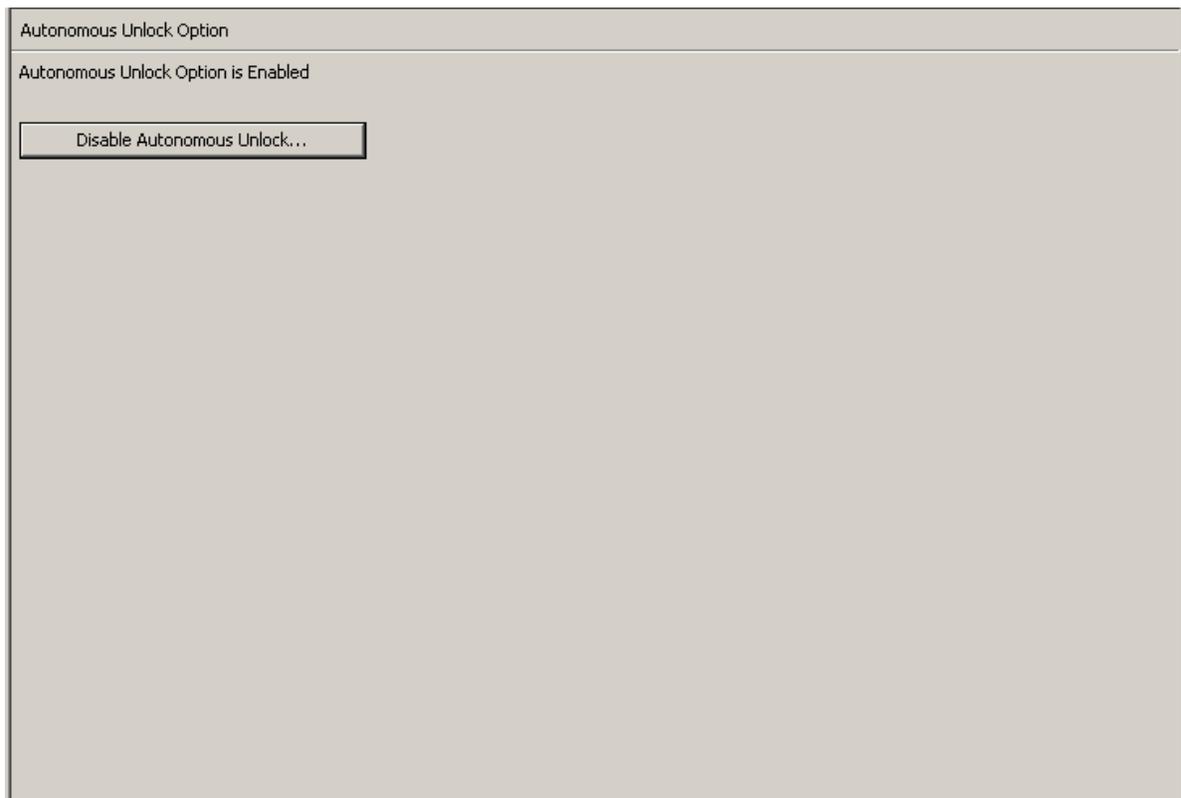
---

## Autonomous Unlock Option (Option de déverrouillage autonome)

L'option de menu Autonomous Unlock Option (Option de déverrouillage autonome) permet au responsable de la sécurité d'activer ou de désactiver l'option autonome s'appliquant au KMA.

Pour activer ou désactiver l'option Autonomous Unlock Option (Option de déverrouillage autonome) :

1. Dans le menu Core Security (Sécurité principale), choisissez Autonomous Unlock Option (Option de déverrouillage autonome). L'écran Autonomous Unlock Option (Option de déverrouillage autonome) s'affiche, indiquant le statut actuel.



2. Selon le statut d'initialisation autonome actif, choisissez Enable Autonomous Unlock (Activer le déverrouillage autonome) pour activer cette option ou Disable Autonomous Unlock dans le cas contraire.

---

### Remarque –

- Le bouton Lock/Unlock (Verrouiller/Déverrouiller) permet de basculer entre les deux états et de définir l'état verrouillé du KMA contraire à l'état actif.
  - Vous devez indiquer un quorum permettant d'activer ou de désactiver l'option de déverrouillage autonome.
-

3. La boîte de dialogue Key Split Quorum Authentication (Authentification du quorum de scission de clés) s'affiche. Le quorum doit saisir les noms d'utilisateur et phrases de passe correspondantes afin d'authentifier l'opération.

**Key Split Quorum Authentication** [X]

To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials.

Split User 1:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 2:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 3:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 4:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 5:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 6:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 7:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 8:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 9:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 10:	<input type="text"/>	Passphrase:	<input type="text"/>

OK Cancel

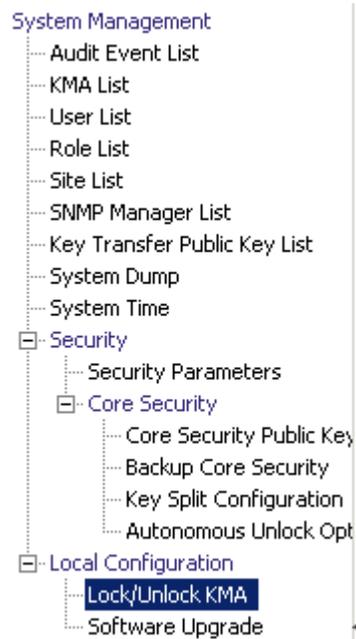
4. Lorsque vous cliquez sur OK après avoir saisi les derniers nom d'utilisateur et phrase de passe, ceux-ci sont envoyés au KMA à des fins d'authentification.
5. Si l'authentification réussit, la boîte de dialogue Key Split Quorum Authentication (Authentification du quorum de scission de clés) se ferme et la nouvelle option d'initialisation autonome est définie pour le KMA.

---

# Menu Local Configuration (Configuration locale)

Le menu Local Configuration (Configuration locale) propose les options suivantes :

- Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA)
- Software Upgrade (Mettre à niveau le logiciel)



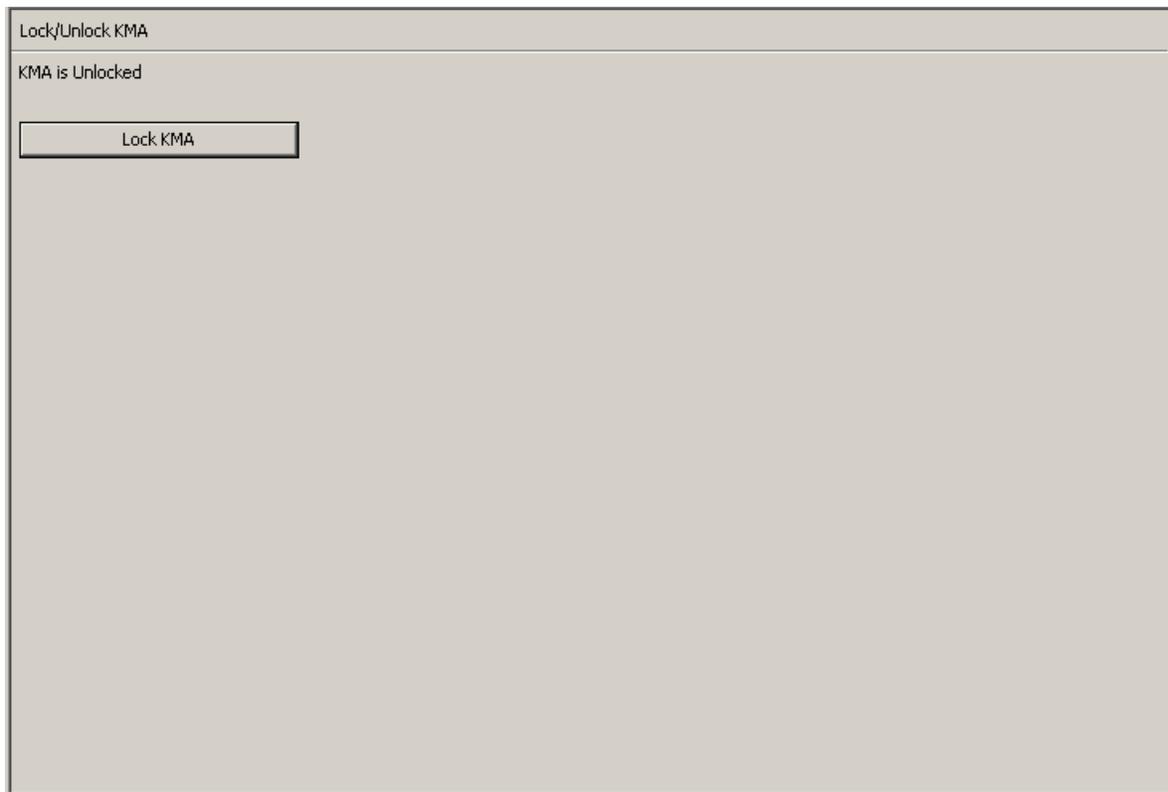
## Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA)

L'option de menu Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA) permet au responsable de la sécurité de verrouiller ou de déverrouiller la sécurité principale du KMA. Reportez-vous à la section « [Sécurité principale](#) », page 155 pour en savoir plus sur la sécurité principale et le comportement du KMA lorsque celle-ci est verrouillée ou déverrouillée.

### Verrouillage du KMA

Pour verrouiller le KMA :

1. Dans le menu System Management (Gestion du système), choisissez Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA). L'écran Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA) s'affiche, indiquant l'état du KMA. Dans cet exemple, il s'agit de l'état Unlocked.



2. Cliquez sur le bouton Lock KMA (Verrouiller le KMA) afin de verrouiller le KMA. Une fois le bouton activé, il se transforme en Unlock KMA (Déverrouiller le KMA), indiquant le nouvel état de verrouillage et l'opération autorisée. Le KMA est à présent verrouillé.

---

**Remarque** – Le bouton Lock KMA/Unlock KMA permet de basculer entre les deux états et de définir l'état verrouillé du KMA contraire à l'état actif. Une fois le bouton activé, le libellé de texte et le libellé du bouton changent de manière à refléter le nouvel état de verrouillage et l'opération autorisée.

---

## Déverrouillage du KMA

Pour déverrouiller le KMA :

1. Dans l'écran Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA), cliquez sur le bouton Unlock KMA (Déverrouiller le KMA).



2. La boîte de dialogue Key Split Quorum Authentication (Authentification du quorum de scission de clés) s'affiche. Le quorum doit saisir les noms d'utilisateur et phrases de passe correspondantes afin d'authentifier l'opération.

**Key Split Quorum Authentication** [X]

To perform this operation, you must authenticate with a quorum of the existing Core Security key split credentials.

Split User 1:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 2:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 3:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 4:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 5:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 6:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 7:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 8:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 9:	<input type="text"/>	Passphrase:	<input type="text"/>
Split User 10:	<input type="text"/>	Passphrase:	<input type="text"/>

OK Cancel

3. Cliquez sur le bouton OK une fois le dernier nom d'utilisateur et la dernière phrase de passe indiqués. Les noms d'utilisateur et les phrases de passe sont envoyés au KMA à des fins d'authentification.

4. Si l'authentification réussit, la boîte de dialogue Key Split Quorum Authentication (Authentification du quorum de scission de clés) se ferme et le KMA est déverrouillé.



## Menu System Time (Heure système)

L'option de menu System Time (Heure système) permet à l'utilisateur de définir l'horloge système à laquelle l'utilisateur est connectée. Pour garantir le bon fonctionnement de la solution KMS, il est extrêmement important de maintenir les heures des différents KMA d'un cluster dans une plage d'écart maximale de cinq minutes les uns par rapport aux autres

### Récupération des informations sur l'horloge locale

Pour récupérer les informations sur l'horloge locale :

Dans le menu Local Configuration (Configuration locale), choisissez **System Time (Heure système)**. L'écran System Time (Heure système) s'affiche.

System Time

Current System Time: 12/21/2007 10:52:07 AM

System Time Retrieved at: 12/21/2007 10:51:30 AM

Adjust Time...

NTP Server:

Specify NTP Server

Les champs et leur description sont fournis ci-dessous :

**Current System Time (Heure système actuelle)**

Affiche l'heure système active.

**System Time Retrieved At (Heure système récupérée à)**

Affiche l'heure locale du client au moment de la récupération de l'heure système du KMA.

**Adjust Time (Régler l'heure)**

Cliquez sur ce bouton pour modifier l'heure système.

Si vous souhaitez modifier l'horloge du KMA, cliquez sur le bouton Adjust Time (Régler l'heure). Pour plus d'informations, reportez-vous à la section « [Réglage de l'horloge locale du KMA](#) » ci-dessous.

**NTP Server (Serveur NTP)**

Affiche le serveur NTP utilisé par ce KMA (le cas échéant).

**Specify NTP Server (Spécifier le serveur NTP)**

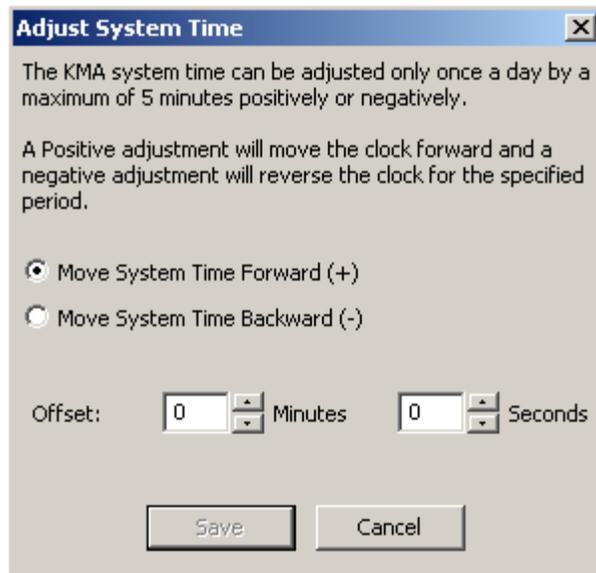
Cliquez sur ce bouton pour spécifier le serveur NTP devant être utilisé par ce KMA.

## Réglage de l'horloge locale du KMA

**Vous pouvez uniquement régler l'horloge d'un KMA une fois par jour d'un écart maximal de plus ou moins 5 minutes.** Un réglage positif (+) fait avancer l'horloge lentement tandis qu'un réglage négatif (-) la fait reculer.

Pour régler l'heure locale du KMA :

1. Dans le menu System Time (Heure système), cliquez sur le bouton Adjust Time (Régler l'heure). La boîte de dialogue Adjust System Time (Réglage de l'heure système) s'affiche.



2. Sélectionnez le bouton radio Move System Time Forward (+) (Avancer l'heure système) afin d'appliquer un réglage positif à l'horloge. Sinon, sélectionnez le bouton radio Move System Time Backward (-) (Reculer l'heure système) pour appliquer un réglage négatif à l'horloge.
3. Dans la zone de texte Offset Minutes (Minutes de décalage), sélectionnez un nombre.
4. Dans la zone de texte Offset Seconds (Secondes de décalage), sélectionnez un nombre.

---

**Remarque** – Si le décalage spécifié est trop grand, un message d'erreur s'affiche, vous invitant à saisir une valeur plus petite. Cliquez sur OK pour fermer la boîte de dialogue, puis saisissez une nouvelle valeur.

---

5. Cliquez sur Save (Enregistrer) pour valider les modifications. L'horloge système est réglée.

## Tâches du responsable de la conformité

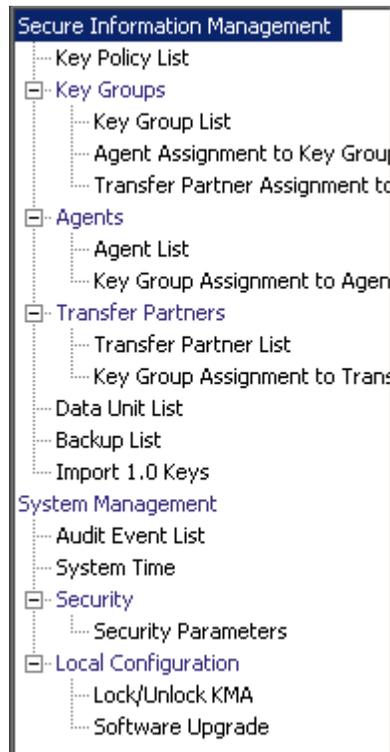
---

Ce chapitre décrit les opérations pouvant être effectuées par un utilisateur doté du rôle Compliance Officer (Responsable de la conformité). Si plusieurs rôles vous ont été assignés, reportez-vous aux chapitres appropriés. Vous y trouverez des instructions sur les tâches associées à chaque rôle.

---

## Rôle Compliance Officer (Responsable de la conformité)

L'utilisateur doté du rôle Compliance Officer (Responsable de la conformité) est chargé de gérer le flux de données à l'échelle de l'entreprise. Il est habilité à définir et à déployer les contextes de données (groupes de clés) et les règles déterminant le mode de protection et, en dernier lieu, de destruction des données (stratégies de clés). Les menus proposant ces fonctions sont indiqués ci-dessous.



---

## Stratégies de clés

Les stratégies de clés orientent le mode de gestion des données. KMS Manager fait appel à des stratégies de clés afin de déterminer les modes de protection et de destruction des données. Les stratégies de clés doivent être définies préalablement à la création des clés et à leur transmission aux agents.

Seul un utilisateur de type Compliance Officer (Responsable de la conformité) est habilité à créer et à modifier des stratégies de clés. Cette restriction permet de garantir la conformité des données à une stratégie pendant toute leur durée de vie.

### Menu Key Policy List (Liste des stratégies de clés)

Le menu Key Policies List (Liste des stratégies de clés) vous permet de gérer les stratégies de clés appliquées dans l'entreprise.

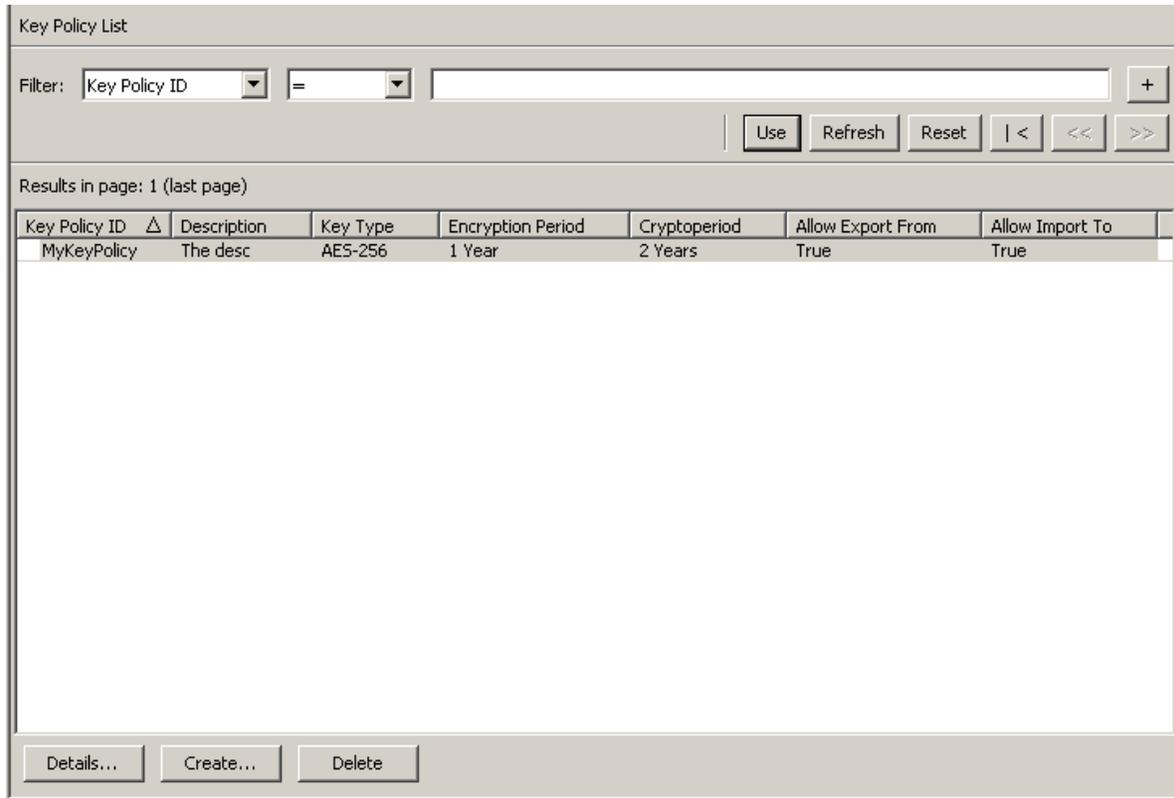
L'option de menu Key Policy List (Liste des stratégies de clés) vous permet d'effectuer les opérations suivantes :

- Affichage des stratégies de clés
- Affichage/Modification des détails d'une stratégie de clés
- Création d'une stratégie de clés
- Suppression d'une stratégie de clés existante

## Affichage des stratégies de clés

Pour afficher les stratégies de clés :

1. Dans le menu Secure Information Management (Gestion des informations sécurisées), choisissez **Key Policy List (Liste des stratégies de clés)**. L'écran Key Policy List (Liste des stratégies de clés) s'affiche.



Vous pouvez également faire défiler la base de données et filtrer la liste des stratégies de clés selon l'un des critères suivants :

- Key Policy ID (ID de la stratégie de clés)
- Description
- Key Type (Type de clé)
- Encryption Period (Période de chiffrement)
- Cryptoperiod (Durée de validité)
- Allow Export From (Autoriser l'exportation depuis)
- Allow Import To (Autoriser l'importation vers)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour la stratégie de clés.

Les champs et leur description sont fournis ci-dessous :

**Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Key Policy ID (ID de la stratégie de clés)
- Description
- Key Type (Type de clé)
- Encryption Period (Période de chiffrement)
- Cryptoperiod (Durée de validité)
- Allow Export From (Autoriser l'exportation depuis)
- Allow Import To (Autoriser l'importation vers)

**Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

**Zone de texte Filter Value (Valeur de filtre)**

Indiquez la valeur selon laquelle l'attribut sélectionné doit être trié. Cette option de filtrage est masquée pour certains attributs.

**Boîte combinée Filter Value (Valeur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez la valeur selon laquelle l'attribut sélectionné doit être filtré. Cette option de filtrage est masquée pour certains attributs.



Cliquez sur ce bouton pour ajouter d'autres filtres.



Cliquez sur ce bouton pour supprimer un filtre. Ce bouton est visible uniquement si plusieurs filtres sont affichés.

**Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer les filtres sélectionnés à la liste affichée et atteindre la première page.

**Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

**Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**Key Policy ID (ID de la stratégie de clés)**

Affiche l'identificateur unique qui différencie les stratégies de clés les unes des autres. Cet ID doit comprendre entre 1 et 64 caractères. Il est impossible de modifier un ID de stratégie de clés une fois qu'il est créé.

**Description**

Décrit la stratégie de clés. Cette description doit comprendre entre 1 et 64 caractères.

**Key Type (Type de clé)**

Indique le type d'algorithme de chiffrement utilisé par les clés associées à cette stratégie. La seule valeur possible est AES-256.

---

**Remarque** – La période de chiffrement et la durée de validité débutent au moment de la transmission initiale de la clé à un agent. Il est impossible de modifier ces deux paramètres pour une stratégie. Cette restriction a pour objectif d'empêcher qu'une modification de la stratégie de clés ait un impact sur de trop nombreuses clés.

---

**Encryption Period (Période de chiffrement)**

Indique comment les clés longues associées à cette stratégie de clés permettent de chiffrer et de déchiffrer des données. Les unités de temps utilisées sont les suivantes : minutes, heures, jours, semaines, mois et années.

**Cryptoperiod (Durée de validité)**

Indique comment les clés longues associées à cette stratégie de clés permettent de déchiffrer (mais pas de chiffrer) des données. Les unités de temps utilisées sont les suivantes : minutes, heures, jours, semaines, mois et années.

**Allow Export From (Autoriser l'exportation depuis)**

Indique si les unités de données associées à cette stratégie de clés peuvent être exportées. Les valeurs possibles sont True (Vrai) ou False (Faux).

**Allow Import To (Autoriser l'importation vers)**

Indique si les unités de données associées à cette stratégie de clés peuvent être importées. Les valeurs possibles sont True (Vrai) ou False (Faux).

Si vous souhaitez créer une stratégie de clés, cliquez sur le bouton Create (Créer). Pour plus d'informations, reportez-vous à la section « [Création d'une stratégie de clés](#) », page 180.

Si vous souhaitez visualiser/modifier une stratégie de clés, mettez-la en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage/Modification d'une stratégie de clés](#) », page 182.

Si vous souhaitez supprimer une stratégie de clés, cliquez sur le bouton Delete (Supprimer). Pour plus d'informations, reportez-vous à la section « [Suppression d'une stratégie de clés](#) », page 183.

## Création d'une stratégie de clés

Pour créer une stratégie de clés :

1. Dans l'écran Key Policy List (Liste des stratégies de clés), cliquez sur le bouton Create (Créer). L'écran Create Key Policy (Création d'une stratégie de clés) s'affiche.



2. Remplissez les champs des paramètres suivants :

### Key Policy ID (ID de la stratégie de clés)

Saisissez une valeur permettant d'identifier la stratégie. Cet ID doit comprendre entre 1 et 64 caractères.

### Description

Saisissez une valeur décrivant la stratégie. Cette description doit comprendre entre 1 et 64 caractères. Ce champ peut rester vide.

### Encryption Period (Période de chiffrement)

Indique comment les clés longues associées à cette stratégie de clés permettent de chiffrer et de déchiffrer des données. Les unités de temps utilisées sont les suivantes : minutes, heures, jours, semaines, mois et années.

### Cryptoperiod (Durée de validité)

Indique comment les clés longues associées à cette stratégie de clés permettent de déchiffrer (mais pas de chiffrer) des données. Les unités de temps utilisées sont les suivantes : minutes, heures, jours, semaines, mois et années.

**Flags (Indicateurs)****Allow Export From (Autoriser l'exportation depuis)**

Indique si les unités de données associées à cette stratégie de clés peuvent être exportées. Les valeurs possibles sont True (Vrai) ou False (Faux).

**Allow Import To (Autoriser l'importation vers)**

Indique si les unités de données associées à cette stratégie de clés peuvent être exportées. Les valeurs possibles sont True (Vrai) ou False (Faux).

3. Cliquez sur le bouton Save (Enregistrer) pour sauvegarder la stratégie de clés. La nouvelle stratégie de clés s'affiche dans l'écran Key Policy List (Liste des stratégies de clés). Elle est désormais prête à être utilisée par des groupes de clés.

Key Policy List

Filter: Key Policy ID =  +

Use Refresh Reset | < << >>

Results in page: 2 (last page)

Key Policy ID 	Description	Key Type	Encryption Period	Cryptoperiod	Allow Export From	Allow Import To
AnotherPolicy	Just a test	AES-256	1 Year	1 Year	True	True
MyKeyPolicy	The desc	AES-256	1 Year	2 Years	True	True

Details... Create... Delete

## Affichage/Modification d'une stratégie de clés

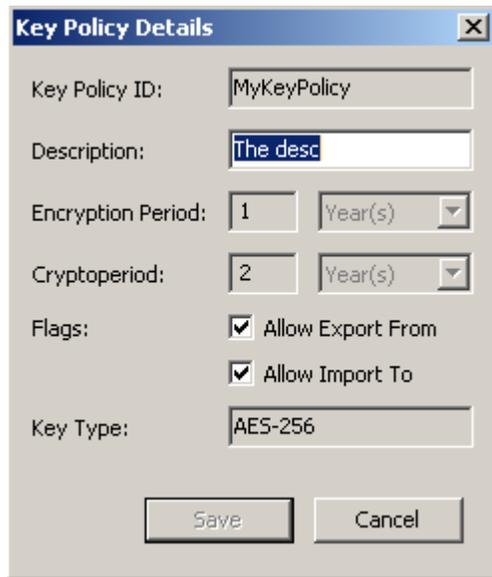
---

**Remarque** – Seul un utilisateur doté du rôle Compliance Officer (Responsable de la conformité) est habilité à afficher les informations détaillées relatives à une stratégie de clés.

---

Pour modifier les détails d'une stratégie de clés :

1. Dans l'écran Key Policy List (Liste des stratégies de clés), double-cliquez sur une stratégie de clés pour laquelle vous souhaitez obtenir des informations détaillées ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). L'écran Key Policy Details (Détails de la stratégie de clés) s'affiche.



The screenshot shows a dialog box titled "Key Policy Details". It contains the following fields and controls:

- Key Policy ID: MyKeyPolicy
- Description: The desc
- Encryption Period: 1 Year(s)
- Cryptoperiod: 2 Year(s)
- Flags:  Allow Export From,  Allow Import To
- Key Type: AES-256
- Buttons: Save, Cancel

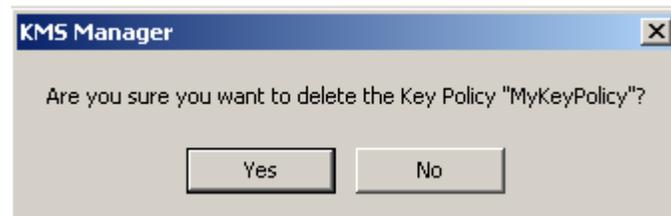
2. Le cas échéant, modifiez les valeurs des champs Description, Allow Export From et Allow Import To. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer) afin d'enregistrer les modifications. Une fois que le système a vérifié et validé la nouvelle stratégie de clés, le groupe de clés y est associé.
3. Si vous cliquez sur le bouton Cancel (Annuler), vos modifications ne sont pas enregistrées et la boîte de dialogue se ferme.

## Suppression d'une stratégie de clés

Il est possible de supprimer une stratégie de clés à condition qu'elle ne soit pas en cours d'utilisation par un groupe de clés ou une clé.

Pour supprimer une stratégie de clés :

1. Dans l'écran Key Policy List (Liste des stratégies de clés), mettez la stratégie à supprimer en surbrillance et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue suivante s'affiche, vous demandant de confirmer la suppression de la stratégie indiquée.



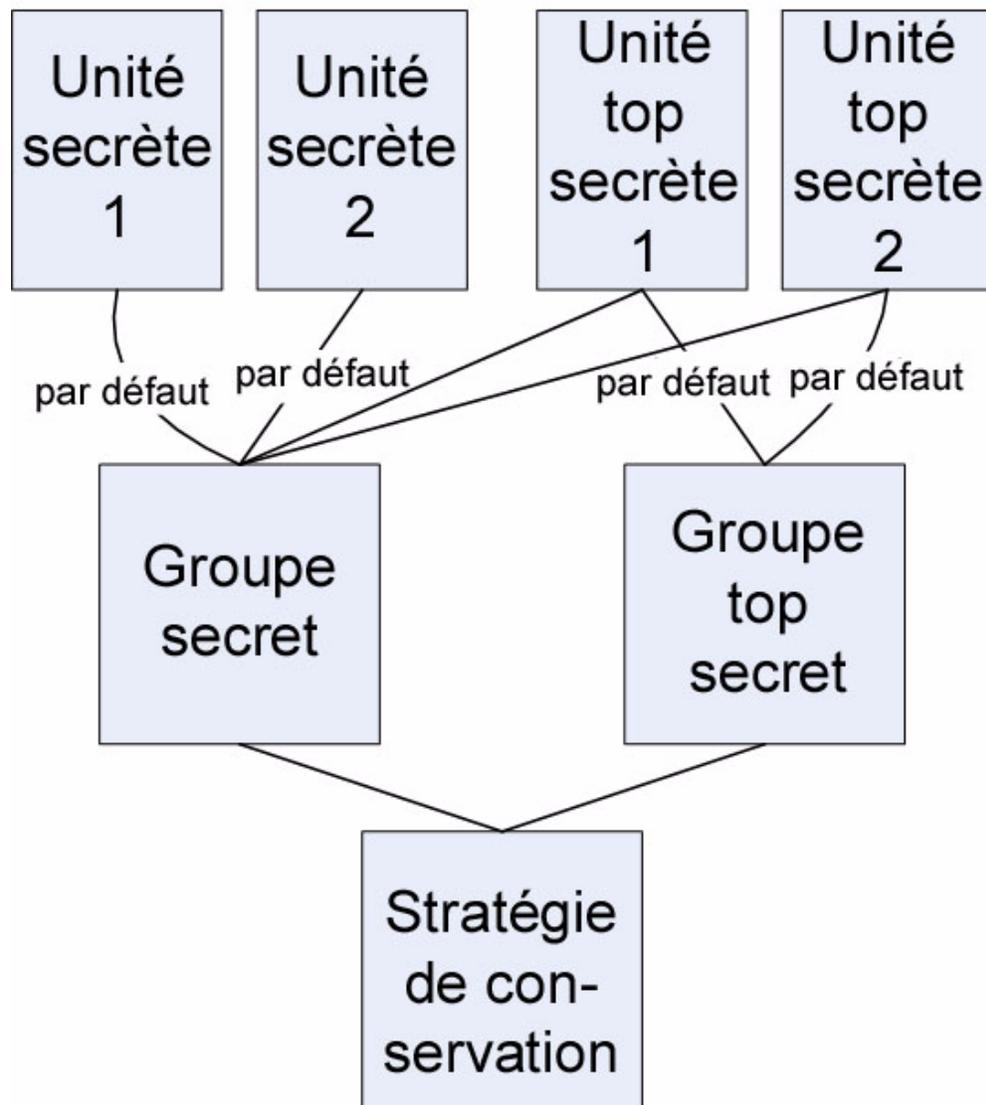
2. Cliquez sur le bouton Yes (Oui) pour supprimer la stratégie de clés. La stratégie de clés est supprimée de la base de données. Vous revenez à l'écran Key Policy List (Liste des stratégies de clés), dans lequel la stratégie n'apparaît plus.

## Groupes de clés

Un groupe de clés représente un contexte de données déterminant la stratégie de clés à laquelle il s'applique et les agents pouvant y accéder. Lorsqu'une clé est assignée à un agent et qu'elle est utilisée pour la première fois pour une unité de données, elle est associée à un groupe de clés. Lors de la création d'un groupe de clés, vous devez sélectionner une stratégie de clés. La stratégie de clés sélectionnée est alors appliquée aux clés du groupe.

Des agents sont associés aux groupes de clés. Un agent est autorisé à accéder à un ou plusieurs groupes de clés. Il peut uniquement récupérer des clés faisant partie de groupes auxquels il est autorisé à accéder. Un agent peut également disposer d'un groupe de clés par défaut. Lorsqu'un agent alloue une nouvelle clé, celle-ci est placée dans le groupe de clés par défaut qui lui est assigné. Un agent peut allouer de nouvelles clés s'il dispose d'un groupe de clés par défaut.

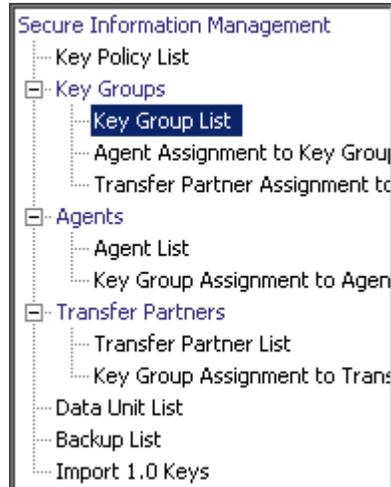
La FIGURE 6-1, page 185 indique les relations entre les groupes de clés, les stratégies de clés, les agents et les unités de données.



**FIGURE 6-1** Relations entre les groupes de clés, les stratégies de clés, les agents et les unités de données

## Menu Key Groups (Groupes de clés)

Le menu Key Groups (Groupes de clés) comprend l'option Key Group List (Liste des groupes de clés), laquelle permet au responsable de la conformité de gérer les groupes de clés.



## Menu Key Group List (Liste des groupes de clés)

L'option de menu Key Group List (Liste des groupes de clés) permet à l'utilisateur d'effectuer les opérations suivantes :

- Affichage des groupes de clés
- Création d'un groupe de clés
- Modification d'un groupe de clés existant
- Suppression d'un groupe de clés existant

## Affichage des groupes de clés

Pour afficher tous les groupes de clés :

1. Dans le menu Key Groups (Groupes de clés), choisissez **Key Group List** (Liste des groupes de clés). L'écran Key Group List (Liste des groupes de clés) s'affiche.

Key Group List

Filter: Key Group ID =

Use Refresh Reset | < << >>

Results in page: 2 (last page)

Key Group ID	Description	Key Policy ID
Key Group 1	This is the first Key Group	MyKeyPolicy
MyKeyGroup	This is a key group	MyKeyPolicy

Details... Create... Delete

Vous pouvez également faire défiler la base de données et filtrer la liste des groupes de clés selon l'un des critères suivants :

- Key Group ID (ID du groupe de clés)
- Description
- Key Policy ID (ID de la stratégie de clés)

Le bouton Use (Utiliser) applique le filtre à la liste affichée pour le groupe de clés.

Les champs et leur description sont fournis ci-dessous :

### Filter (Filtre)

Sélectionnez les options de filtrage afin de filtrer la liste des groupes de clés. Seuls les groupes de clés répondant à tous les critères de filtrage sont affichés.

### Boîte combinée Filter Attribute (Attribut de filtre)

Cliquez sur la flèche pointant vers le bas et sélectionnez un attribut de filtrage. Les valeurs possibles sont les suivantes :

- Key Group ID (ID du groupe de clés)
- Description
- Key Policy ID (ID de la stratégie de clés)

### Zone Filter Operator (Opérateur de filtre)

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opération de filtrage à appliquer à l'attribut sélectionné. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

### Zone de texte Filter Value (Valeur de filtre)

Indiquez la valeur selon laquelle l'attribut sélectionné doit être trié.

### Boîte combinée Filter Value (Valeur de filtre)

Cliquez sur la flèche pointant vers le bas et sélectionnez la valeur selon laquelle l'attribut sélectionné doit être filtré. Cette option de filtrage est masquée pour certains attributs.



Cliquez sur ce bouton pour ajouter d'autres filtres.



Cliquez sur ce bouton pour supprimer un filtre. Ce bouton est visible uniquement si plusieurs filtres sont affichés.

### Utiliser (Utiliser)

Cliquez sur ce bouton pour appliquer les filtres sélectionnés à la liste affichée et atteindre la première page.

### Refresh (Actualiser)

Ce bouton permet d'actualiser la liste affichée. Il ne s'applique pas aux filtres sélectionnés depuis la dernière activation du bouton Use (Utiliser) ou Reset (Réinitialiser), et il ne modifie pas la page de la liste.

### Reset (Réinitialiser)

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'éléments pouvant être affichés sur la page active. Ajoute la mention (last page) au nombre d'éléments si vous avez atteint la fin de la liste. Le nombre maximum d'éléments affichés sur une page est défini par la valeur de l'option Query Page Size (Taille d'une page de requête) disponible dans la boîte de dialogue Options.

**Key Group ID (ID du groupe de clés)**

Affiche l'identificateur unique qui différencie les groupes de clés les uns des autres. Cette description doit comprendre entre 1 et 64 caractères. Il est impossible de modifier un ID de groupe de clés une fois qu'il est défini.

**Description**

Décrit le groupe de clés. Cette description doit comprendre entre 1 et 64 caractères.

**Key Policy ID (ID de la stratégie de clés)**

Affiche un identificateur unique pour une stratégie de clés existante s'appliquant à chaque unité de données du groupe de clés.

Il est impossible de modifier l'ID d'une stratégie de clés appliquée à un groupe de clés existant. Cette restriction permet d'éviter qu'un changement ait un impact sur un trop grand nombre de clés.

Si vous souhaitez créer un groupe de clés, cliquez sur le bouton Create (Créer). Pour plus d'informations, reportez-vous à la section « [Création d'un groupe de clés](#) », page 190.

Si vous souhaitez visualiser/modifier un groupe de clés, mettez-le en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage/Modification des détails d'un groupe de clés](#) », page 192.

Si vous souhaitez supprimer un groupe de clés, cliquez sur le bouton Delete (Supprimer). Pour plus d'informations, reportez-vous à la section « [Suppression d'un groupe de clés](#) », page 193.

## Création d'un groupe de clés

Pour créer un groupe de clés :

1. Dans l'écran Key Group List (Liste des groupes de clés), cliquez sur le bouton Create (Créer). L'écran Create Key Group (Création d'un groupe de clés) s'affiche.



The screenshot shows a dialog box titled "Create Key Group" with a close button (X) in the top right corner. It contains three input fields: "Key Group ID:" followed by a text box, "Description:" followed by a text box, and "Key Policy ID:" followed by a dropdown menu showing "Please Select a Key Policy". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

2. Remplissez les champs des paramètres suivants :

### Key Group ID (ID du groupe de clés)

Saisissez une valeur permettant d'identifier le groupe de clés. Cette valeur doit comprendre entre 1 et 64 caractères.

### Description

Saisissez une valeur décrivant le groupe de clés. Cette valeur doit comprendre entre 1 et 64 caractères.

### Key Policy ID (ID de la stratégie de clés)

Cliquez sur la flèche pointant vers le bas et sélectionnez la stratégie à laquelle vous souhaitez associer ce groupe de clés. Lors de la création d'un groupe de clés, les stratégies de clés existantes s'affichent.

3. Cliquez sur le bouton Save (Enregistrer). Le nouveau groupe de clés est créé et enregistré dans la base de données. Il figure dans l'écran Key Group List (Liste des groupes de clés). Il est désormais prêt pour être utilisé par des unités de données, des agents, etc.

Key Group List

Filter: Key Group ID ▾ = ▾  +

Use Refresh Reset | < << >>

Results in page: 3 (last page)

Key Group ID <small>△</small>	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

## Affichage/Modification des détails d'un groupe de clés

---

**Remarque** – Si vous n'êtes pas responsable de la conformité, tous les champs (y compris le bouton Save (Enregistrer)) sont désactivés lors de la visualisation des informations détaillées relatives à un groupe de clés.

---

Pour modifier un groupe de clés :

1. Dans l'écran Key Group List (Liste des groupes de clés), double-cliquez sur une entrée du groupe de clés pour laquelle vous souhaitez obtenir des informations détaillées ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). L'écran Key Group Details (Détails du groupe de clés) s'affiche.



Les paramètres suivants s'affichent à l'écran :

**Key Group ID (ID du groupe de clés)**

Permet d'identifier de manière unique le groupe de clés. Ce champ est en lecture seule.

**Description**

Saisissez une valeur décrivant le groupe de clés. Cette valeur doit comprendre entre 1 et 64 caractères. Ce champ peut rester vide.

**Key Policy ID (ID de la stratégie de clés)**

Affiche l'identificateur unique d'une stratégie de clés existante associée au groupe de clés ainsi que toutes les clés faisant partie du groupe. Ce champ est en lecture seule.

2. Le champ Description est le seul champ modifiable. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer) afin d'enregistrer les modifications. Vous revenez à l'écran Key Group List (Liste des groupes de clés).

## Suppression d'un groupe de clés

---

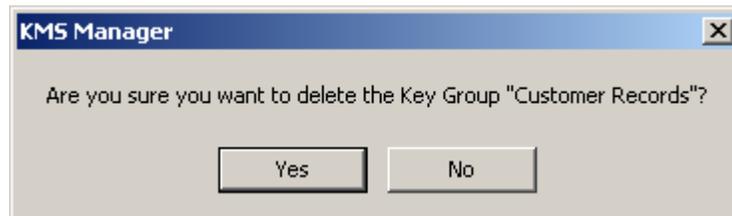
**Remarque** – Il est impossible de supprimer un groupe de clés actif, c'est-à-dire un groupe auquel des agents ou des unités de données sont assignés.

---

Pour supprimer un groupe de clés :

1. Dans l'écran Key Groups List (Liste des groupes de clés), mettez le groupe à supprimer en surbrillance et cliquez sur le bouton Delete (Supprimer). La boîte de dialogue de confirmation vous invite à confirmer l'opération.

Il est possible de supprimer un groupe de clés uniquement lorsqu'il n'est pas utilisé par une clé et lorsqu'il n'est pas associé à un agent.



2. Cliquez sur le bouton Yes (Oui) pour supprimer le groupe de clés. Le groupe de clés et les entrées associées sont supprimés de la base de données. Vous revenez à l'écran Key Groups List (Liste des groupes de clés), dans lequel le groupe de clés ne figure plus.

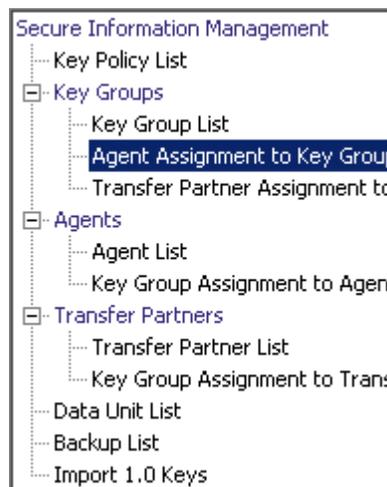
## Menu Agent Assignment to Key Groups (Assignation d'un agent à des groupes de clés)

L'option de menu Agent Assignment to Key Groups (Assignation d'un agent à des groupes de clés) permet à l'utilisateur d'assigner des agents à des groupes de clés. Lorsque vous assignez un agent à des groupes de clés, vous identifiez les périphériques de stockage auxquels l'agent peut accéder. Cette option fonctionne en parallèle avec l'option Key Group Assignment (Assignation d'un groupe de clés) disponible dans le menu Agents, les deux aboutissant au même résultat.

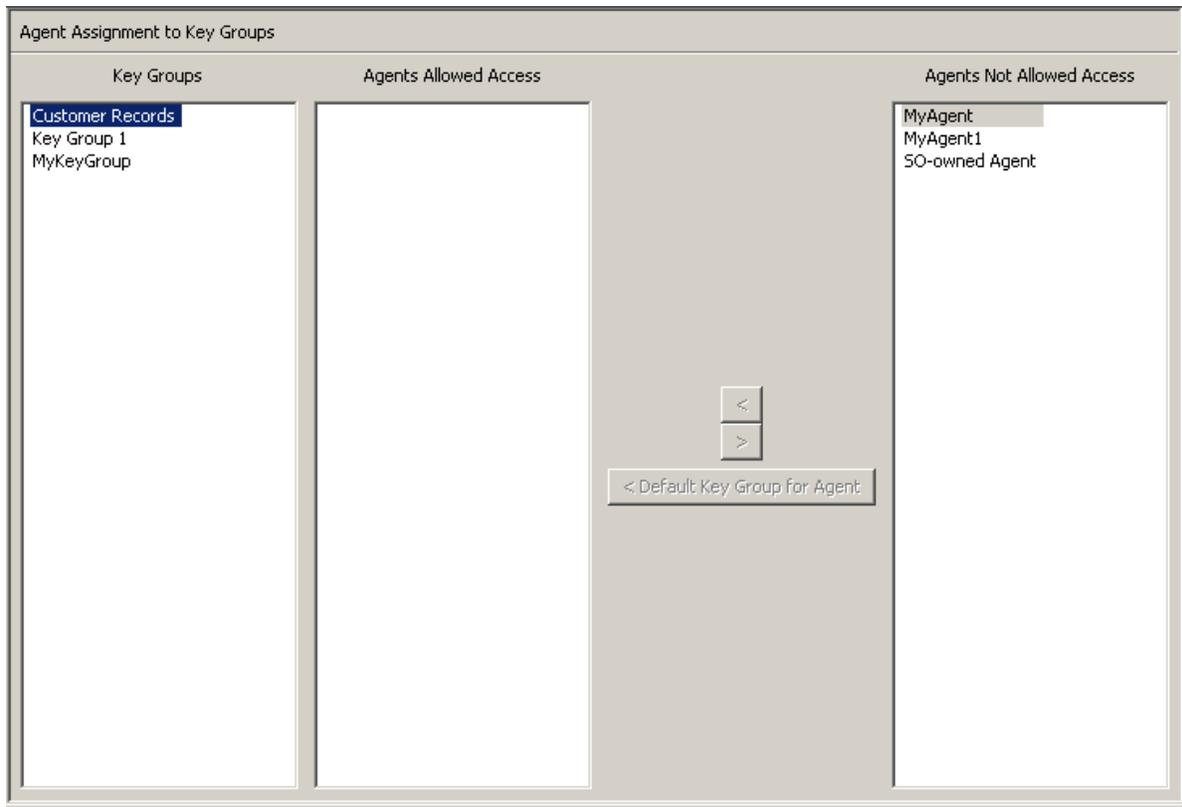
---

**Important** – Vous devez définir un groupe de clés par défaut pour un agent avant que celui-ci puisse allouer des clés.

---



Pour afficher les assignations d'agents, dans le menu Key Groups (Groupes de clés), choisissez Agent Assignment to Key Groups (Assignment d'un agent à des groupes de clés). L'écran Agent Assignment to Key Groups (Assignment d'un agent à des groupes de clés) s'affiche.

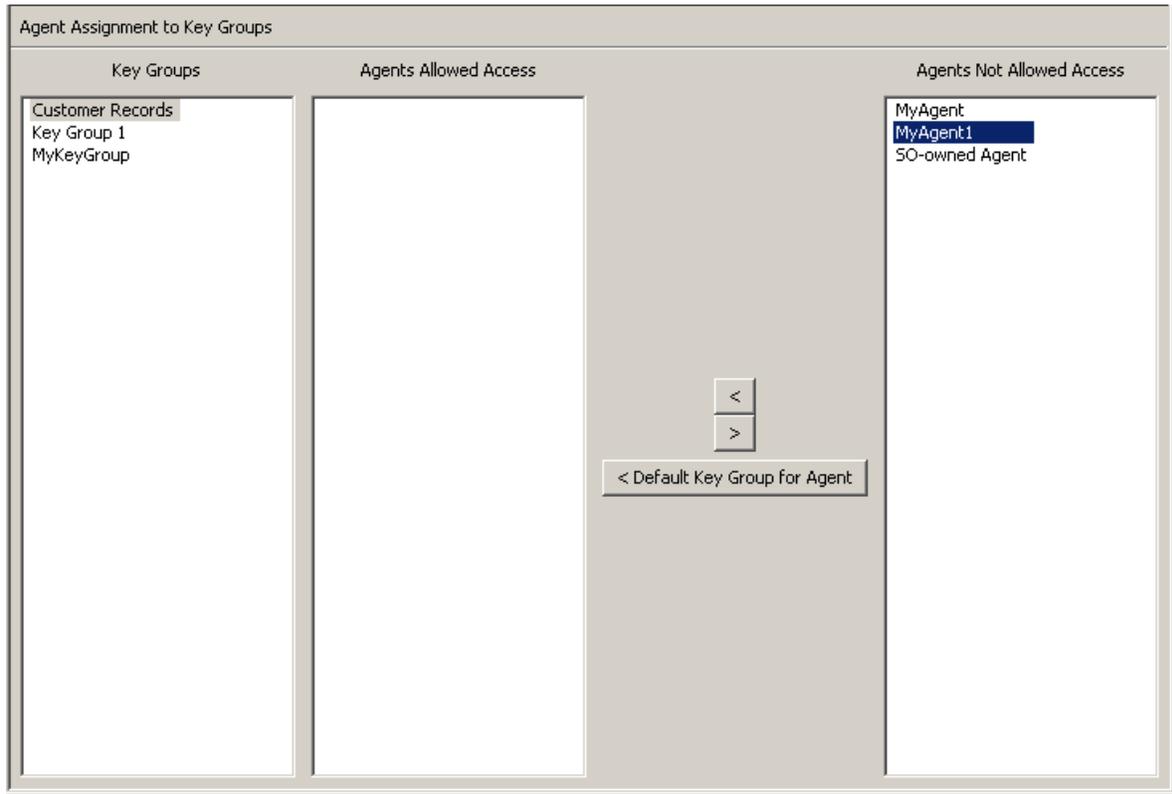


La colonne Key Groups dresse la liste des groupes de clés. La colonne Agents Allowed Access dresse la liste des agents assignés au(x) groupe(s) de clés sélectionné(s). La colonne Agents Not Allowed Access dresse la liste des agents non assignés au(x) groupe(s) de clés sélectionné(s).

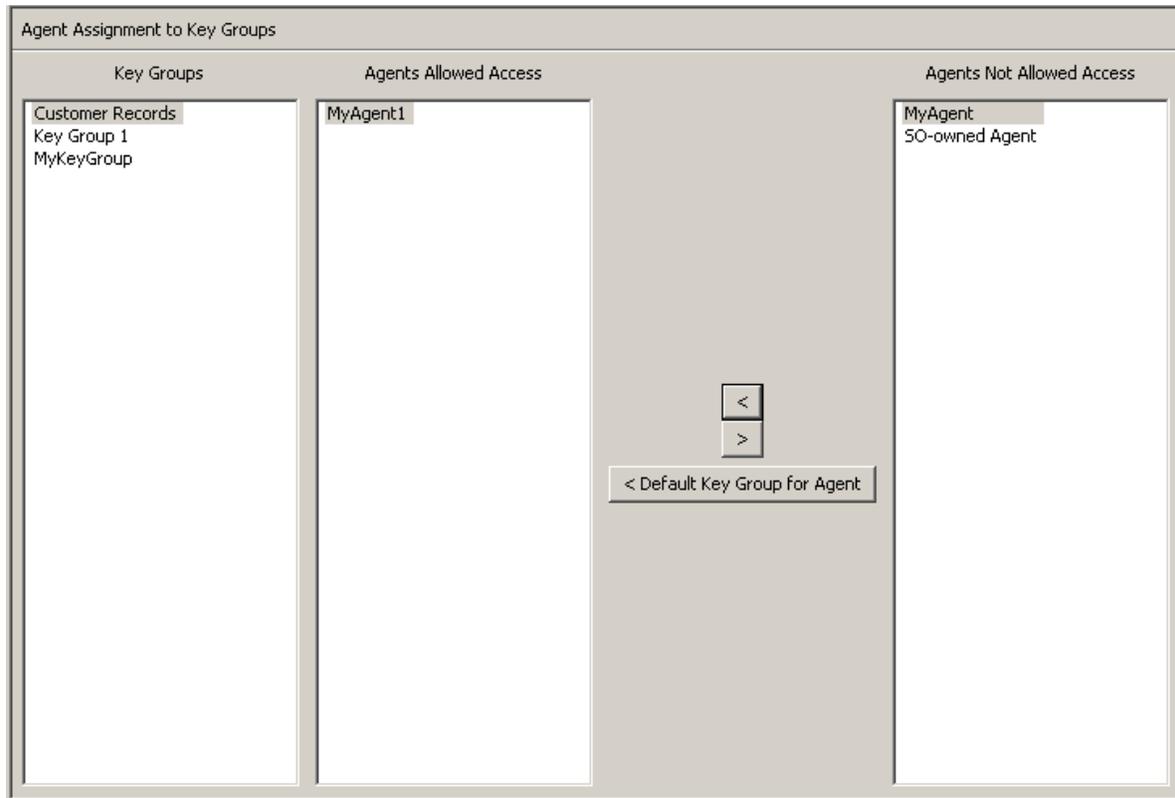
## Assignment d'un agent à un groupe de clés

Pour assigner un agent à un groupe de clés :

1. Dans la colonne Key Groups (Groupes de clés), mettez le groupe souhaité en surbrillance. Dans la colonne Agents Not Allowed Access (Agents non autorisés), mettez en surbrillance l'agent à ajouter, puis cliquez sur le bouton Move to  (Déplacer vers).



- L'agent sélectionné est déplacé vers la colonne Agents Allowed Access (Agents autorisés), indiquant que l'agent a bien été ajouté à la liste des agents du groupe de clés sélectionné.



Pour assigner un agent à un groupe de clés et définir le groupe de clés par défaut :

- Dans l'écran Agent Assignment to Key Groups (Assignment d'un agent à un groupe de clés), sélectionnez le groupe de clés voulu dans la liste.
- Dans la liste des agents non autorisés, sélectionnez un ou plusieurs agents et définissez le groupe de clés par défaut correspondant.
- Cliquez sur le bouton Default Key Group for Agent (Groupe de clés par défaut de l'agent). Les agents sélectionnés sont déplacés vers la liste des agents autorisés et leur groupe de clés par défaut est défini pour le groupe de clés. Les agents sont dorénavant autorisés à accéder au groupe de clés.

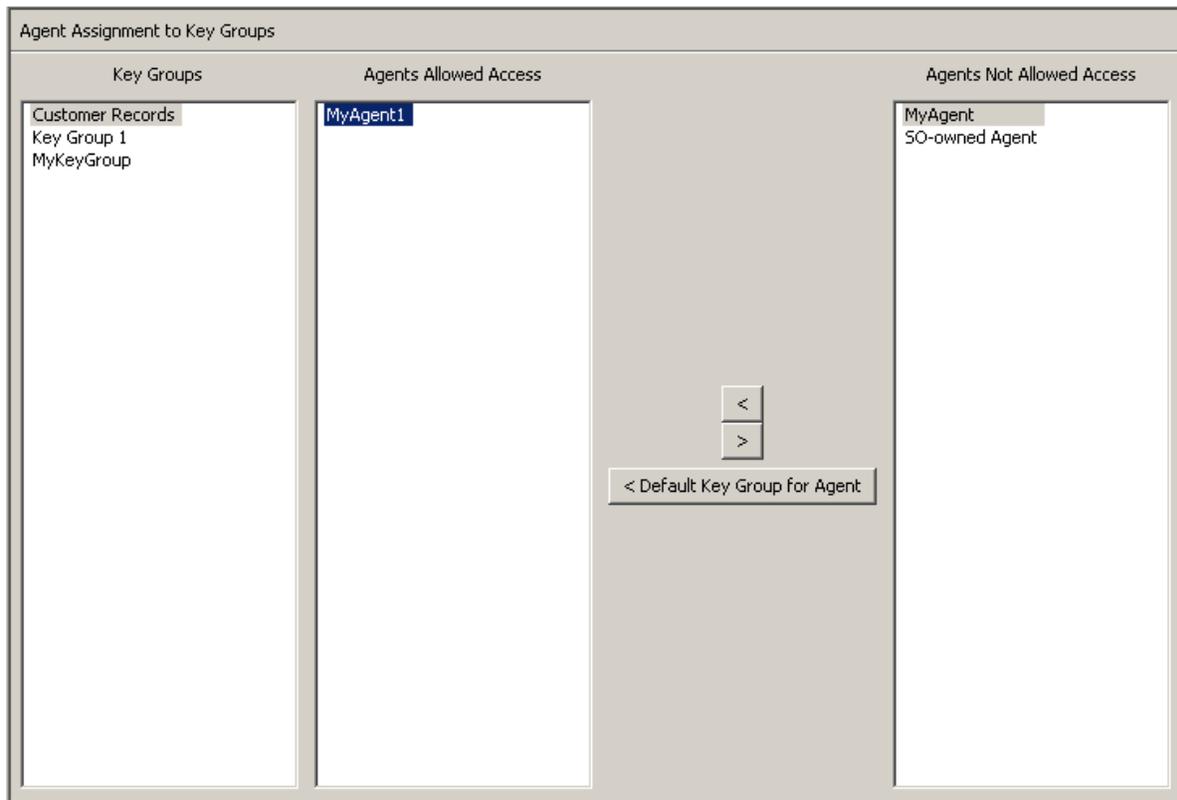
Pour définir le groupe de clés par défaut d'agents déjà assignés :

- Dans l'écran Agent Assignment to Key Groups (Assignment d'un agent à un groupe de clés), sélectionnez le groupe de clés voulu dans la liste.
- Dans la liste Agents Allowed Access (Agents autorisés), sélectionnez un ou plusieurs agents pour lesquels le groupe de clés sélectionné n'est pas défini par défaut.
- Cliquez sur le bouton Default Key Group for Agent (Groupe de clés par défaut de l'agent). Le groupe de clés par défaut des agents sélectionnés est défini pour le groupe de clés.

## Suppression d'un agent dans un groupe de clés

Pour supprimer un agent de la liste des agents d'un groupe de clés :

1. Dans la colonne Key Groups (Groupes de clés), mettez le groupe souhaité en surbrillance. Dans la colonne Agents Allowed Access (Agents autorisés), mettez en surbrillance l'agent à supprimer, puis cliquez sur le bouton Move from  (Déplacer depuis).



2. L'entrée sélectionnée est supprimée de la colonne des agents autorisés et figure dans celle des agents non autorisés. L'agent n'est plus assigné au groupe de clés sélectionné.

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

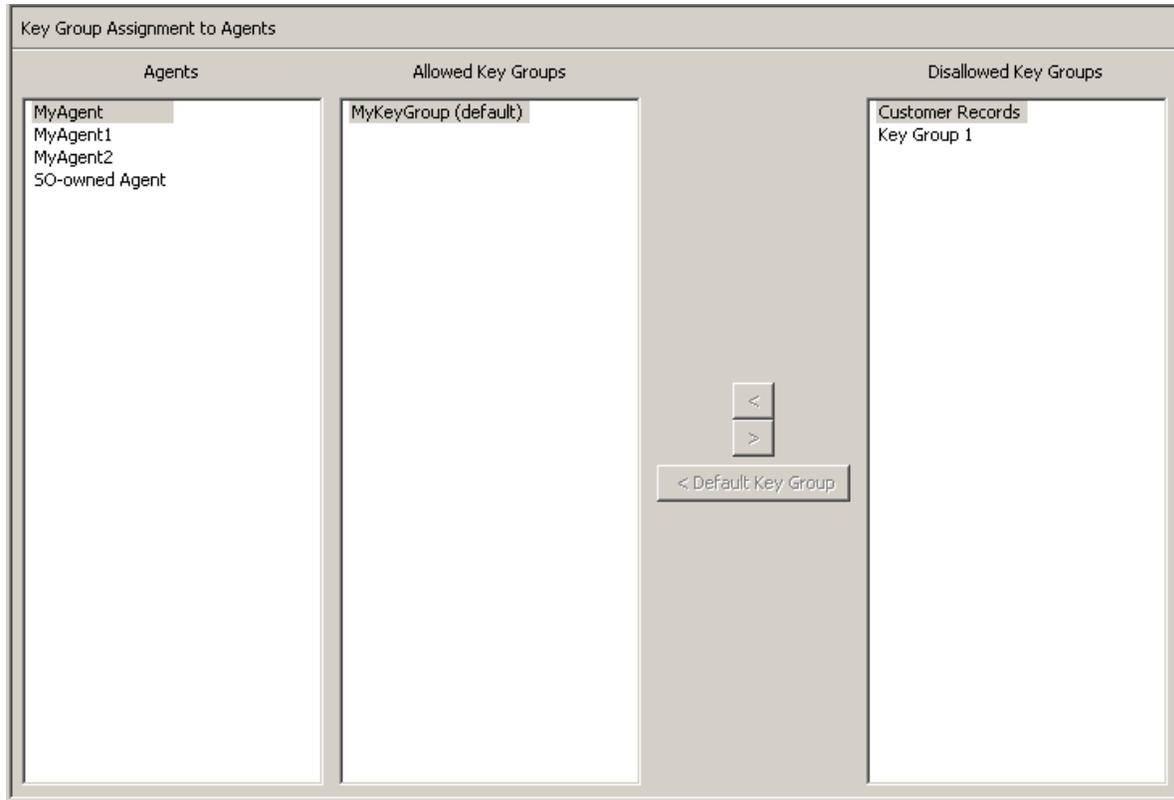
## Menu Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent)

L'option de menu Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent) vous permet d'assigner des groupes de clés à un agent. Cette option fonctionne en parallèle avec l'option Agent Assignment to Key Groups (Assignment d'un agent à des groupes de clés), les deux aboutissant au même résultat.



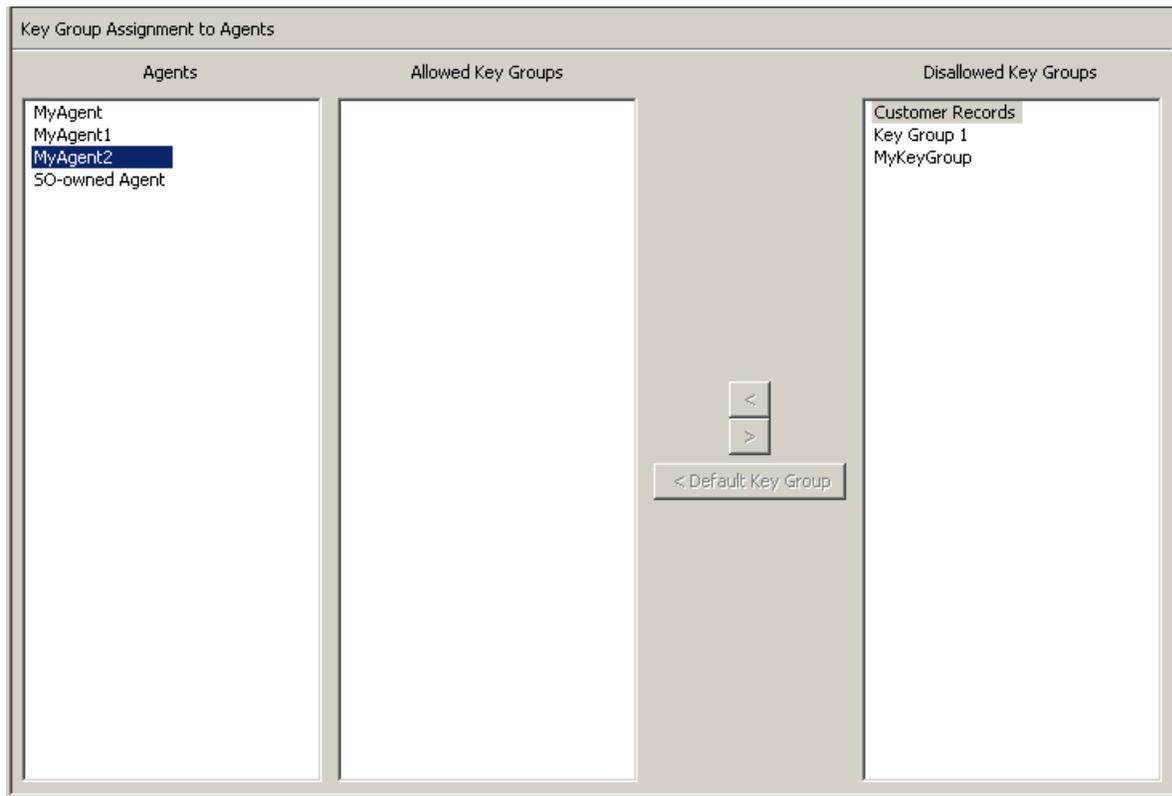
Pour afficher les groupes de clés :

1. Dans le menu Agents, choisissez Key Group Assignment (Assignment d'un groupe de clés). L'écran Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent) s'affiche.



La colonne Agents dresse la liste des agents figurant dans la base de données. La colonne Allowed Key Groups (Groupes de clés autorisés) indique les groupes de clés auxquels l'agent a accès tandis que la colonne Disallowed Key Groups (Groupes de clés non autorisés) présente ceux auxquels il n'a pas accès.

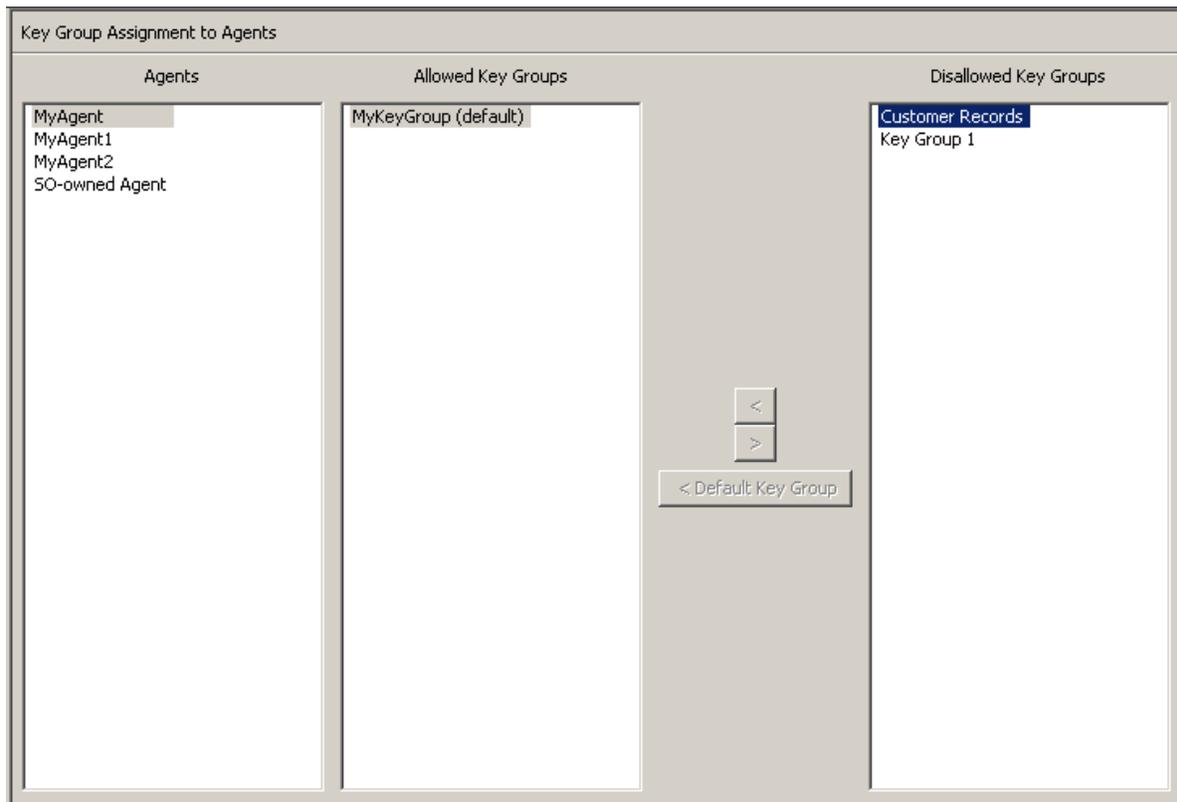
2. Si vous cliquez sur une entrée d'agent, les groupes de clés faisant partie ou non de l'agent sont affichés.



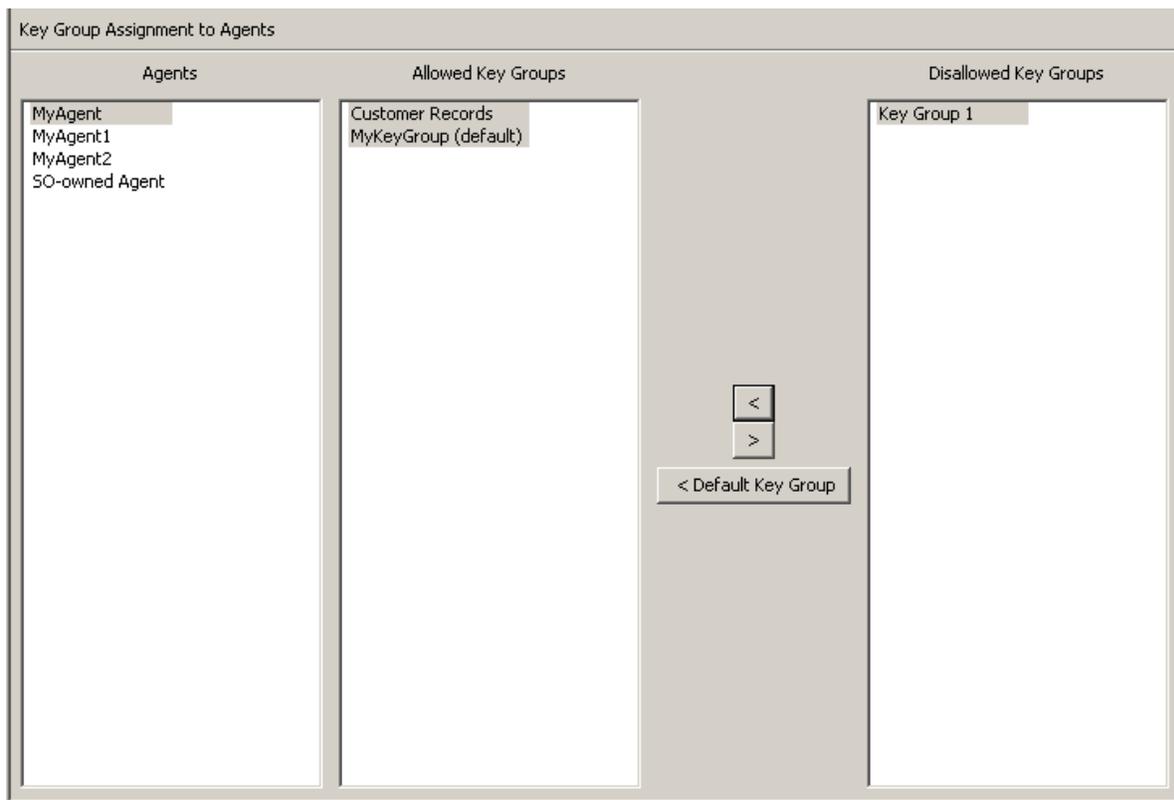
## Assignment d'un groupe de clés à un agent

Pour assigner un groupe de clés à un agent :

1. Dans l'écran Key Group Assignment to Agents (Assignment d'un groupes de clés à un agent), dans la colonne Agents, mettez l'agent voulu en surbrillance. Dans la colonne Disallowed Key Groups (Groupes de clés non autorisés), mettez le groupe à ajouter en surbrillance et cliquez sur le bouton Move to  (Déplacer vers).



2. L'entrée sélectionnée est déplacée vers la colonne Allowed Key Groups (Groupes de clés autorisés) et le groupe est ajouté à l'agent sélectionné.



Pour assigner un groupe de clés à un agent comme groupe par défaut :

1. Dans l'écran Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent), sélectionnez l'agent voulu dans la liste.
2. Dans la liste des groupes de clés non autorisés, sélectionnez le groupe à ajouter et définissez-le par défaut.
3. Cliquez sur le bouton Default Key Group (Groupe de clés par défaut). Le groupe de clés sélectionné est déplacé vers la liste Allowed Key Groups (Groupes de clés autorisés) et est défini par défaut pour l'agent. L'agent est dorénavant autorisé à accéder au groupe de clés.

Pour définir un groupe de clés déjà assigné au groupe par défaut :

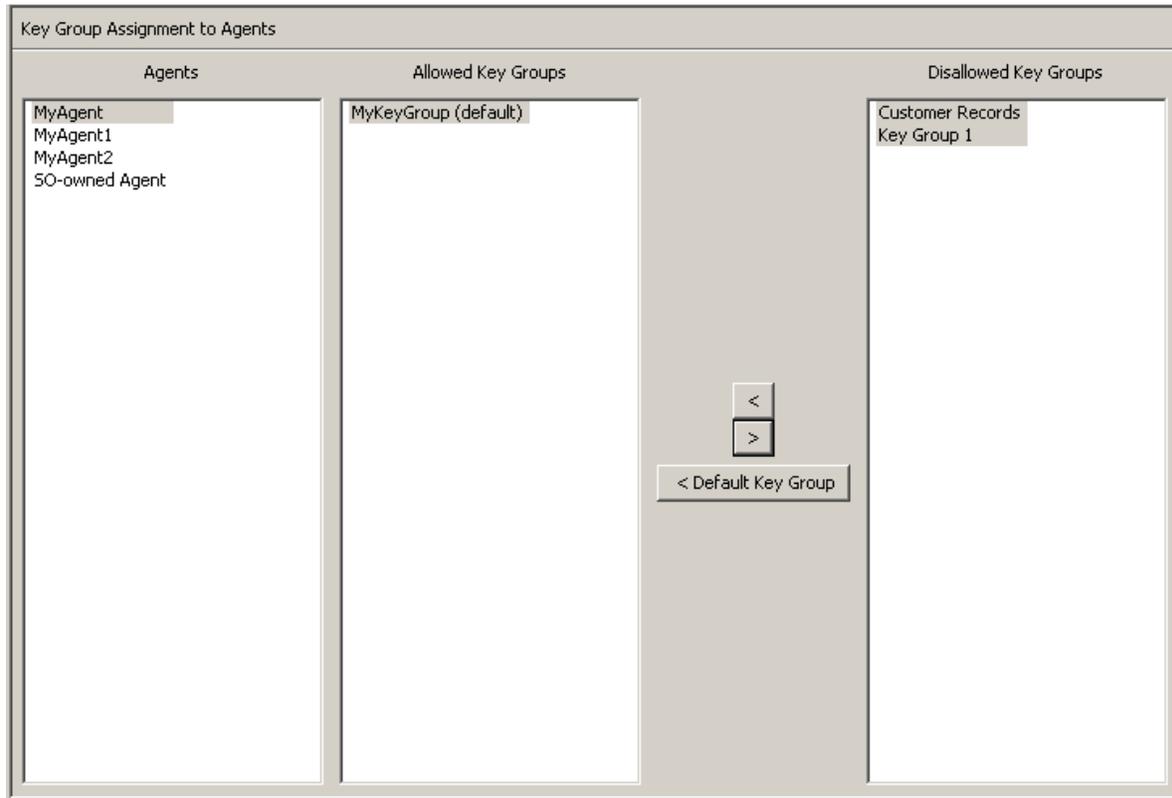
1. Dans l'écran Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent), sélectionnez l'agent voulu dans la liste.
2. Dans la liste Allowed Key Groups (Groupes de clés autorisés), sélectionnez un groupe non défini par défaut pour l'agent.

Cliquez sur le bouton Default Key Group (Groupe de clés par défaut). Le groupe de clés par défaut de l'agent est défini pour le groupe de clés sélectionné.

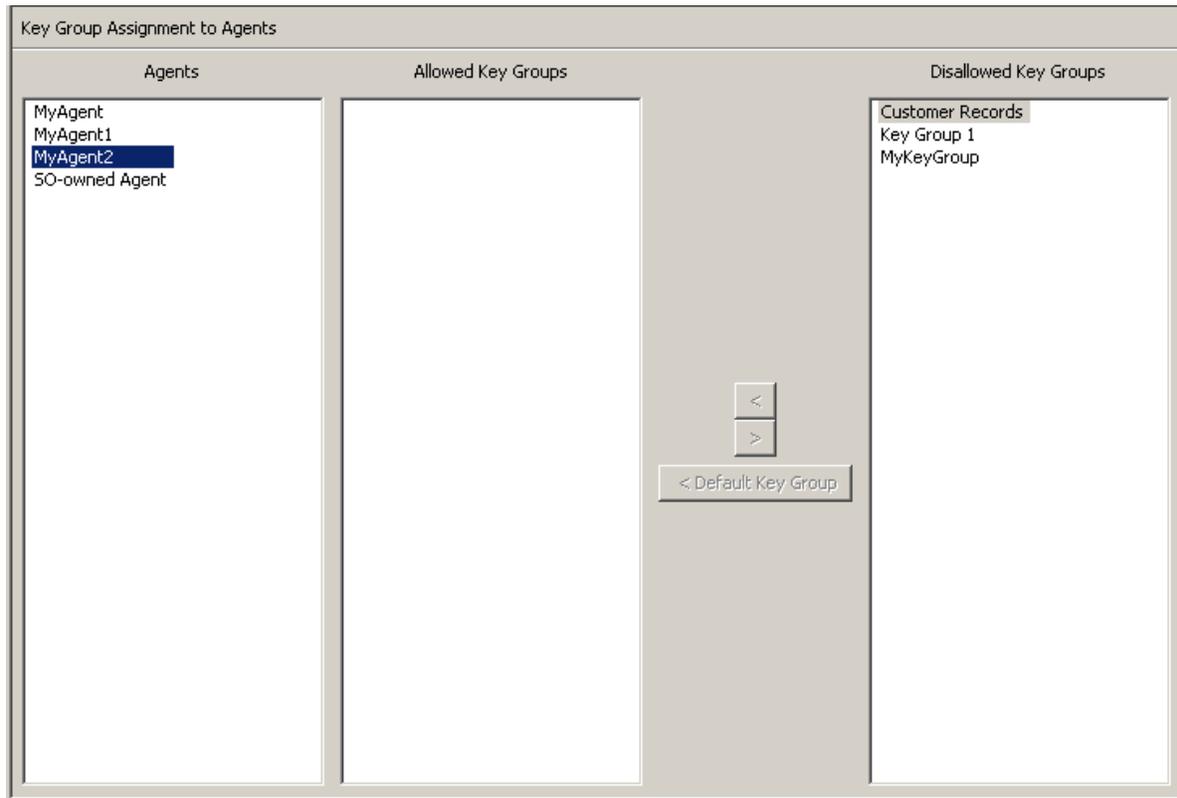
## Suppression d'un groupe de clés pour un agent

Pour supprimer un groupe de clés d'un agent :

1. Dans l'écran Key Group Assignment to Agents (Assignment d'un groupes de clés à un agent), dans la colonne Agents, mettez l'agent voulu en surbrillance. Dans la colonne Allowed Key Groups (Groupes de clés autorisés), mettez le groupe à supprimer en surbrillance et cliquez sur le bouton Move from  (Déplacer depuis).



2. L'entrée sélectionnée est supprimée de la colonne Allowed Key Groups (Groupes de clés autorisés) vers la colonne Non-member of Info. Groups (Non membre des groupes d'infos.) et n'est plus assignée à l'agent.



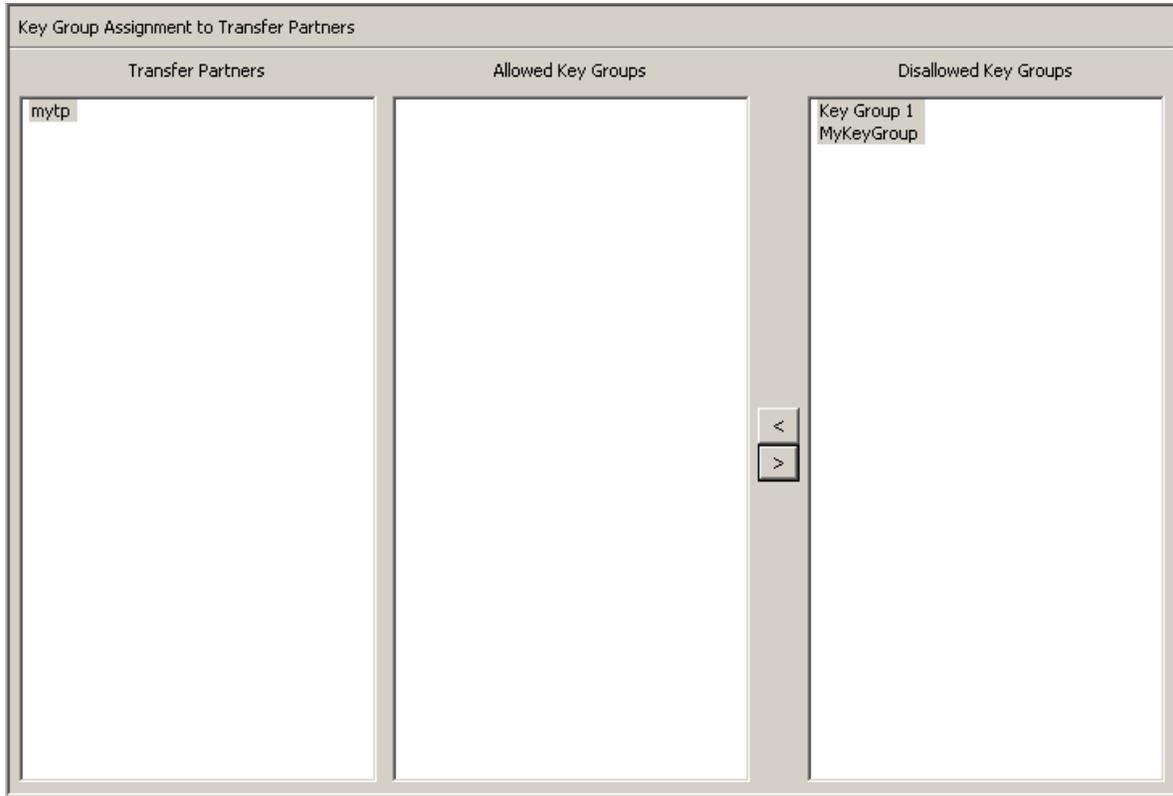
## Menu Key Group Assignment to Transfer Partners (Assignment d'un groupe de clés à un partenaire de transfert)

L'option de menu Key Group Assignment to Transfer Partners (Assignment d'un groupe de clés à un partenaire de transfert) vous permet d'assigner des groupes de clés à des partenaires de transfert.



## Affichage des assignations de groupes de clés

Pour afficher les assignations de groupes de clés, dans le menu Transfer Partners (Partenaires de transfert), choisissez Key Group Assignment to Transfer Partners (Assignation d'un groupe de clés à un partenaire de transfert). L'écran suivant s'affiche.

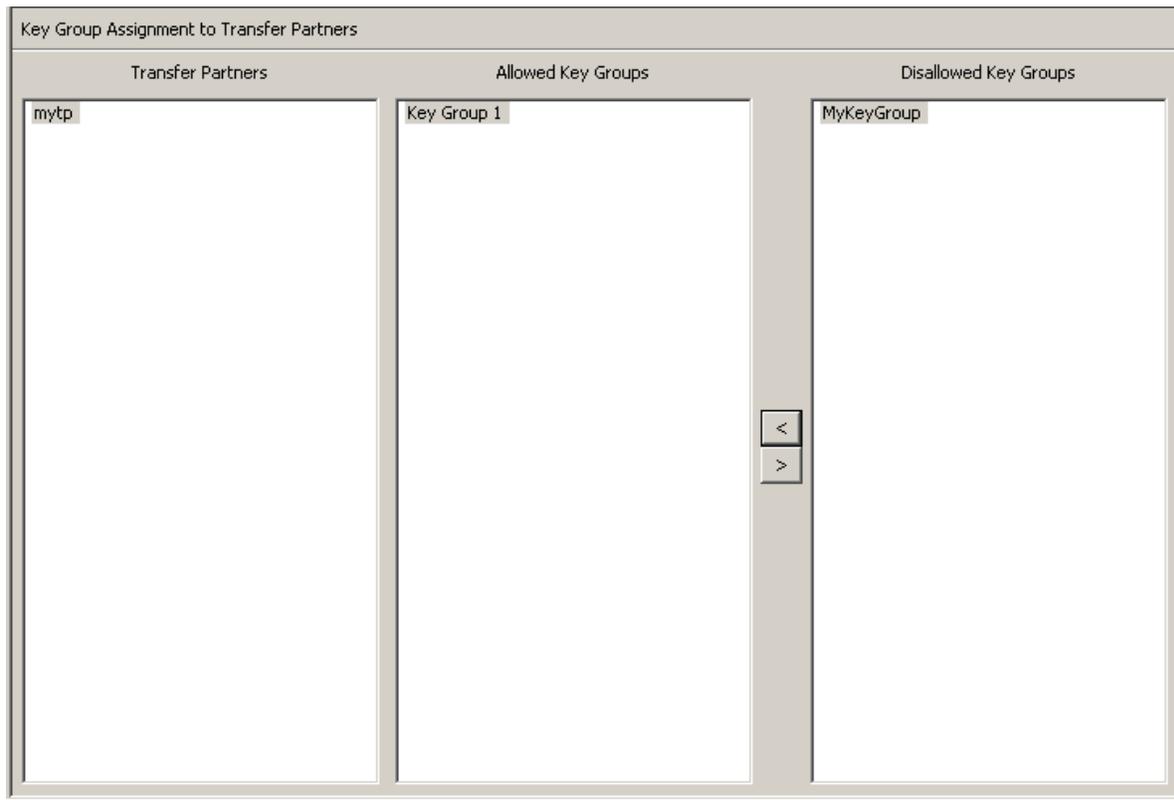


Cet écran affiche les groupes de clés ayant accès à un partenaire de transfert. La colonne Allowed Key Groups (Groupes de clés autorisés) dresse la liste des groupes de clés assignés au partenaire de transfert sélectionné. La colonne Disallowed Key Groups (Groupes de clés non autorisés) affiche les groupes de clés non assignés au partenaire de transfert.

## Ajout d'un groupe de clés à un partenaire de transfert

Pour ajouter un groupe de clés à la liste des partenaires de transfert :

1. Dans la colonne Transfer Partners (Partenaires de transfert), mettez le partenaire concerné en surbrillance. Dans la colonne Disallowed Key Groups (Groupes de clés non autorisés), mettez le groupe à ajouter en surbrillance et cliquez sur le bouton Move to  (Déplacer vers).

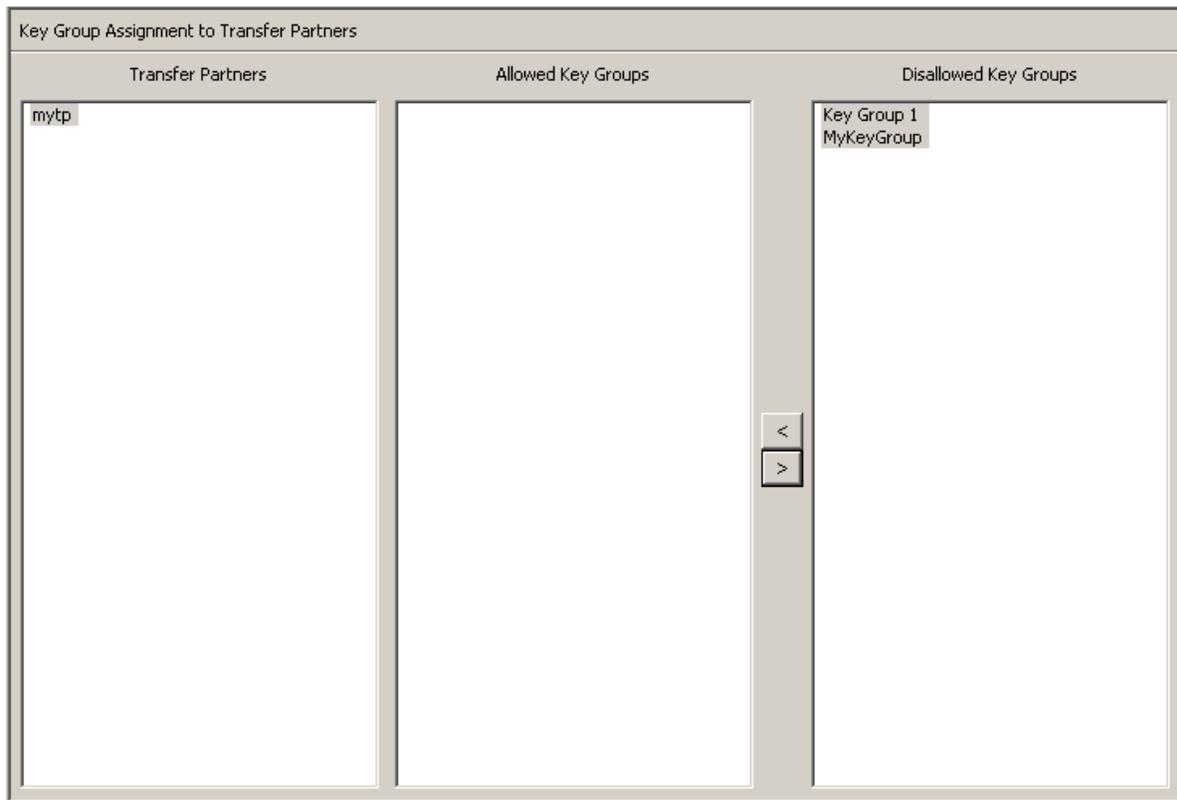


2. Le groupe de clés sélectionné est déplacé vers la colonne Allowed Key Groups (Groupes de clés autorisés), indiquant que le partenaire de transfert peut désormais accéder à ce groupe.

## Suppression d'un groupe de clés d'un partenaire de transfert

Pour supprimer une liste de groupes de clés d'un partenaire de transfert :

1. Dans la colonne Transfer Partners (Partenaires de transfert), mettez le partenaire concerné en surbrillance. Dans la colonne Allowed Key Groups (Groupes de clés autorisés), mettez le groupe à supprimer en surbrillance et cliquez sur le bouton Move from  (Déplacer depuis).



2. Le groupe de clés sélectionné est déplacé vers la colonne Disallowed Key Groups (Groupes de clés non autorisés), indiquant que le partenaire de transfert ne peut plus accéder à ce groupe.

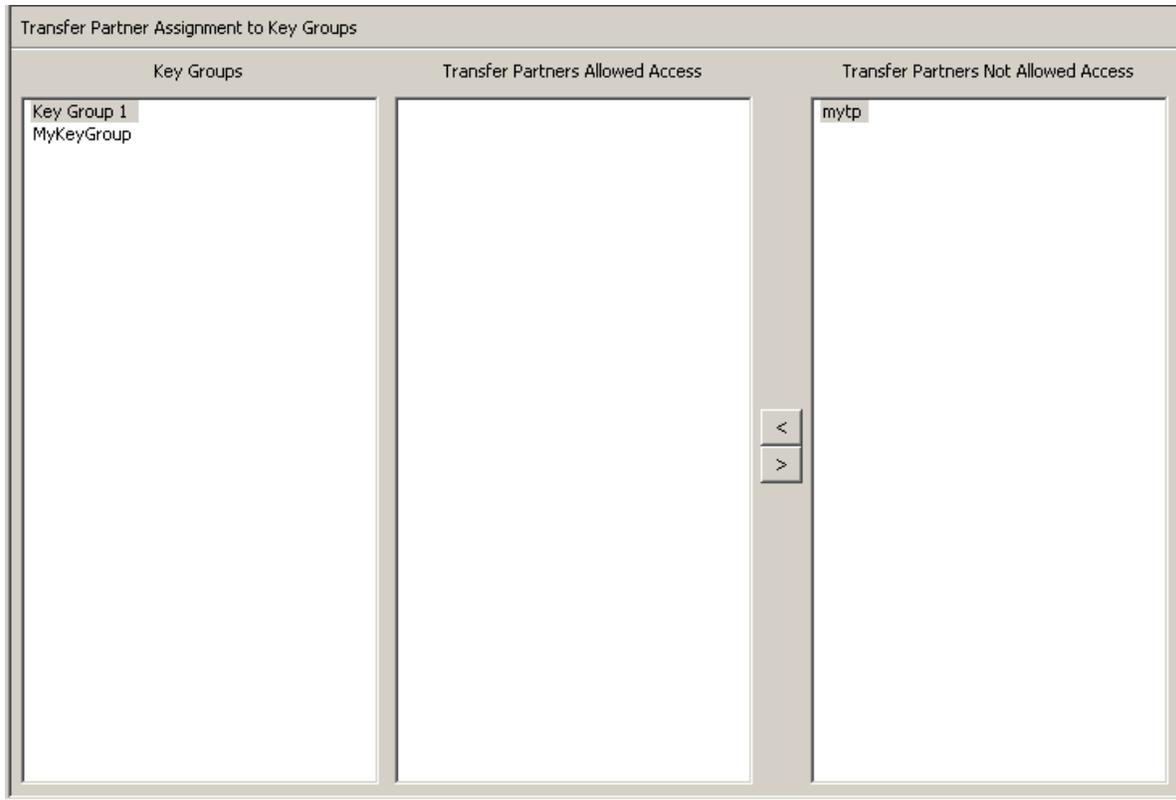
## Menu Transfer Partner Assignment to Key Groups (Assignment d'un partenaire de transfert à des groupes de clés)

Le menu Transfer Partner Assignment to Key Groups (Assignment d'un partenaire de transfert à des groupes de clés) vous permet d'ajouter un partenaire de transfert de clés au jeu de partenaires autorisés à accéder à un groupe de clés particulier.



## Affichage des assignations de groupes de transfert

Pour afficher les assignations de groupes de transfert, dans le menu Key Groups (Groupes de clés), choisissez Transfer Partner Assignment to Key Groups (Assignation d'un partenaire de transfert à des groupes de clés). L'écran suivant s'affiche.

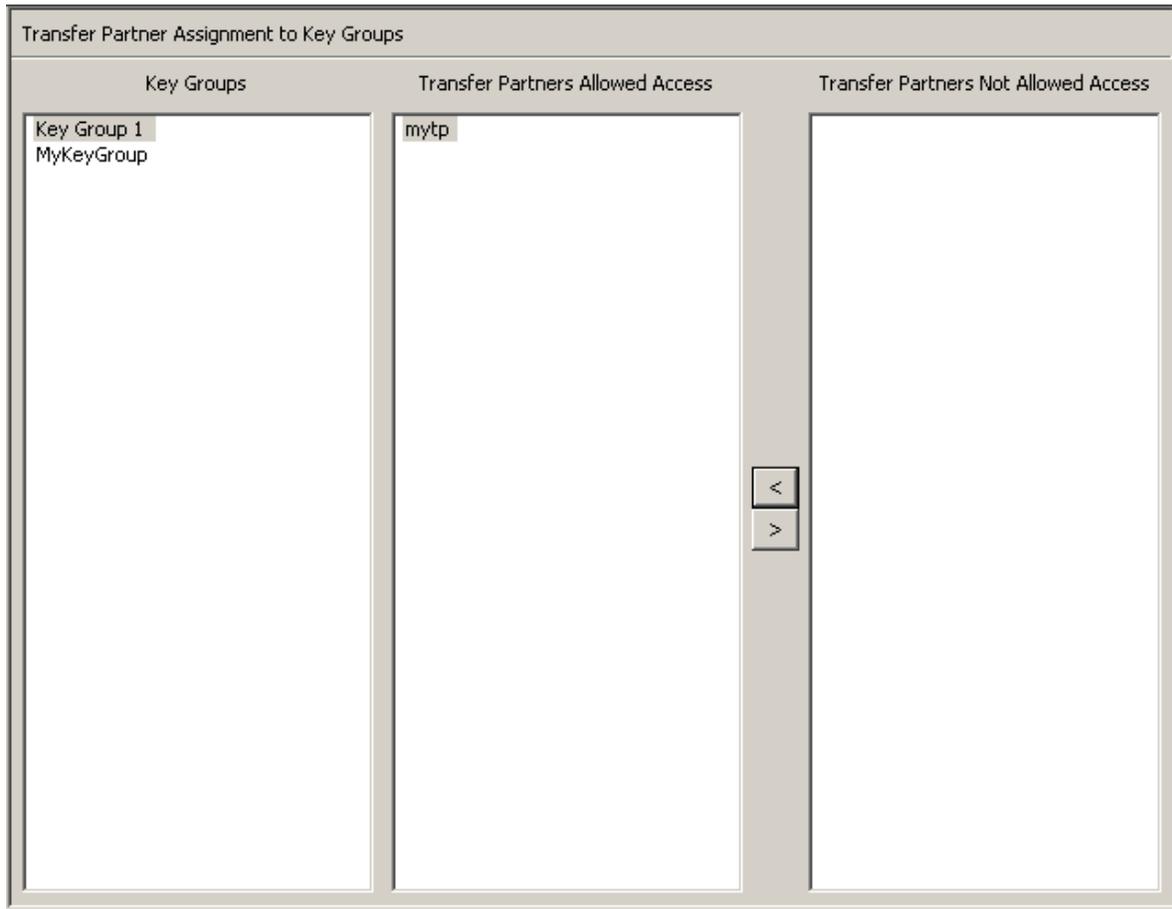


L'écran affiche les partenaires de transfert pouvant accéder à un groupe de clés. La colonne Transfer Partners Allowed Access (Accès autorisé pour les partenaires de transfert) dresse la liste des partenaires de transfert assignés au groupe de clés. La colonne Transfer Partners Not Allowed Access (Accès non autorisé pour les partenaires de transfert) dresse la liste des partenaires de transfert non assignés au groupe de clés.

## Ajout d'un partenaire de transfert à un groupe de clés

Pour ajouter un partenaire de transfert à un groupe de clés :

1. Dans la colonne Key Groups (Groupes de clés), mettez le groupe concerné en surbrillance. Dans la colonne Transfer Partners Allowed Access (Accès autorisé pour les partenaires de transfert), mettez le groupe à ajouter en surbrillance et cliquez sur le bouton Move to  (Déplacer vers).

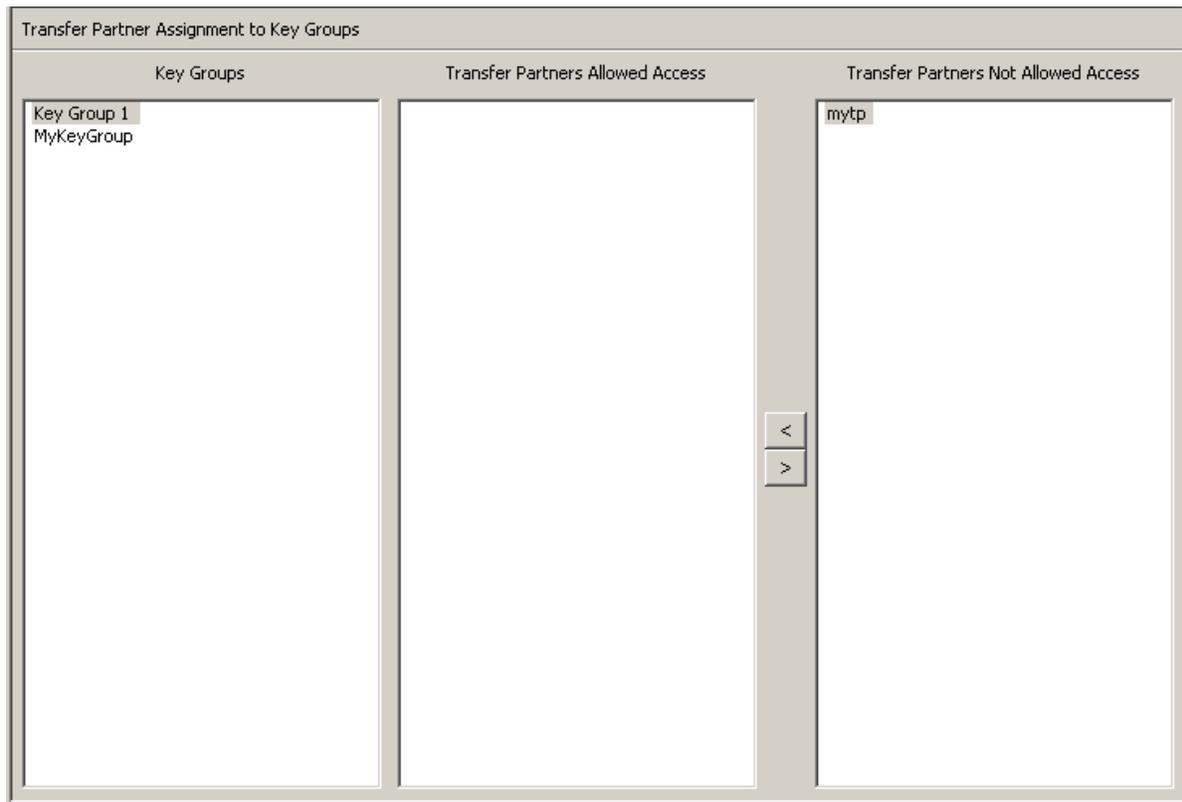


2. Le partenaire de transfert sélectionné est déplacé vers la colonne Transfer Partners Allowed Access, indiquant que le groupe de clés peut désormais accéder à ce partenaire.

## Suppression d'un partenaire de transfert d'un groupe de clés

Pour supprimer un partenaire de transfert d'un groupe de clés :

1. Dans la colonne Key Groups (Groupes de clés), mettez le groupe concerné en surbrillance. Dans la colonne Transfer Partners Allowed Access (Accès autorisé pour les partenaires de transfert), mettez le partenaire à supprimer en surbrillance et cliquez sur le bouton Move from  (Déplacer depuis).

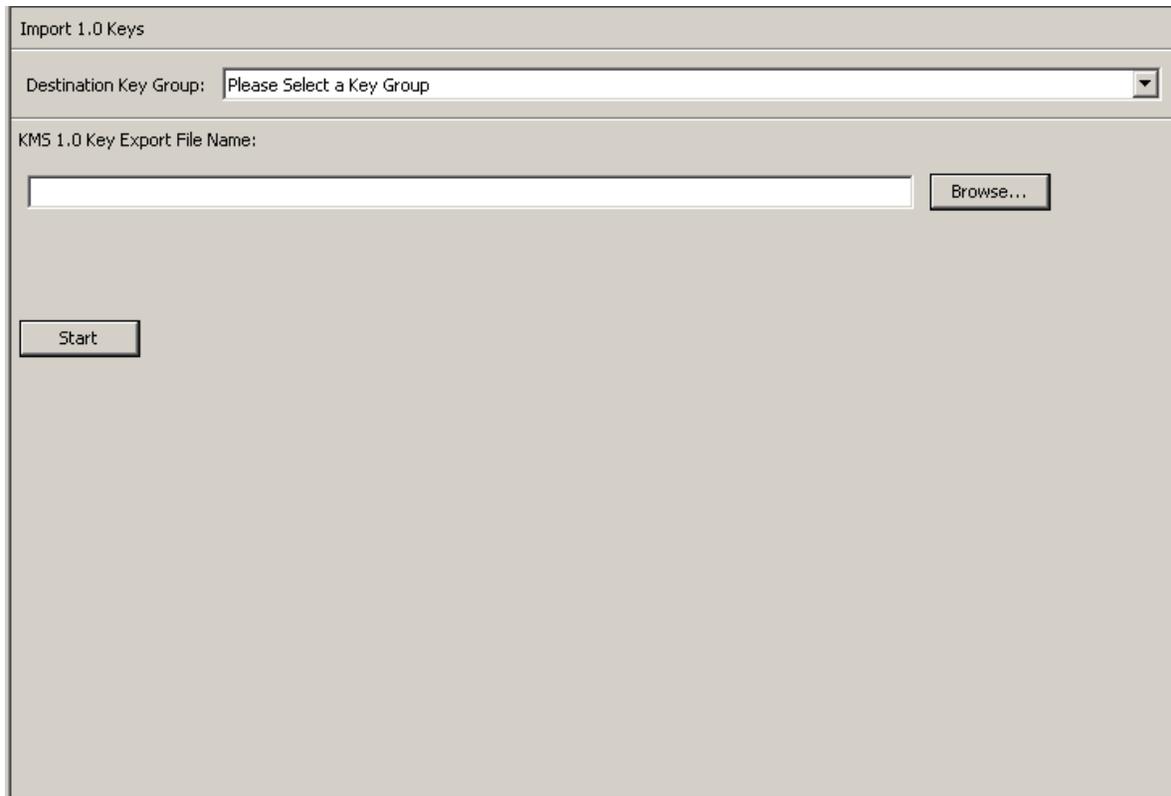


2. Le partenaire de transfert sélectionné est déplacé vers la colonne Transfer Partners Not Allowed Access, indiquant que le groupe de clés ne peut plus accéder à ce partenaire.

## Importation d'un fichier d'exportation de clés KMS 1.0

Pour importer un fichier d'exportation de clés KMS 1.0 vers le KMA et créer une clé pour chaque clé contenue dans le fichier :

1. Accédez au système KMS 1.2 et exportez les clés dans un fichier. Seules les clés exportées à partir de systèmes KMS 1.2 peuvent être importées. Les systèmes KMS 1.0 et 1.1 doivent être mis à niveau vers la version 1.2 avant l'exportation de clés.
2. Dans le menu Secure Information Management (Gestion des informations sécurisées), choisissez **Import 1.0 Keys** (Importer des clés 1.0).



Import 1.0 Keys

Destination Key Group: Please Select a Key Group

KMS 1.0 Key Export File Name:

Browse...

Start

3. Remplissez les champs des paramètres suivants :

**Destination Key Group (Groupe de clés cible)**

Sélectionnez le groupe de clés cible dans lequel ces clés seront importées.

**KMS 1.0 Key Export File Name (Nom du fichier d'exportation de clés KMS 1.0)**

Saisissez le nom du fichier d'exportation de clés KMS 1.0.

**Browse (Parcourir)**

Cliquez sur ce bouton pour localiser le fichier.

**Start (Commencer)**

Cliquez sur ce bouton pour lancer le téléchargement du fichier de clés KMS 1.0 vers le KMA ; une nouvelle clé est créée pour chaque clé du fichier. Chaque nouvelle clé est associée au groupe de clés sélectionné. Des messages vous informent du déroulement du téléchargement et de l'application du fichier.

# Menu Audit Event List (Liste des événements d'audit)

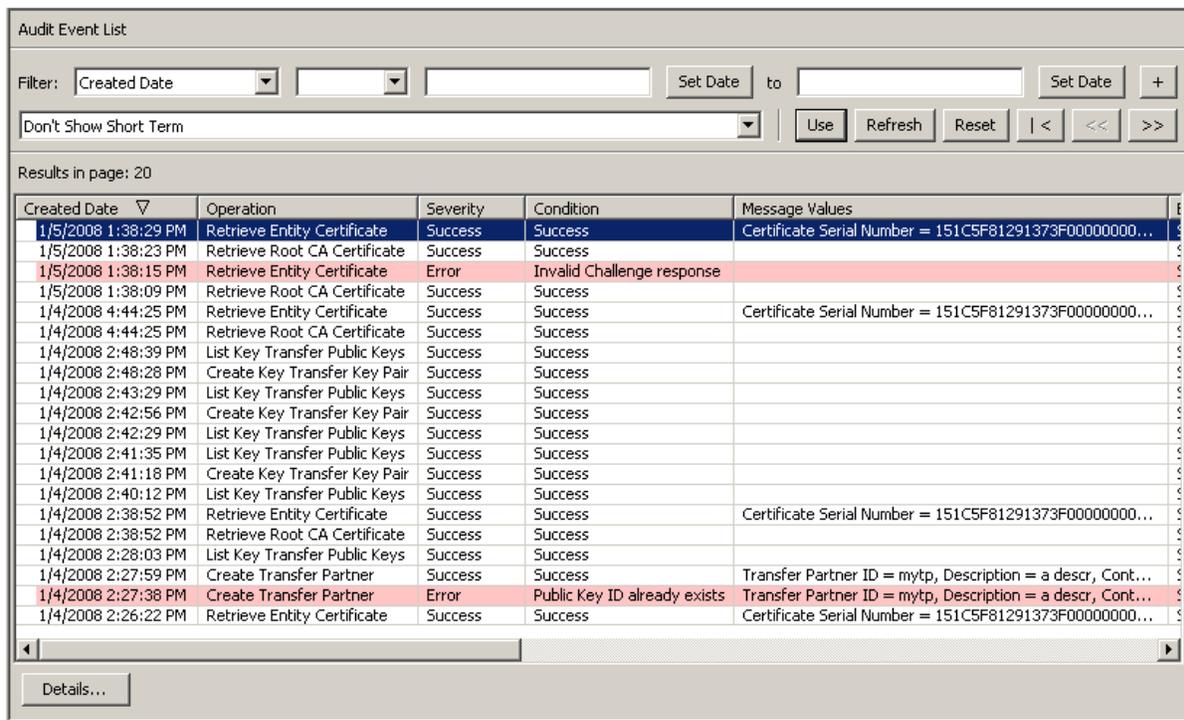
Le menu Audit Event List (Liste des événements d'audit) vous permet de visualiser les événements consignés dans un journal d'audit.



## Affichage des journaux d'audit

Pour afficher les événements d'un journal d'audit :

Dans le menu System Management (Gestion du système), choisissez Audit Event List (Liste des événements d'audit). L'écran Audit Event List (Liste des événements d'audit) s'affiche.



The screenshot shows the 'Audit Event List' application window. It features a filter section at the top with a dropdown menu set to 'Created Date', a 'Set Date' button, and a 'to' field. Below the filter is a 'Don't Show Short Term' checkbox and a 'Use' button. There are also 'Refresh', 'Reset', and navigation buttons ('<', '<<', '>>'). The main area displays a table of results, with 'Results in page: 20' indicated above it. The table has columns for 'Created Date', 'Operation', 'Severity', 'Condition', and 'Message Values'. The data includes various operations like 'Retrieve Entity Certificate', 'Retrieve Root CA Certificate', and 'List Key Transfer Public Keys', with statuses ranging from 'Success' to 'Error'.

Created Date	Operation	Severity	Condition	Message Values
1/5/2008 1:38:29 PM	Retrieve Entity Certificate	Success	Success	Certificate Serial Number = 151C5F81291373F00000000...
1/5/2008 1:38:23 PM	Retrieve Root CA Certificate	Success	Success	
1/5/2008 1:38:15 PM	Retrieve Entity Certificate	Error	Invalid Challenge response	
1/5/2008 1:38:09 PM	Retrieve Root CA Certificate	Success	Success	
1/4/2008 4:44:25 PM	Retrieve Entity Certificate	Success	Success	Certificate Serial Number = 151C5F81291373F00000000...
1/4/2008 4:44:25 PM	Retrieve Root CA Certificate	Success	Success	
1/4/2008 2:48:39 PM	List Key Transfer Public Keys	Success	Success	
1/4/2008 2:48:28 PM	Create Key Transfer Key Pair	Success	Success	
1/4/2008 2:43:29 PM	List Key Transfer Public Keys	Success	Success	
1/4/2008 2:42:56 PM	Create Key Transfer Key Pair	Success	Success	
1/4/2008 2:42:29 PM	List Key Transfer Public Keys	Success	Success	
1/4/2008 2:41:35 PM	List Key Transfer Public Keys	Success	Success	
1/4/2008 2:41:18 PM	Create Key Transfer Key Pair	Success	Success	
1/4/2008 2:40:12 PM	List Key Transfer Public Keys	Success	Success	
1/4/2008 2:38:52 PM	Retrieve Entity Certificate	Success	Success	Certificate Serial Number = 151C5F81291373F00000000...
1/4/2008 2:38:52 PM	Retrieve Root CA Certificate	Success	Success	
1/4/2008 2:28:03 PM	List Key Transfer Public Keys	Success	Success	
1/4/2008 2:27:59 PM	Create Transfer Partner	Success	Success	Transfer Partner ID = mytp, Description = a descr, Cont...
1/4/2008 2:27:38 PM	Create Transfer Partner	Error	Public Key ID already exists	Transfer Partner ID = mytp, Description = a descr, Cont...
1/4/2008 2:26:22 PM	Retrieve Entity Certificate	Success	Success	Certificate Serial Number = 151C5F81291373F00000000...

Vous pouvez également faire défiler la base de données et filtrer la liste des événements d'audit selon l'un des critères suivants :

- Created Date (Date de création)
- Operation (Opération)
- Severity (Gravité)
- Condition
- Entity ID (ID de l'entité)
- Entity Network Address (Adresse réseau de l'entité)
- KMA ID (ID du KMA)
- KMA Name (Nom du KMA)
- Class (Classe)
- Retention Term (Durée de conservation)
- Audit Log ID (ID du journal d'audit)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour le journal d'audit.

Les champs et leur description sont fournis ci-dessous :

#### **Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Created Date (Date de création)
- Operation (Opération)
- Severity (Gravité)
- Condition
- Entity ID (ID de l'entité)
- Entity Network Address (Adresse réseau de l'entité)
- KMA Name (Nom du KMA)
- Class (Classe)
- Retention Term (Durée de conservation)
- Audit Log ID (Journal d'audit ID)

#### **Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Vide
- Non vide

#### **Zone Filter Value 1 (Valeur de filtre 1)**

Si vous avez sélectionné le filtre de date, cliquez sur Set Date (Définir la date) afin de spécifier la date et l'heure de départ. La valeur s'affiche comme valeur de départ de la plage des clés de filtrage. Si vous avez sélectionné n'importe quel autre filtre, saisissez une valeur dans ce champ.

#### **Zone Filter Value 2 (Valeur de filtre 2)**

Si vous avez sélectionné le filtre de date, cliquez sur Set Date (Définir la date) afin de sélectionner une date et une heure de fin. La valeur s'affiche comme valeur de fin de la plage de clés de filtrage.

### **Zone Filter Value 3 (Valeur de filtre 3)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'un des filtres suivants :

- Don't Show Short Term (Ne pas afficher le court terme)
- Show All Retentions (Afficher toutes les durées de conservation)

### **Created Date (Date de création)**

Affiche les date et heure de création de l'événement d'audit.

### **Operation (Opération)**

Affiche l'opération ayant entraîné la création de l'enregistrement dans le journal d'audit.

### **Severity (Gravité)**

Indique le niveau de gravité de la condition si l'opération a échoué. Les valeurs possibles sont Success (no error) (Réussite sans erreur), Warning, (Avertissement) et Error (Erreur).

### **Condition**

Indique si l'opération s'est bien ou mal déroulée.

---

**Remarque** – Les erreurs sont signalées en rouge et les avertissements en jaune. Si vous immobilisez le curseur sur un message d'erreur, une description détaillée de l'erreur s'affiche.

---

### **Event Message (Message de l'événement)**

Affiche des informations détaillées sur l'entrée de l'événement d'audit.

### **Entity ID (ID de l'entité)**

Affiche le nom de l'utilisateur ayant effectué l'opération.

### **Entity Network Address (Adresse réseau de l'entité)**

Affiche l'adresse réseau de l'entité ayant généré l'événement d'audit.

### **KMA ID (ID du KMA)**

Affiche le dispositif à l'origine de l'entrée de l'événement d'audit.

### **KMA Name (Nom du KMA)**

Affiche l'identificateur fourni par l'utilisateur qui permet de différencier les dispositifs d'un cluster.

### **Class (Classe)**

Identifie la classe des opérations à laquelle l'entrée de l'événement d'audit appartient. Les valeurs possibles sont les suivantes :

- Agent Access Control Management Operations (Opérations de gestion du contrôle d'accès des agents)
- Agent Client Generated Audits (Audits des agents générés par le client)
- Agent Management Operations (Opérations de gestion des agents)
- Appliance Management Operations (Opérations de gestion des dispositifs)
- Audit Log Agent Operations (Opérations agent relatives aux journaux d'audit)
- Audit Log Management Operations (Opérations de gestion des journaux d'audit)
- Audit Log Operations (Opérations relatives aux journaux d'audit)

- Backup Management Operations (Opérations de gestion des sauvegardes)
- CA Operations (Opérations AC)
- Cluster Client Communication (Communication des clients du cluster)
- Cluster Operations (Opérations relatives aux clusters)
- Communication and Authentication (Communication et authentification)
- Console Security Management Operations (Opérations de gestion de la sécurité de la console)
- Data Unit Agent Operations (Opérations agent relatives aux unités de données)
- Data Unit Management Operations (Opérations de gestion des unités de données)
- Discovery Operations (Opérations de découverte)
- Key Group Agent Operations (Opérations agent relatives aux groupes de clés)
- Key Group Management Operations (Opérations de gestion des groupes de clés)
- Key Policy Management Operations (Opérations de gestion des stratégies de clés)
- License Key Management Operations (Opérations de gestion des clés de licence)
- Local Management Operations (Opérations de gestion locales)
- Management Client Generated Audits (Audits de gestion générés par le client)
- Passphrase Agent Operations (Opérations agent relatives aux phrases de passe)
- Replication Operations (Opérations de réplication)
- Retrieve Certificate Operations (Opération de récupération de certificats)
- Role Management Operations (Opérations de gestion des rôles)
- SNMP Management Operations (Opérations de gestion SNMP)
- Security Management Operations (Opérations de gestion de la sécurité)
- Security Parameter Management Operations (Opérations de gestion des paramètres de sécurité)
- Security Violation (Violation de la sécurité)
- Site Management Operations (Opérations de gestion du site)
- System Messages (Messages système)
- User Management Operations (Opérations de gestion des utilisateurs)

#### **Retention Term (Durée de conservation)**

Affiche le laps de temps défini pendant lequel l'enregistrement de l'événement d'audit est conservé. Les valeurs possibles sont décrites ci-après :

##### **Long Term (Long terme)**

Les enregistrements des événements doivent être stockés pendant une longue période.

##### **Medium Term (Moyen terme)**

Les enregistrements des événements doivent être stockés pendant une période moyenne.

##### **Short Term (Court terme)**

Les enregistrements des événements doivent être stockés pendant une courte période.

#### **Audit Log Entry ID (ID de l'entrée du journal d'audit)**

Affiche un identificateur unique généré par le système permettant de différencier les différents types d'entrées du journal d'audit.

**Audit Log ID (Journal d'audit ID)**

Affiche un identificateur unique généré par le système permettant de différencier les différentes entrées du journal d'audit.

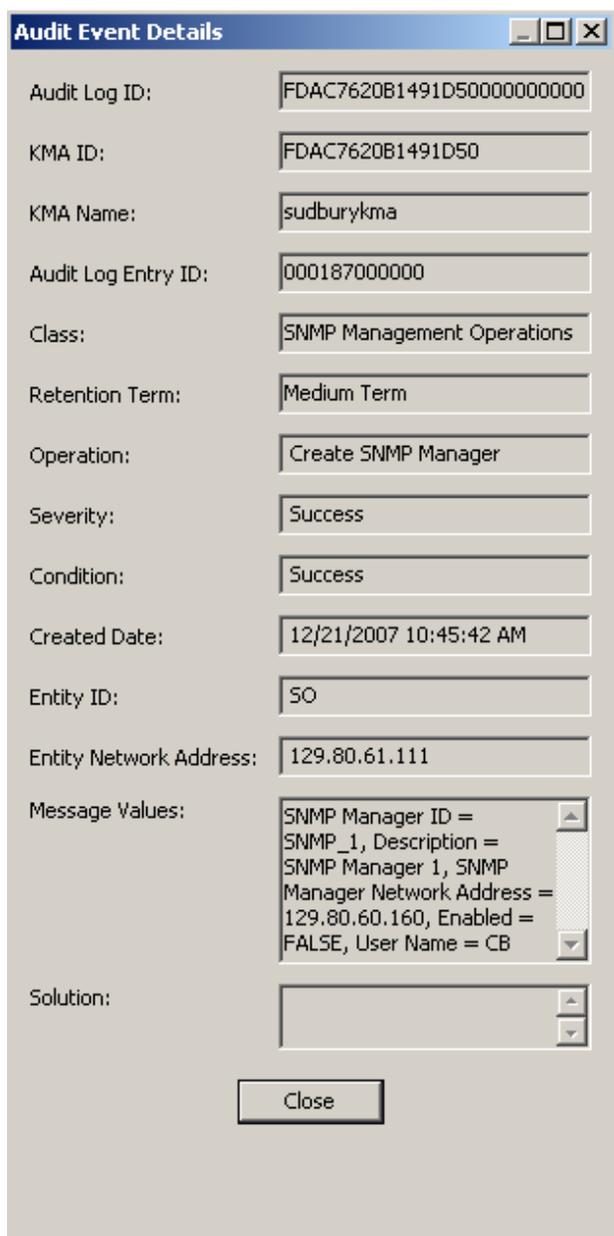
Pour plus d'informations sur un journal d'audit, mettez celui qui vous intéresse en surbrillance et cliquez sur le bouton **Details (Détails)**. Pour plus d'informations, reportez-vous à la section « [Affichage des détails du journal d'audit](#) » ci-dessous.

Cliquez sur le bouton **Export (Exporter)** afin d'exporter le journal d'audit. Pour plus d'informations, reportez-vous à la section « [Exportation d'un journal d'audit](#) », page 222.

## Affichage des détails du journal d'audit

Pour afficher les détails du journal d'audit :

1. Dans l'écran Audit Event List (Liste des événements d'audit), sélectionnez l'entrée de journal d'audit qui vous intéresse et cliquez sur le bouton Détails (Détails) ou double-cliquez sur l'entrée. L'écran Audit Event Details (Détails de l'événement d'audit) s'affiche, tous les champs étant désactivés à l'exception du bouton Close (Fermer).



The screenshot shows a window titled "Audit Event Details" with the following fields and values:

Audit Log ID:	FDAC7620B1491D500000000000
KMA ID:	FDAC7620B1491D50
KMA Name:	sudburykma
Audit Log Entry ID:	000187000000
Class:	SNMP Management Operations
Retention Term:	Medium Term
Operation:	Create SNMP Manager
Severity:	Success
Condition:	Success
Created Date:	12/21/2007 10:45:42 AM
Entity ID:	50
Entity Network Address:	129.80.61.111
Message Values:	SNMP Manager ID = SNMP_1, Description = SNMP Manager 1, SNMP Manager Network Address = 129.80.60.160, Enabled = FALSE, User Name = CB
Solution:	

Close

2. Cliquez sur Close pour revenir à l'écran Audit Event List (Liste des événements d'audit).

## Exportation d'un journal d'audit

La fonction d'exportation permet à l'utilisateur d'exporter une partie ou la totalité des entrées du journal d'audit dans un fichier texte situé sur sa station de travail.

L'utilisateur peut ensuite ouvrir le fichier dans un tableur.

Pour exporter un journal d'audit :

1. Dans l'écran Audit Event List (Liste des événements d'audit), choisissez `Save Report` (Enregistrer le rapport) dans le menu `View` (Affichage) ou appuyez sur les touches `Ctrl+S`.
2. Cela fait, cliquez sur le bouton `Start` (Commencer) afin de lancer le processus d'exportation. Si vous avez filtré les entrées affichées dans l'écran Audit Event List (Liste des événements d'audit), seules les entrées visibles sont exportées. Sinon, tous les événements d'audit sont inclus dans l'opération.
3. Une fois le processus d'exportation terminé, le nombre de journaux d'audit exportés est indiqué en bas de la boîte de dialogue.
4. Cliquez sur le bouton `Close` (Fermer) pour fermer cette boîte de dialogue et revenir à l'écran Audit Event List (Liste des événements d'audit).

---

## Menu Data Units (Unités de données)

Pour connaître les procédures d'utilisation de ce menu, reportez-vous à la section « [Menu Data Unit List \(Liste des unités de données\)](#) », page 240.

## Autres fonctions

Un responsable de la conformité est également habilité à effectuer les opérations suivantes :

- Affichage de la liste des événements d'audit
- Affichage de l'heure système
- Verrouillage/Déverrouillage du statut du KMA

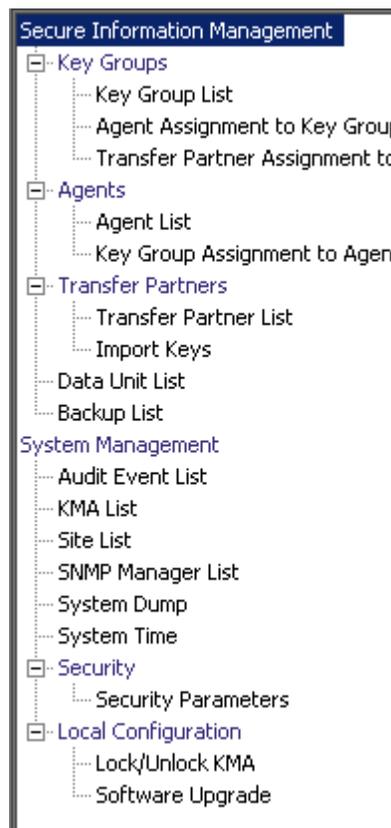
Pour connaître les procédures de visualisation de ces fonctions, reportez-vous à la section [chapitre 5, « Tâches du responsable de la sécurité »](#).

## Tâches de l'opérateur

Ce chapitre décrit les opérations pouvant être effectuées par un utilisateur doté du rôle Operator (Opérateur). Si plusieurs rôles vous ont été assignés, reportez-vous au chapitre pertinent pour des instructions sur les tâches associées à chaque rôle.

### Rôle Operator (Opérateur)

En tant qu'opérateur, vous êtes chargé de gérer les opérations quotidiennes relatives au système.



## Menu Key Groups (Groupes de clés)

Le menu Key Groups (Groupes de clés) propose les options suivantes.



Il vous permet d'effectuer les opérations suivantes :

- Affichage de la liste des groupes de clés
- Affichage des assignations d'agents à des groupes de clés
- Affichage des assignations de partenaires de transfert à des groupes de clés

### Key Group List (Liste des groupes de clés)

L'option de menu Key Group List (Liste des groupes de clés) permet à l'utilisateur de gérer vos groupes de clés. Pour plus d'informations à ce sujet, reportez-vous à la section « [Menu Key Group List \(Liste des groupes de clés\)](#) », page 186.

### Agent Assignment to Key Groups (Assignation d'un agent à des groupes de clés)

L'option de menu Agent Assignment to Key Groups (Assignation d'un agent à des groupes de clés) permet à l'utilisateur de visualiser les agents assignés à des groupes de clés. Pour plus d'informations à ce sujet, reportez-vous à la section « [Menu Agent Assignment to Key Groups \(Assignation d'un agent à des groupes de clés\)](#) », page 194.

### Transfer Partner Assignment to Key Groups (Assignation d'un partenaire de transfert à des groupes de clés)

L'option Transfer Partner Assignment to Key Groups (Assignation d'un partenaire de transfert à des groupes de clés) permet à l'utilisateur d'afficher l'assignation d'un partenaire de transfert de clés au jeu de partenaires autorisés à accéder à un groupe de clés particulier. Pour plus d'informations à ce sujet, reportez-vous à la section « [Menu Transfer Partner Assignment to Key Groups \(Assignation d'un partenaire de transfert à des groupes de clés\)](#) », page 211.

## Menu Agent List (Liste des agents)

L'option de menu Agent List (Liste des agents) vous permet d'effectuer les opérations suivantes :

- Affichage des agents
- Création d'un agent
- Affichage/Modification d'un agent
- Suppression d'un agent existant



## Affichage de la liste des agents

L'option de menu Agent List (Liste des agents) permet à l'utilisateur d'afficher tous les agents associés à un groupe de clés spécifique.

Pour afficher cet écran :

1. Dans le menu Agents, choisissez **Agent List** (Liste des agents). L'écran Agent List (Liste des agents) s'affiche.
2. Cliquez sur la flèche pointant vers le bas en regard du champ Key Group (Groupe de clés) et sélectionnez un groupe de clés. Les agents associés à ce groupe s'affichent à l'écran.

Agent List

Filter: Agent ID =

Key Group 1 Use Refresh Reset | < << >>

Results in page: 3 (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
SO-owned Agent	agent for testing.	Toronto		True	0	False

Details... Create... Delete Activity History...

Vous pouvez également faire défiler la base de données et filtrer les listes d'agents selon l'un des critères suivants :

- Agent ID (ID de l'agent)
- Description
- Site
- Default Key Group (Groupe de clés par défaut)
- Enabled (Activé)
- Failed Login Attempts (Tentatives de connexion ayant échoué)
- Enrolled (Inscrit)

Le bouton **Use** (Utiliser) applique le filtre à la liste affichée pour l'agent.

Les champs et leur description sont fournis ci-dessous :

#### **Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Agent ID (ID de l'agent)
- Description
- Site
- Default Key Group (Groupe de clés par défaut)
- Enabled (Activé)
- Failed Login Attempts (Tentatives de connexion ayant échoué)
- Enrolled (Inscrit)

#### **Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

#### **Zone de texte Filter Value (Valeur de filtre)**

Indiquez la valeur selon laquelle l'attribut sélectionné doit être trié. Cette option de filtrage est masquée pour certains attributs.

#### **Boîte combinée Filter Value (Valeur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez la valeur selon laquelle l'attribut sélectionné doit être filtré. Cette option de filtrage est masquée pour certains attributs.



Cliquez sur ce bouton pour ajouter d'autres filtres.



Cliquez sur ce bouton pour supprimer un filtre. Ce bouton est visible uniquement si plusieurs filtres sont affichés.

#### **Show Agents in any Key Group (Afficher les agents de tous les groupes)**

Option permettant de filtrer les agents selon leur association à des groupes de clés spécifiques ; seuls les agents liés à ce groupe de clés sont visibles. Cliquez sur la flèche pointant vers le bas et sélectionnez un groupe de clés de filtrage.

#### **Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer les filtres sélectionnés à la liste affichée et atteindre la première page.

#### **Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

**Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**Agent ID (ID de l'agent)**

Affiche l'identificateur unique spécifié par l'utilisateur qui permet de différencier les agents les uns des autres.

**Description**

Donne une description de l'agent.

**Site**

Affiche un identificateur unique indiquant le site auquel l'agent appartient.

**Default Key Group (Groupe de clés par défaut)**

Groupe de clés associé à toutes les clés créées par cet agent lorsque ce dernier n'en définit pas un autre de manière explicite.

**Enabled (Activé)**

Indique le statut de l'agent. Les valeurs possibles sont True (Vrai) ou False (Faux). Si ce champ est défini sur False (Faux), l'agent ne peut pas établir de session avec le KMA.

**Failed Login Attempts (Tentatives de connexion ayant échoué)**

Affiche le nombre de tentatives de connexions ayant échoué.

**Enrolled (Inscrit)**

Indique si l'agent est bien inscrit auprès du cluster KMS. Les valeurs possibles sont True (Vrai) ou False (Faux). Ce champ est défini sur False (Faux) s'il s'agit du premier agent créé ou si la phrase de passe a été modifiée.

## Création d'un agent

Pour créer un agent :

1. Dans l'écran Agents List (Liste des agents), cliquez sur le bouton Create (Créer).  
L'écran Create Agent (Création d'un agent) s'affiche avec l'onglet General (Général) activé.

2. Remplissez les champs des paramètres suivants :

### Agent ID (ID de l'agent)

Saisissez une valeur permettant d'identifier l'agent de manière unique. Cette valeur doit comprendre entre 1 et 64 caractères.

### Description

Saisissez une valeur décrivant l'agent. Cette valeur doit comprendre entre 1 et 64 caractères.

### Site ID (ID du site)

Cliquez sur la flèche pointant vers le bas et mettez en surbrillance le site auquel l'agent appartient. Ce champ est facultatif.

3. Activez l'onglet Passphrase (Phrase de passe).

4. Remplissez les champs des paramètres suivants :

**Enter Passphrase (Saisissez la phrase de passe)**

Tapez la phrase de passe associée à cet utilisateur. La phrase de passe doit contenir entre 8 et 64 caractères. Le nombre de caractère par défaut est 8.

Conditions requises pour les phrases de passe :

- Une phrase de passe ne doit pas contenir l'ID de l'agent de l'utilisateur.
- Une phrase de passe doit contenir trois des quatre classes de caractères : majuscule, minuscule, nombre ou caractère spécial.

Les caractères spéciaux suivants sont autorisés :

' ~ ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } \ | ; : ' " < > , . / ?

- Les caractères de contrôle, tabulations et sauts de ligne compris, ne sont pas admis.

---

**Remarque** – Pour modifier la longueur minimale requise des phrases de passe, reportez-vous à la section « [Modification des paramètres de sécurité](#) », page 154.

---

**Confirm Passphrase (Confirmer la phrase de passe)**

Saisissez la même valeur que celle indiquée dans le champ de la phrase de passe.

Un exemple d'écran de création d'agent rempli est présenté ci-dessous.



5. Cliquez sur le bouton Save (Enregistrer). L'enregistrement de l'agent est ajouté à la base de données et affiché dans l'écran Agent List (Liste des agents).

6. Effectuez la procédure d'inscription spécifique à l'agent au moyen de l'interface prévue à cet effet. Par exemple, pour les lecteurs Sun, utilisez le panneau VOP (Virtual Operator Panel, panneau d'opérateur virtuel) afin d'effectuer cette procédure.

Agent List

Filter: Agent ID =  +

Key Group 1 Use Refresh Reset | < << >>

Results in page: 4 (last page)

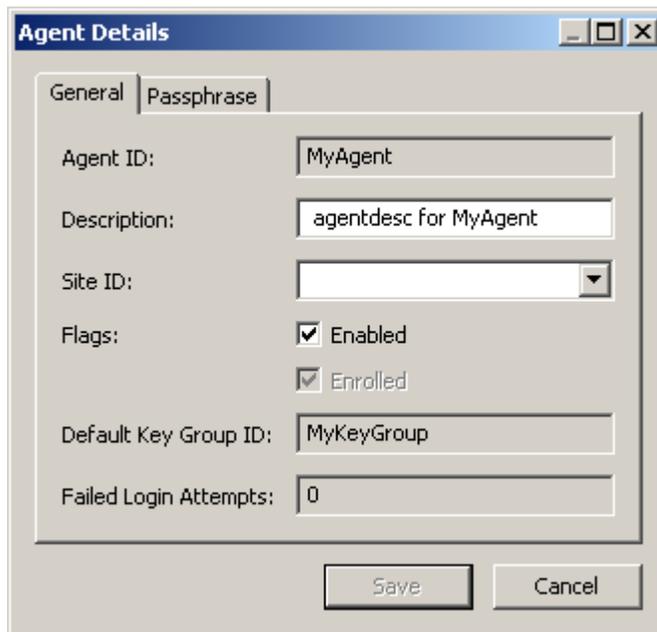
Agent ID 	Description	Site	Default Key Group	Enabled	Failed Login Attempts	Enrolled
MyAgent	agentdesc for MyAgent		MyKeyGroup	True	0	True
MyAgent1	agentdesc for MyAgent		MyKeyGroup	True	0	False
MyAgent2	agentdesc for MyAgent	Louis...		True	0	False
SO-owned Agent	agent for testing.	Toronto		True	0	False

Details... Create... Delete Activity History...

## Affichage/Modification d'un agent

Pour modifier les détails d'un agent :

1. Dans l'écran Agents List (Liste des agents), double-cliquez sur l'entrée d'un agent pour lequel vous souhaitez obtenir des informations détaillées ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). L'écran Agent Details (Détails de l'agent) s'affiche.



The screenshot shows a window titled "Agent Details" with two tabs: "General" and "Passphrase". The "General" tab is selected. The form contains the following fields and controls:

- Agent ID: Text box containing "MyAgent"
- Description: Text box containing "agentdesc for MyAgent"
- Site ID: Dropdown menu (empty)
- Flags: Two checked checkboxes labeled "Enabled" and "Enrolled"
- Default Key Group ID: Text box containing "MyKeyGroup"
- Failed Login Attempts: Text box containing "0"
- Buttons: "Save" and "Cancel" at the bottom right.

2. Ouvrez l'onglet General (Général) et modifiez les champs suivants, selon vos besoins :
  - Description
  - Site ID (ID du site)
  - Flags - Enabled (Indicateurs - Activés)

---

**Remarque** – Modifiez la phrase de passe de l'agent uniquement si vous pensez qu'elle a été compromise. Pour plus d'informations à ce sujet, reportez-vous à la section « Définition de la phrase de passe d'un agent », page 235.

---

3. Lorsque vous avez terminé, cliquez sur le bouton Save (Enregistrer). Les modifications sont apportées à la base de données de KMS Manager et vous revenez à l'écran Agents List (Liste des agents).

## Définition de la phrase de passe d'un agent

Lorsque vous définissez la phrase de passe d'un agent, vous révoquez le certificat de l'agent qui permettait à celui-ci de s'authentifier auprès du KMA. En tant qu'opérateur, vous pouvez définir le certificat par phrase de passe d'un agent si vous pensez que le certificat et/ou la phrase de passe ont été compromis.

Pour définir la phrase de passe d'un agent :

1. Dans l'écran Agents List (Liste des agents), double-cliquez sur l'entrée de l'agent dont vous souhaitez définir la phrase de passe ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). L'écran Agent·Details·(Détails de l'agent) s'affiche. Activez l'onglet Passphrase (Phrase de passe).

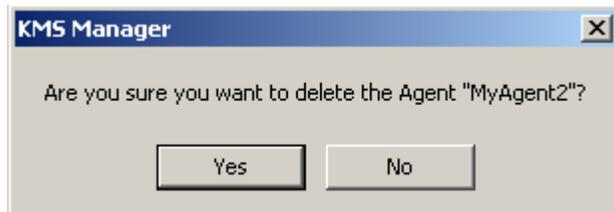
The image shows a dialog box titled "Agent Details" with a blue header bar. Below the header, there are two tabs: "General" and "Passphrase". The "Passphrase" tab is selected. Inside the dialog, there are two text input fields. The first is labeled "Enter Passphrase:" and the second is labeled "Confirm Passphrase:". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

2. Modifiez les champs suivants, puis cliquez sur le bouton Save (Enregistrer).
  - Enter Passphrase (Saisissez la phrase de passe)
  - Confirm Passphrase (Confirmer la phrase de passe)
3. Les modifications sont apportées à la base de données et vous revenez à l'écran Agents List (Liste des agents).
4. Inscrivez à nouveau l'agent en suivant la procédure correspondante. Par exemple, pour les lecteurs de bande Sun, utilisez le panneau VOP pour réinscrire l'agent auprès du cluster KMS. Une fois la phrase de passe d'un agent modifiée, celui-ci ne peut plus émettre de requête auprès du cluster KMS tant qu'il n'est pas réinscrit.

## Suppression d'un agent

Pour supprimer un agent :

1. Dans l'écran Agents List (Liste des agents), mettez l'agent à supprimer en surbrillance. La boîte de dialogue suivante s'affiche, vous demandant de confirmer la suppression de l'agent sélectionné.



2. Cliquez sur Yes (Oui) pour supprimer l'agent. L'agent est supprimé de la base de données et vous revenez à l'écran Agents List (Liste des agents), où l'agent ne figure plus.

## Menu Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent)

L'option de menu Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent) vous permet d'afficher les groupes de clés assignés à un agent. Pour plus d'informations à ce sujet, reportez-vous à la section « [Menu Key Group Assignment to Agents \(Assignment d'un groupe de clés à un agent\)](#) », page 200.



## Menu Import Keys (Importer des clés)

Cette option de menu permet d'importer des clés et des unités de données dans un cluster KMS. Les informations sur les clés et les unités de données sont contenues dans un fichier de transfert de clés envoyé par un partenaire de transfert.

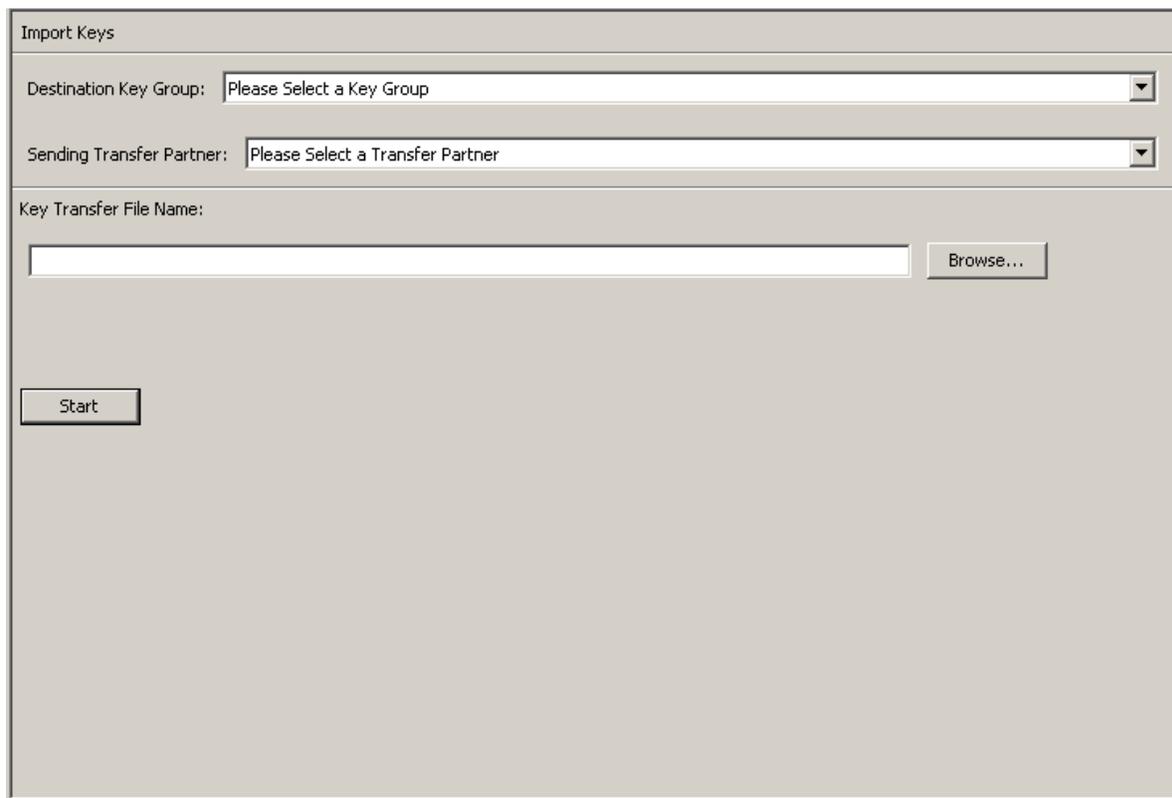
---

**Remarque** – Cet écran vous permet de télécharger et d'importer des clés vers le cluster KMS. Ces clés sont exportées à partir d'un autre cluster KMS.

---

Pour importer des clés :

1. Dans le menu Transfer Partners (Partenaires de transfert), choisissez Import Keys (Importer des clés). L'écran Import Keys (Importer des clés) s'affiche.



Import Keys

Destination Key Group: Please Select a Key Group

Sending Transfer Partner: Please Select a Transfer Partner

Key Transfer File Name:

Browse...

Start

2. Remplissez les champs des paramètres suivants :

**Destination Key Group (Groupe de clés cible)**

Sélectionnez le groupe de clés cible dans lequel ces clés seront importées.

L'indicateur Allow Imports (Autoriser les importations) doit être coché en regard de la stratégie de clés s'appliquant à ce groupe de clés. Il doit s'agir d'un groupe de clés autorisé pour le partenaire de transfert expéditeur sélectionné.

**Sending Transfer Partner (Partenaire de transfert expéditeur)**

Sélectionnez le partenaire de transfert ayant exporté ces clés.

**Key Transfer File (Fichier de transfert de clés)**

Saisissez le nom du fichier de transfert de clés. Une autre solution consiste à cliquer sur le bouton Browse (Parcourir) afin de sélectionner un chemin de destination.

3. Cliquez sur le bouton Start (Commencer) pour lancer le téléchargement et le processus d'importation des clés. Des messages vous informent du déroulement du téléchargement et de l'application du fichier.

---

## Unités de données

Les unités de données sont des périphériques de stockage logique, tels que des disques, des bandes ou des objets. Elles sont sécurisées par des stratégies de clés valides associées à leurs groupes de clés. Un agent doit avoir accès à l'unité de données sélectionnée.

---

**Remarque** – Un opérateur est habilité à effectuer toutes les fonctions, à l'exception de la modification du groupe de clés d'une unité de données. Seul un responsable de la conformité peut effectuer cette opération.

---

### Menu Data Unit List (Liste des unités de données)

Le menu Data Unit List (Liste des unités de données) propose les options suivantes :



Il vous permet d'effectuer les opérations suivantes :

- Affichage des unités de données
- Affichage/Modification des informations détaillées d'une unité de données
- Affichage de l'historique des activités relatif à une unité de données
- Destruction des clés post-opérationnelles d'une unité de données

## Affichage des unités de données

Pour afficher les unités de données, dans le menu Data Units (Unités de données), choisissez Data Unit List (Liste des unités de données). L'écran Data Unit List (Liste des unités de données) s'affiche.

Data Unit List

Filter: Data Unit ID =

Show Data Units in any Key Group Use Refresh Reset | < << >>

Results in page: 15 (last page)

Data Unit ID	External Unique ID	Description
D75BB76E261B05F64AA938305DEDD3B9		
FDAC7620B1491D5014B42E4F7C533F8E		
FDAC7620B1491D5041A98D806AEC18B5	745F33ACECA3E509297643D214B29E1CB9BD4CDF9456...	
FDAC7620B1491D5065906BDAC533C0DB	B49548C84E2B68B90B8100830730F1910956497C5CB4C...	
FDAC7620B1491D5065B3DB5B991A4F18	91BB80FFB62BC006C4BD61E45E6D1C8ABFD29FDDA7A5...	
FDAC7620B1491D506CB5E9AB176DB3B0	563513FE2096254BAF1D069518FE950D79734341E7C7B...	
FDAC7620B1491D506DC3C3B2E286ADDF	FD8F94E8CC77FA07E30CDA204C2E2C6EE3835179E4A5...	Description for Data Unit te
FDAC7620B1491D5077E2EAE578D79F2D	D89550D598A811C2F140BF5D880BE842DCDDA9CD826F...	
FDAC7620B1491D507D0919C428CF50E0	F1DA375B1243A8F557ECFFF9010D663B5E01FBDA0924...	
FDAC7620B1491D5090E82378AEEAD80D	9D697FCCA082AF775C0244500444EF0DF155D96FF9C3...	
FDAC7620B1491D509DA29E93ACD06FD2	9A20955340BFAD0EA7B498B31A2D2499726A88B006C1...	
FDAC7620B1491D50B543A1A1312417E1	3E5BAFE1923CE8C49F913B62989228DC92EA5E72A711...	
FDAC7620B1491D50F37D23722C616818	45B1180CB4AD661D41EADBC783B9745BE42D2B075EBB...	
FDAC7620B1491D50FAB86E1F886F559B		
FDAC7620B1491D50FFF4DB6487307C4A	37FA9EBBA83122591DFB921156003A4C1DDF3AFAEB73...	

Details... Activity History... Destroy Keys... Modify Key Group... Export Keys...

Vous pouvez également faire défiler la base de données et filtrer la liste des unités de données selon l'un des critères suivants :

- Data Unit ID (ID de l'unité de données)
- External Unique ID (ID unique externe)
- Description
- External Tag (Balise externe)
- Created Date (Date de création)
- Imported (Importée)
- Exported (Exportée)
- State (État)

Le bouton Use (Utiliser) applique le filtre à la liste affichée pour l'unité de données.

Les champs et leur description sont fournis ci-dessous :

**Filter (Filtre)**

Affiche les champs que vous pouvez utiliser pour filtrer les résultats des requêtes passées au KMA. Les valeurs possibles sont les suivantes :

- Data Unit ID (ID de l'unité de données)
- External Unique ID (ID unique externe)
- Description
- External Tag (Balise externe)
- Created Date (Date de création)
- Imported (Importée)
- Exported (Exportée)
- State (État)

**Zone Filter Operator (Opérateur de filtre)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'opérateur de filtre voulu. Les valeurs possibles sont les suivantes :

- Égal à =
- Différent de <>
- Supérieur à >
- Inférieur à <
- Supérieur ou égal à >=
- Inférieur ou égal à <=
- Commence par ~
- Vide
- Non vide

**Zone Filter Value 1 (Valeur de filtre 1)**

Si vous avez sélectionné le filtre de date, cliquez sur Set Date (Définir la date) afin de spécifier la date et l'heure de départ. La valeur s'affiche comme valeur de départ de la plage des clés de filtrage. Si vous avez sélectionné n'importe quel autre filtre, saisissez une valeur dans ce champ.

**Zone Filter Value 2 (Valeur de filtre 2)**

Si vous avez sélectionné le filtre de date, cliquez sur Set Date (Définir la date) afin de sélectionner une date et une heure de fin. La valeur s'affiche comme valeur de fin de la plage de clés de filtrage.

**Zone Filter Value 3 (Valeur de filtre 3)**

Cliquez sur la flèche pointant vers le bas et sélectionnez l'un des filtres suivants :

**Show Data Units in Any Key Group (Afficher les unités de données de tous les groupes de clés) Utiliser (Utiliser)**

Cliquez sur ce bouton pour appliquer le filtre à la liste affichée.

**Refresh (Actualiser)**

Ce bouton permet d'actualiser la liste affichée.

**Reset (Réinitialiser)**

Ce bouton permet de supprimer tous les filtres et de réinitialiser la liste affichée sur la première page.



Ce bouton permet d'atteindre la première page de la liste.



Ce bouton permet d'atteindre la page précédente.



Ce bouton permet d'atteindre la page suivante.

**Results in Page (Résultats de la page)**

Affiche le nombre d'enregistrements par page qui ont été configurés dans le champ Query Page Size (Taille d'une page de requête) de la boîte de dialogue Options.

**Data Unit ID (ID de l'unité de données)**

Affiche un identificateur unique généré par le système permettant de différencier les unités de données les unes des autres.

**External Unique ID (ID unique externe)**

Affiche un identificateur externe unique pour l'unité de données.

Cette valeur est envoyée au KMS par l'agent et peut ne pas être visible en externe par l'utilisateur final. Pour les bandes LTO Gen 4, il s'agit du numéro de série gravé sur la cartouche lors de sa fabrication. Ne confondez pas cette valeur avec le numéro de série du volume (volser, volume serial number) d'un barre à codes optique ou d'une étiquette de bande ANSI. Cette valeur n'est pas utilisée par les lecteurs de bande Sun.

**Description**

Donne une description de l'unité de données.

**External Tag (Balise externe)**

Décrit une balise externe unique pour l'unité de données.

Pour les bandes figurant dans une bibliothèque de bandes Sun ou celles dotées d'une étiquette normalisée ANSI, ce champ correspond au numéro de volume. Si la bande se trouve dans une bibliothèque et dispose d'une étiquette ANSI, le numéro de volume de la bibliothèque (c.-à-d., le code à barres optique) est utilisé s'il diffère de celui indiqué sur l'étiquette ANSI. Pour les bandes écrites sur des lecteurs autonomes sans étiquette ANSI, ce champ est vide.

**Created Date (Date de création)**

Indique les date et heure de création/d'enregistrement de l'unité de données.

### **Imported (Importée)**

Indique si l'unité de données a été importée.

### **Exported (Exportée)**

Indique si l'unité de données a été exportée.

### **State (État)**

Indique l'état de l'unité de données. Les valeurs possibles sont les suivantes :

- **No Key (Pas de clé)** : état défini lors de la création de l'unité de données, quand celle-ci n'est encore associée à aucune clé.
- **Readable (Lisible)** : état défini lorsque l'unité de données comporte des clés permettant de la déchiffrer (lire) au moins partiellement.
- **Normal** : état défini lorsque l'unité de données comporte des clés permettant de la déchiffrer (lire) au moins partiellement. De plus, l'unité de données comporte au moins une clé d'état de protection et traitement pouvant servir à chiffrer les données. L'unité de données est donc inscriptible.

- **Needs ReKey** : état défini lorsque l'unité de données comporte des clés permettant de la déchiffrer (lire) au moins partiellement. Toutefois, l'unité de données ne dispose pas d'au moins une clé d'état de protection et traitement.

Si des données sont écrites sur cette bande, elles se voient automatiquement attribuer une nouvelle clé de protection et traitement.

- **Shredded (Éliminé)** : état défini lorsque toutes les clés associées à cette unité de données sont détruites. Il est alors impossible de lire cette unité de données ou d'y écrire. Toutefois, il est possible de créer une nouvelle clé pour cette unité de données, en rétablissant son état sur Normal.

## Affichage/Modification des informations détaillées sur une unité de données

**Remarque** – Si vous n'êtes pas opérateur, tous les champs (y compris le bouton Save (Enregistrer)) sont désactivés lors de la visualisation des informations détaillées relatives à une unité de données. Si vous êtes doté du rôle Compliance Officer (Responsable de la conformité), le champ Key Group (Groupe de clés) est activé.

Pour modifier les informations d'une unité de données :

1. Dans l'écran Data Unit List (Liste des unités de données), sélectionnez l'unité de données à modifier, puis cliquez sur le bouton Details (Détails). L'écran Data Unit Details (Détails de l'unité de données) s'affiche.

The screenshot shows a window titled "Data Unit Details" with three tabs: "General", "Key List", and "Backups with Destroyed Keys List". The "General" tab is active. The fields are as follows:

Data Unit ID:	FDAC7620B1491D506DC3C3B2E286AD0F
Description:	Description for Data Unit test 1, modified
External Unique ID:	FD8F94E8CC77FA07E30CDA204C2E2C6EE3835179E4A5B6956F65D54235912DDC
External Tag:	External Tag for Data Unit test 1, modified
Created Date:	12/4/2007 8:30:04 AM
State:	Shredded
Flags:	<input type="checkbox"/> Imported <input type="checkbox"/> Exported

At the bottom right, there are "Save" and "Cancel" buttons.

2. Vous pouvez modifier les paramètres suivants :

### Description

Saisissez une nouvelle valeur. Les informations initiales sont fournies par le pilote de chiffrement du logiciel au cours de l'enregistrement. Cette valeur doit comprendre entre 1 et 64 caractères ou être vide.

### External Tag (Balise externe)

Affiche un identificateur externe unique pour l'unité de données. Cette valeur doit comprendre entre 1 et 64 caractères ou être vide. Ce champ contient généralement l'étiquette ou le code à barres de la cartouche de bande.

3. Cliquez sur le bouton Save (Enregistrer) pour sauvegarder vos modifications.

Les champs suivants ne sont pas modifiables :

### Onglet General (Général)

- Data Unit ID (ID de l'unité de données)
- External Unique ID (ID unique externe)
- Created Date (Date de création)
- State (État)
- Flags Imported/Exported (Indicateurs importés/exportés)

### Onglet Key List (Liste des clés)

**Data Unit Details**

General | **Key List** | Backups with Destroyed Keys List

Data Unit ID: FDAC7620B1491D506DC3C3B2E286AD0F

Data Unit Description: Description for Data Unit test 1, modified

Key List

Filter: Key ID =

Use Refresh Reset |< << >>

Results in page: 1 (last page)

Key ID	Key Type	Created Date	Activation Date ▾	Destroyed Date
FDAC7620B1491D503AC99FEDBCC45D40CBC536982E...	AES-256	12/4/2007 8:20:53 AM	12/4/2007 8:30:04 AM	12/4/2007 8:30:04 AM

Details... Compromise... Activity History... Save Report...

Save Cancel

#### Data Unit ID (ID de l'unité de données)

Permet d'identifier de manière unique l'unité de données.

#### Data Unit Description (Description de l'unité de données)

Donne une description de l'unité de données.

#### Key ID (ID de la clé)

Affiche des informations relatives à la clé associée à l'unité de données.

#### Key Type (Type de clé)

Indique le type d'algorithme de chiffrement utilisé par cette clé. La seule valeur possible est AES-256.

#### Created Date (Date de création)

Affiche les date et heure de création de la clé.

**Activation Date (Date d'activation)**

Affiche les date et heure d'activation de la clé. Il s'agit des date et heure de l'envoi initial de la clé à l'agent. Ces dates correspondent aux date et heure de début de la période de chiffrement et de la durée de validité de la clé.

**Destroyed Date (Date de destruction)**

Affiche la date de destruction de la clé. Si ce champ est vide, la clé n'est pas détruite.

**Destruction Comment (Commentaire sur la destruction)**

Affiche des informations fournies par l'utilisateur concernant la destruction de la clé. Si ce champ est vide, la clé n'est pas détruite.

**Imported (Importée)**

Indique si l'unité de données a été importée.

**Exported (Exportée)**

Indique si l'unité de données a été exportée.

**Key Group (Groupe de clés)**

Affiche le groupe de clés associé à l'unité de données.

**Encryption End Date (Date de fin du chiffrement)**

Affiche les date et heure à partir desquelles la clé ne sera plus utilisée ou depuis lesquelles elle n'a plus été utilisée pour chiffrer des données.

**Deactivation Date (Date de désactivation)**

Affiche les date et heure de désactivation de la clé.

**Compromised Date (Date de compromis)**

Affiche la date à laquelle la clé a été compromise. Si ce champ est vide, la clé n'est pas compromise.

**Compromised Comment (Commentaire sur le compromis)**

Affiche des informations fournies par l'utilisateur concernant la clé compromise. Si ce champ est vide, la clé n'est pas compromise.

**Key State (État de la clé)**

Indique l'état de la clé de l'unité de données. Les valeurs possibles sont les suivantes :

**Generated (Généré)**

État défini suite à la création de la clé sur un KMA faisant partie d'un cluster KMS. La clé reste générée tant qu'elle n'est pas répliquée sur au moins un autre KMA dans le cadre d'un cluster KMS composé de plusieurs dispositifs de gestion des clés. Dans un cluster comportant un seul KMA, la clé reste générée jusqu'à son enregistrement dans au moins une sauvegarde.

**Ready (Prêt)**

État défini lorsque la clé a été protégée contre les pertes de données par répllication ou par exécution d'une sauvegarde. Une clé définie dans cet état est disponible pour l'assignation.

**Protect and Process (Protection et traitement)**

État défini si la clé a été assignée lorsqu'un agent de chiffrement demande la création d'une nouvelle clé. Une clé définie dans cet état peut servir à des fins de chiffrement et de déchiffrement.

**Process Only (Traitement seul)**

État défini lorsque la clé a été assignée mais que sa période de chiffrement est arrivée à échéance. Une clé définie dans cet état peut servir à des fins de déchiffrement, mais pas de chiffrement.

**Deactivated (Désactivé)**

État défini lorsque la clé a dépassé sa durée de validité, mais qu'elle est peut-être encore nécessaire pour traiter (déchiffrer) des informations.

**Compromised (Compromis)**

État défini lorsque la clé a été déverrouillée ou découverte par une entité non autorisée. Une clé définie dans cet état peut servir à des fins de déchiffrement, mais pas de chiffrement.

**Incompletely Destroyed (Détruit partiellement)**

État défini lorsque la clé a été détruite, mais qu'elle figure encore dans au moins une sauvegarde.

**Completely Destroyed (Entièrement détruit)**

État défini lorsque toutes les sauvegardes dans lesquelles la clé détruite apparaît ont été détruites.

**Compromised and Incompletely Destroyed (Compromis et détruit partiellement)**

État défini lorsque la clé compromise figure toujours dans au moins une sauvegarde.

**Compromised and Completely Destroyed (Compromis et détruit entièrement)**

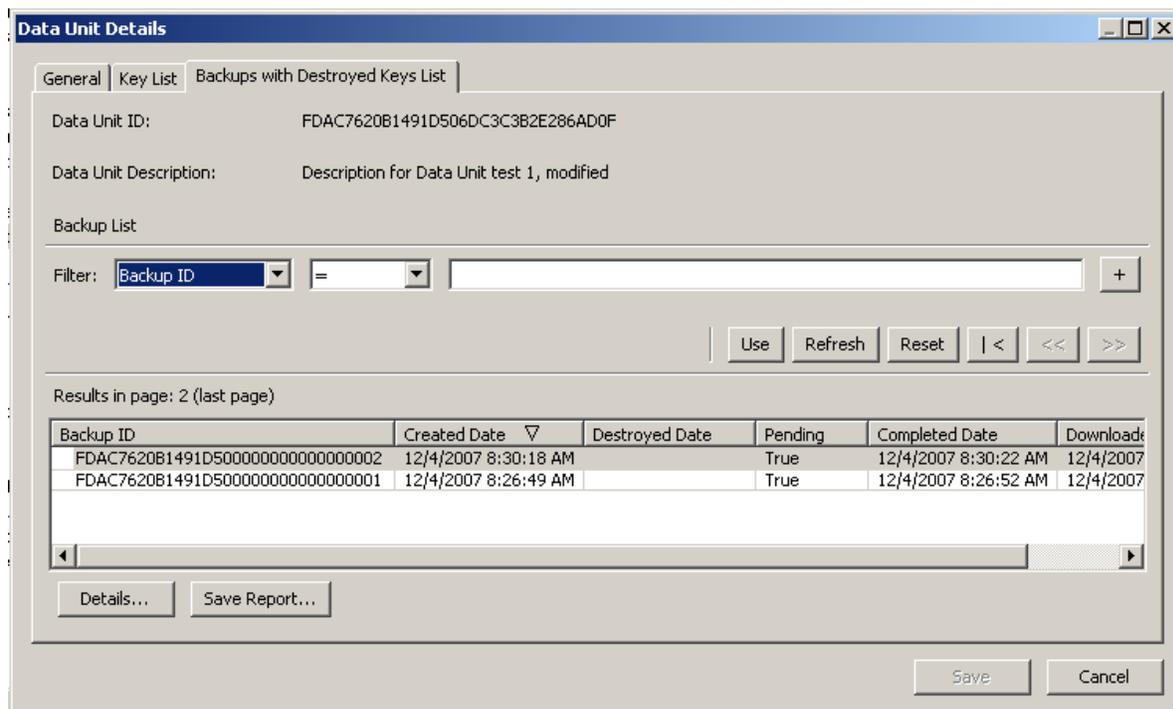
État défini lorsque toutes les sauvegardes dans lesquelles la clé compromise apparaît ont été détruites.

**Recovery Activated (Activé pour la récupération)**

Indique si la clé est liée à l'unité de données par une action de récupération.

Cette condition se produit lorsqu'une clé est utilisée pour une unité de données par un KMA d'un cluster KMS puis que, suite à une panne, la clé est ensuite demandée par un autre KMA pour cette unité de données. Si la panne (coupure réseau, par exemple) a empêché la diffusion de l'allocation de la clé au second KMA, celui-ci crée la liaison à l'unité de données. Une clé de ce type se trouve dans un état « activé pour la récupération ». L'administrateur souhaitera peut-être évaluer les KMA du système ou les pannes réseau. Les valeurs possibles sont True (Vrai) ou False (Faux).

### Onglet Backups with Destroyed Keys List (Liste des sauvegardes avec clés détruites)



Une unité de données ne peut pas être considérée comme « entièrement détruite » tant que toutes les sauvegardes contenant les clés associées n'ont pas été détruites.

L'onglet Backups with Destroyed Keys List (Liste des sauvegardes avec clés détruites) de la boîte de dialogue Data Unit Details (Détails de l'unité de données) facilite l'identification des sauvegardes contenant des clés associées à l'unité de données et de leur statut de destruction.

La logique à suivre pour déterminer si une sauvegarde donnée contient effectivement une clé de données particulière est la suivante :

Une sauvegarde contient une clé d'unité de données si elle a été créée après l'unité de données **et** si la clé n'a pas été détruite ou bien si elle a été détruite **et** que sa destruction a eu lieu après la création de la sauvegarde.

Toutefois, la comparaison des date et heure doit prendre en compte le fait que les horloges des différents KMA d'un cluster ne sont pas toujours synchronisées de manière automatique (si aucun serveur NTP n'est spécifié) et, de ce fait, que les heures indiquées ne sont pas nécessairement identiques. Pour tenir compte d'une éventuelle différence horaire entre les KMA, une fenêtre de temps des sauvegardes est utilisée dans la comparaison. Cette fenêtre est réglée sur cinq minutes de décalage. En tenant compte de cette fenêtre, la vérification comparative se comporte de la manière suivante :

Une sauvegarde contient une clé d'unité de données si elle a été créée dans un délai de cinq minutes par rapport à la clé **et** si la clé de l'unité de données a été détruite dans les cinq minutes précédant ou suivant la création de la sauvegarde.

La fenêtre permet de réduire la probabilité d'erreurs concernant la prétendue absence d'une unité de données dans une sauvegarde alors qu'il n'en est rien. Une telle situation, appelée « faux négatif », nuit gravement aux exigences de conformité en matière de destruction de données. L'utilisation de cette fenêtre de temps augmente cependant la probabilité d'occurrences de clés d'unités de données signalées comme faisant partie d'une sauvegarde alors qu'il n'en est rien. Contrairement aux « faux négatifs », les « faux positifs » ne nuisent pas aux exigences de conformité en matière de destruction de données.

**Data Unit ID** (ID de l'unité de données)

Permet d'identifier de manière unique l'unité de données.

**Data Unit Description** (Description de l'unité de données)

Donne une description de l'unité de données.

**Data Unit Destruction Status** (Statut de destruction de l'unité de données)

Indique le statut de destruction de l'unité de données.

**Backup ID (ID de la sauvegarde)**

Identifie la sauvegarde.

**Created Date** (Date de création)

Affiche les date et heure de création du fichier de sauvegarde (c.-à-d., le démarrage de la sauvegarde).

**Destroyed Date** (Date de destruction)

Affiche les date et heure de destruction du fichier de sauvegarde.

**Pending** (En attente)

Indique si la sauvegarde est encore en attente. Les valeurs possibles sont True (Vrai) ou False (Faux).

**Completed Date (Date de fin)**

Affiche les date et heure de fin du fichier de sauvegarde.

**Downloaded Date (Date de téléchargement)**

Affiche les date et heure de téléchargement du fichier de sauvegarde.

4. Cliquez sur le bouton Save (Enregistrer) pour sauvegarder vos modifications.

## Destruction des clés post-opérationnelles

Pour détruire des clés post-opérationnelles associées à une unité de données :

1. Dans l'écran Data Unit List (Liste des unités de données), mettez en surbrillance l'unité de données à détruire, puis cliquez sur le bouton Destroy Keys (Détruire les clés).
2. La boîte de dialogue suivante s'affiche, vous invitant à spécifier les clés à détruire.



### **Deactivated keys (Clés désactivées)**

Cochez cette case si vous souhaitez détruire les clés ayant dépassé leur durée de validité mais qui peuvent encore servir à traiter (déchiffrer) des informations sur les données.

### **Compromised keys (Clés compromises)**

Cochez cette case si vous souhaitez détruire les clés déverrouillées ou découvertes par une entité non autorisée.

### **Destruction Comment (Commentaire sur la destruction)**

Saisissez un commentaire sur la destruction de ces clés.

3. Si vous cliquez sur le bouton Destroy (Détruire), une autre boîte de dialogue s'affiche, confirmant la destruction des clés.
4. Cliquez sur le bouton Yes (Oui). Une autre boîte de dialogue s'affiche, présentant le nombre de clés détruites.

## Menu Software Upgrade (Mise à niveau du logiciel)

L'option Software Upgrade (Mise à niveau du logiciel) permet à l'opérateur de télécharger un fichier de mise à niveau logicielle vers le KMA et de l'appliquer immédiatement. Les mises à jour logicielles sont signées par Sun et vérifiées par le KMA avant leur application.

---

**Remarque** – Avant d'exécuter cette fonction, sauvegardez votre système. Pour plus d'informations à ce sujet, reportez-vous à la section « [Création d'une sauvegarde](#) », page 259.

---

### Téléchargement et application d'une mise à niveau logicielle

Pour mettre à niveau le KMA :

1. Dans le menu Local Configuration (Configuration locale), choisissez **Software Upgrade** (Mise à niveau du logiciel). L'écran Software Upgrade (Mise à niveau du logiciel) s'affiche.

Version	Install Date	Active
Build1.79 (Debug Build)	10/3/2007 7:42:00 AM	True

2. Dans le champ Software Upgrade File Name (Nom du fichier de mise à niveau du logiciel), tapez le nom du fichier de mise à niveau logicielle. Une autre solution consiste à cliquer sur Browse (Parcourir) pour localiser le fichier. Cliquez sur OK pour revenir à l'écran Software Upgrade (Mise à niveau du logiciel). Cliquez sur le bouton Upload and Apply (Télécharger et appliquer).
3. Un message s'affiche, indiquant que le fichier a bien été téléchargé.

4. Un message s'affiche, indiquant que le fichier de mise à niveau est en cours d'application.
5. Pour activer le fichier de mise à niveau, sélectionnez la nouvelle version dans la liste des versions disponibles située en haut de l'écran et cliquez sur le bouton **Activate** (Activer). Tant qu'elle n'est pas activée, la nouvelle version reste inactive sur le système.

## Menu Backup List (Liste des sauvegardes)

Pour connaître les procédures de visualisation des informations détaillées d'un fichier de sauvegarde, reportez-vous à la section « [Menu Backup List \(Liste des sauvegardes\)](#) », page 255.

## Menu Audit Event List (Liste des événements d'audit)

Pour connaître les procédures de visualisation de la liste des événements d'audit, reportez-vous à la section « [Menu Audit Event List \(Liste des événements d'audit\)](#) », page 216.

## Menu KMA List (Liste des KMA)

Pour connaître les procédures de visualisation de la liste des KMA, reportez-vous à la section « [Menu KMA List \(Liste des KMA\)](#) », page 83.

## Menu Site List (Liste des sites)

Pour connaître les procédures de visualisation de la liste des sites, reportez-vous à la section « [Menu Site List \(Liste des sites\)](#) », page 106.

## Menu SNMP Manager List (Liste des gestionnaires SNMP)

Pour connaître les procédures de visualisation de la liste des gestionnaires SNMP, reportez-vous à la section « [Menu SNMP Manager List \(Liste des gestionnaires SNMP\)](#) », page 114.

## Menu System Time (Heure système)

Pour connaître les procédures de visualisation de l'heure du KMA, reportez-vous à la section « [Menu System Time \(Heure système\)](#) », page 170.

## Menu Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA)

Pour connaître les procédures de visualisation du statut de verrouillage du KMA, reportez-vous à la section « [Lock/Unlock KMA \(Verrouiller/Déverrouiller le KMA\)](#) », page 166.

## Tâches du responsable des sauvegardes

Ce chapitre décrit les opérations pouvant être effectuées par un utilisateur doté du rôle Backup Operator (Responsable des sauvegardes). Si d'autres rôles vous ont été assignés, reportez-vous au chapitre approprié. Vous y trouverez des instructions sur les tâches associées à chaque rôle.

### Rôle Backup Operator (Opérateur des sauvegardes)

En tant qu'opérateur des sauvegardes, vous êtes chargé de la sécurisation et du stockage des données et des clés associées.



### Menu Backup List (Liste des sauvegardes)

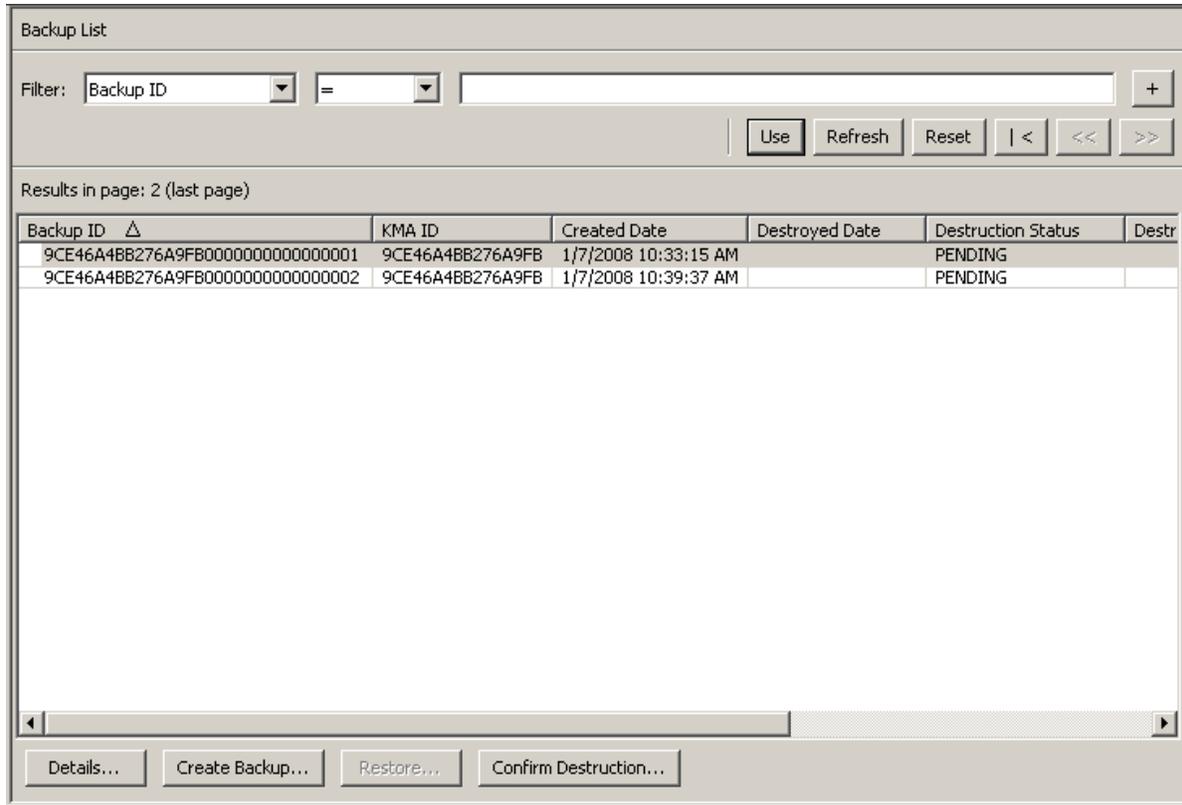
L'option de menu Backup List (Liste des sauvegardes) permet au responsable des sauvegardes d'effectuer les opérations suivantes :

- Afficher l'historique des sauvegardes et confirmer le statut de destruction correspondant
- Créer des sauvegardes

## Affichage de l'historique des fichiers de sauvegarde

Pour afficher l'historique des fichiers de sauvegarde :

Dans le menu Backups (Sauvegardes), choisissez **Backup List (Liste des sauvegardes)**. L'écran Backup List (Liste des sauvegardes) s'affiche.



Pour obtenir plus d'informations sur une sauvegarde, mettez celle-ci en surbrillance et cliquez sur le bouton Details (Détails). Pour plus d'informations, reportez-vous à la section « [Affichage d'informations détaillées sur une sauvegarde](#) ».

Cliquez sur le bouton Create Backup (Créer une sauvegarde) pour créer une sauvegarde. Pour plus d'informations, reportez-vous à la section « [Création d'une sauvegarde](#) », page 259.

Cliquez sur le bouton Confirm Destruction (Confirmer la destruction) afin de confirmer la destruction de la sauvegarde. Pour plus d'informations, reportez-vous à la section « [Confirmation d'une destruction de sauvegarde](#) », page 260.

## Affichage d'informations détaillées sur une sauvegarde

La boîte de dialogue Backup Details (Détails de la sauvegarde) permet d'afficher des informations détaillées sur un fichier de sauvegarde.

---

**Remarque** – Les fichiers de sauvegarde sont téléchargés vers la machine qui exécutait KMS Manager lors de la création de la sauvegarde.

---

Pour afficher des informations détaillées sur un fichier de sauvegarde :

1. Dans l'écran Backups List (Liste des sauvegardes), double-cliquez sur l'entrée de sauvegarde pour laquelle vous souhaitez obtenir des informations détaillées ou mettez-la en surbrillance et cliquez sur le bouton Details (Détails). La boîte de dialogue Backup Details (Détails de la sauvegarde) s'affiche en présentant tous les champs désactivés.

Backup ID:	FDAC7620B1491D500000000000000001
KMA ID:	FDAC7620B1491D50
Created Date:	12/4/2007 8:26:49 AM
Completed Date:	12/4/2007 8:26:52 AM
Downloaded Date:	12/4/2007 8:28:13 AM
Destroyed Date:	
Destruction Status:	PENDING
Destruction Comment:	

2. Les champs et leur description sont fournis ci-dessous :

**Backup ID (ID de la sauvegarde)**

Affiche un identificateur unique généré par le système permettant de différencier les fichiers de sauvegarde les uns des autres.

**KMA ID (ID du KMA)**

Affiche le KMA sur lequel ce fichier de sauvegarde est généré.

**Created Date (Date de création)**

Affiche les date et heure de création du fichier de sauvegarde.

**Completed Date (Date de fin)**

Affiche les date et heure de fin du fichier de sauvegarde.

**Downloaded Date (Date de téléchargement)**

Affiche les date et heure de téléchargement du fichier de sauvegarde.

**Destroyed Date (Date de destruction)**

Affiche la date de destruction du fichier de sauvegarde.

**Destruction Status (Statut de destruction)**

Indique le statut de la sauvegarde par rapport à sa destruction.

**Destruction Comment (Commentaire sur la destruction)**

Affiche des informations fournies par l'utilisateur concernant la destruction du fichier de sauvegarde.

3. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue.

## Création d'une sauvegarde

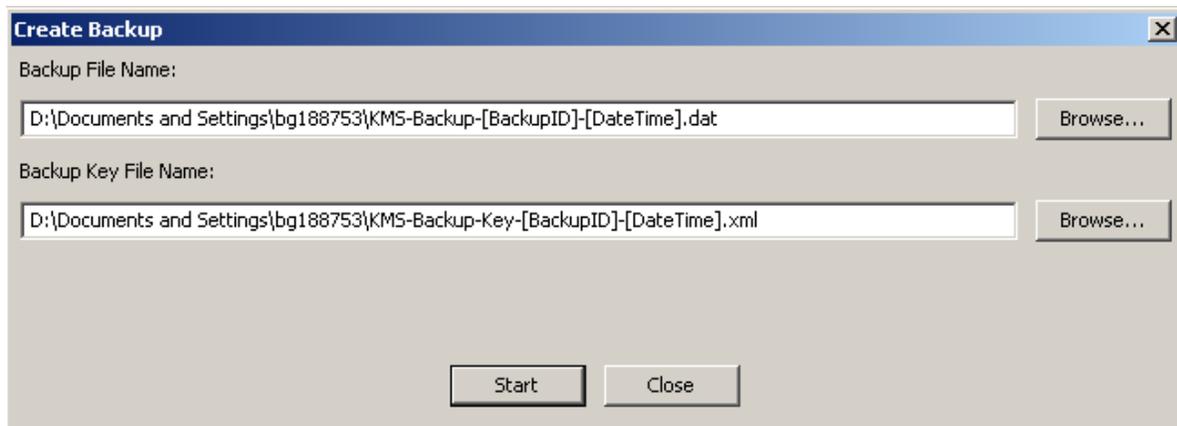
**Important** – Le responsable de la sécurité doit sauvegarder les données de clés de la sécurité principale avant de créer une sauvegarde. Reportez-vous à la section « [Création d'une sauvegarde de sécurité principale](#) », page 157.

À un instant T, il n'existe qu'un seul fichier de sauvegarde et qu'un seul fichier de restauration sur un KMA.

Cette option permet à l'utilisateur de créer une sauvegarde composée de deux fichiers : un fichier de sauvegarde et un fichier de clés de sauvegarde.

Pour créer une sauvegarde :

1. Dans l'écran Backup·List (Liste des sauvegardes), cliquez sur le bouton Create Backup (Créer une sauvegarde). La boîte de dialogue Create Backup (Création d'une sauvegarde) s'affiche.



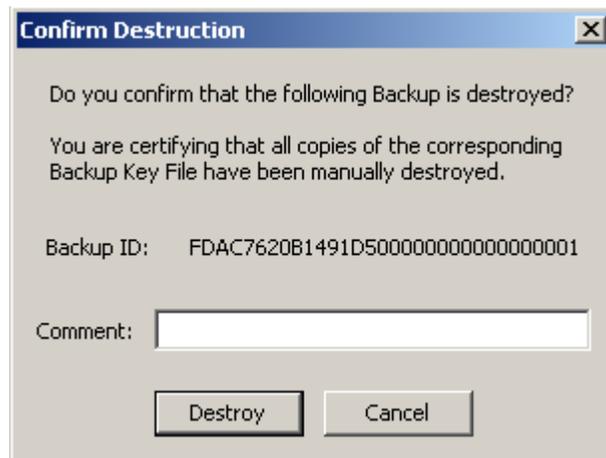
**Remarque** – Les noms du fichier de sauvegarde et du fichier de clés de sauvegarde sont générés automatiquement. Vous pouvez cependant les modifier. Une autre solution consiste à cliquer sur le bouton Browse (Parcourir) afin de sélectionner un chemin de destination.

2. Cliquez sur le bouton Start (Commencer) pour créer le fichier de sauvegarde et télécharger le fichier de clés de sauvegarde vers la destination définie par l'utilisateur.
3. Une fois la sauvegarde terminée, un message vous informe de la fin de l'opération. Cliquez sur le bouton Close (Fermer) pour fermer cette boîte de dialogue.
4. Vous revenez à l'écran Backup List (Liste des sauvegardes), dans lequel apparaît le nouveau fichier.

## Confirmation d'une destruction de sauvegarde

Pour confirmer la destruction d'une sauvegarde :

1. Dans l'écran Backup List (Liste des sauvegardes), mettez la sauvegarde à détruire en surbrillance et cliquez sur le bouton Confirm Destruction (Confirmer la destruction). La boîte de dialogue suivante s'affiche, confirmant la mise à jour du statut de destruction de la sauvegarde sélectionnée. Avant de poursuivre, assurez-vous que toutes les copies du fichier de clés de sauvegarde correspondant ont été détruites manuellement.



2. Si vous êtes certain que toutes les copies du fichier de clés de sauvegarde correspondant ont bien été détruites manuellement, cliquez sur Yes (Oui). Sinon, choisissez No pour arrêter le processus.
3. Si vous avez cliqué sur Yes, la sauvegarde et les unités de données associées sont entièrement détruites.

## Autres fonctions

Un utilisateur doté du rôle Backup Operator (Opérateur des sauvegardes) peut également effectuer les opérations suivantes :

- Affichage de la liste des événements d'audit
- Affichage de l'heure système
- Affichage du statut de verrouillage du KMA

Pour connaître les procédures de visualisation du journal d'audit, reportez-vous à la section « [Menu Audit Event List \(Liste des événements d'audit\)](#) », page 216.

Pour connaître les procédures de visualisation de l'heure du KMA, reportez-vous à la section « [Menu System Time \(Heure système\)](#) », page 170.

Pour connaître les procédures de visualisation du statut de verrouillage du KMA, reportez-vous à la section « [Lock/Unlock KMA \(Verrouiller/Déverrouiller le KMA\)](#) », page 166.



## Tâches du responsable des audits

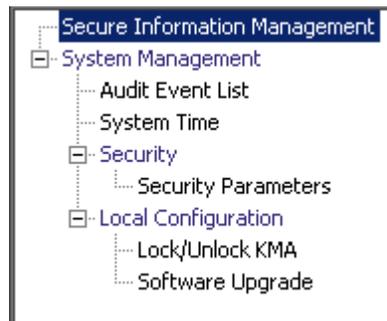
---

Ce chapitre décrit les opérations pouvant être effectuées par un utilisateur doté du rôle Auditor (Responsable des audits). Si d'autres rôles vous ont été assignés, reportez-vous au chapitre approprié. Vous y trouverez des instructions sur les tâches associées à chaque rôle.

---

### Rôle Auditor (Responsable des audits)

En tant que responsable des audits, vous êtes habilité à afficher les événements de la liste des audits et le KMA.



### Menu Audit List (Liste des audits)

Pour connaître les procédures d'utilisation du menu Audit List, reportez-vous à la section « [Menu Audit Event List \(Liste des événements d'audit\)](#) », page 216.

### Menu Security Parameters (Paramètres de sécurité)

Le menu Security Parameters (Paramètres de sécurité) donne à l'auditeur la possibilité de visualiser les paramètres de sécurité du KMA. Pour connaître les procédures d'utilisation de ce menu, reportez-vous à la section « [Menu Security Parameters \(Paramètres de sécurité\)](#) », page 152.

## Autres fonctions

Un utilisateur doté du rôle Auditor (Responsable des audits) peut également :

- afficher l'état de verrouillage/déverrouillage du KMA ;
- afficher l'heure système.

Pour connaître les procédures de visualisation du statut de verrouillage/déverrouillage du KMA, reportez-vous à la section « [Lock/Unlock KMA \(Verrouiller/Déverrouiller le KMA\)](#) », page 166.

Pour connaître les procédures de réglage de l'heure du KMA, reportez-vous à la section « [Menu System Time \(Heure système\)](#) », page 170.

Pour connaître les procédures de visualisation des versions de logiciels installées, reportez-vous à la section « [Menu Software Upgrade \(Mise à niveau du logiciel\)](#) », page 252.

## Utilisation de la console KMS

---

Ce chapitre décrit les options de la console KMS.

---

### Présentation de la console KMS

La console KMS est une interface texte de terminal permettant à l'utilisateur de configurer les fonctions de base du KMA. Pour y accéder, il doit physiquement connecter un moniteur vidéo et un clavier au KMA ou se servir de la fonction de console distante de l'interface du navigateur Web ELOM (voir « [Démarrage du logiciel ELOM \(Embedded Light Out Manager\)](#) », page 20).

La console KMS est lancée automatiquement par le système d'exploitation au démarrage du KMA. Elle ne peut pas être arrêtée par un utilisateur. Selon les rôles assignés à un utilisateur, les options disponibles sur la console KMS varient.

Avant qu'un utilisateur puisse se connecter à la console KMS, les comptes utilisateur doivent être créés dans KMS Manager. Pour se connecter à la console KMS, l'utilisateur doit se servir des mêmes nom d'utilisateur/phrase de passe que ceux utilisés pour l'authentification auprès du KMS.

---

**Remarque** – Seul le premier compte Security Officer (Responsable de la sécurité) est créé lors du lancement du programme QuickStart.

---

---

# Connexion au KMA

Une fois le KMA démarré, les informations suivantes s'affichent.

```
Sun Microsystems, Inc.  
Key Management System Version xxx
```

```
-----  
Please enter your User ID:
```

1. À l'invite, saisissez votre nom d'utilisateur, puis appuyez sur **<Entrée>**.
2. À l'invite `Please enter your Passphrase` (Saisissez votre phrase de passe), saisissez votre phrase de passe, puis appuyez sur **<Entrée>**. Selon les rôles assignés à un utilisateur, les options disponibles sur la console KMS varient. Le menu indique la version du KMA et l'utilisateur connecté.

Les tâches associées aux différents rôles d'utilisateur sont traitées dans les pages suivantes. Il s'agit des rôles suivants :

- Operator (Opérateur) (voir « [Fonctions du rôle Operator \(Opérateur\)](#) », page 270)
- Security Officer (Responsable de la sécurité) (voir « [Fonctions du rôle Security Officer \(Responsable de la sécurité\)](#) », page 277)
- Autres rôles (voir « [Fonctions associées aux autres rôles](#) », page 293)

## Operator (Opérateur)

Le menu suivant illustre les options disponibles pour le rôle d'opérateur.

```
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:
```

## Security Officer (Responsable de la sécurité)

Le menu suivant illustre les options disponibles pour le rôle de responsable de la sécurité.

```
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:
```

---

**Remarque** – Si les rôles d'opérateur et de responsable de la sécurité ont été assignés à un même utilisateur, les options de menu sont combinées de la manière suivante :

```
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:
```

---

## Autres rôles

Pour tous les autres rôles, autrement dit, Backup Operator (Opérateur des sauvegardes), Compliance Officer (Responsable de la conformité) et Auditor (Responsable des audits), un menu similaire à celui de l'exemple suivant s'affiche. Les seules options disponibles sont la déconnexion du KMA et la définition de la disposition du clavier.

```
Key Management System Version xxx (col)
-----

(1) Set Keyboard Layout
(0) Logout
-----
Please enter your choice:
```

## Fonctions du rôle Operator (Opérateur)

Cette section décrit les tâches qu'un opérateur est habilité à effectuer. Il s'agit des tâches suivantes :

- Redémarrage du KMA
- Arrêt du KMA
- Activation/désactivation du support technique
- Désactivation de l'administrateur principal
- Définition de la disposition du clavier
- Déconnexion du KMA

Le menu de l'opérateur est présenté ci-dessous.

```
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:
```

---

**Remarque** – Les options de menu Technical Support (Support technique) et Primary Administrator (Administrateur principal) s'affichent uniquement lorsque leurs paramètres sont activés.

---

## Redémarrage du KMA

L'option de menu Reboot KMA (Redémarrer le KMA) permet à un opérateur d'arrêter puis de redémarrer le KMA et de réinitialiser le système d'exploitation. Cette fonction est strictement réservée à des fins de dépannage.

Pour redémarrer le KMA :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **1**, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que le compte de support est activé.

```
Reboot KMA
-----
Press Ctrl-c to abort.
Are you sure that you want to reboot the KMA? [y/n]:
```

2. À l'invite, tapez **y**, puis appuyez sur <Entrée>. La session active de la console KMS prend fin lorsque le KMA redémarre. Une fois le KMA redémarré, l'invite de connexion de la console KMS s'affiche.

## Arrêt du KMA

Cette option vous permet de terminer (d'arrêter) tous les services exécutés sur le KMA et d'arrêter physiquement le KMA proprement dit.

Pour arrêter le KMA :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **2**, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que le compte de support est activé.

```
Shutdown KMA
-----
Press Ctrl-c to abort
Are you sure that you want to shut down the KMA? [y/n]:
```

2. À l'invite, tapez **y**, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que le système est en train de s'arrêter.

Shutting down...

3. La séquence d'arrêt s'affiche. Cela fait, les informations suivantes s'affichent.

Power down.

4. Le KMA est désormais hors tension. Le KMA peut être mis sous tension à l'aide du bouton marche ou de la fonction de contrôle de l'alimentation à distance ELOM.

## Activation du compte de support technique

L'option de menu Technical Support (Support technique) permet à un opérateur d'activer ou de désactiver le compte support du système d'exploitation et l'accès au shell sécurisé (SSH) correspondant. Par défaut, le compte du support technique comme l'accès SSH sont désactivés. Comme la phrase de passe associée au compte de support est uniquement connue du service de support Sun, l'activation de ce compte n'accorde pas d'accès supplémentaire au KMA à un utilisateur de la console.

1. Pour activer le compte de support technique :

À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **3**, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que le compte de support est désactivé.

```
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. À l'invite, tapez **y**, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, vous invitant à confirmer le changement.

```
Are you sure that you want to commit these changes? [y/n]:
```

3. À l'invite, tapez **y**, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que le compte est activé. Appuyez sur `<Entrée>` pour revenir au menu principal.

```
Press Enter to continue:
```

## Désactivation du compte de support technique

Pour désactiver le compte de support technique :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `3`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que le compte de support est activé.

```

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. À l'invite, tapez `y` afin de désactiver le compte, puis appuyez sur `<Entrée>`.
3. Les informations suivantes s'affichent, vous invitant à confirmer le changement.  
`Are you sure that you want to commit these changes? [y/n]:`
4. À l'invite, tapez `y`, puis appuyez sur `<Entrée>`. Le service SSH s'arrête automatiquement.

## Désactivation de l'administrateur principal

L'option de menu Primary Administrator vous permet d'activer ou de désactiver l'accès de l'administrateur principal sur le KMA.

---

**Remarque** – Cette tâche peut uniquement être *activée* par le responsable de la sécurité ; elle peut être *désactivée* par un opérateur ou un responsable de la sécurité.

---

La désactivation de l'accès de l'administrateur principal entre en vigueur sur le champ. Si un utilisateur est connecté en tant qu'administrateur principal lorsque son accès est désactivé, la prochaine commande qu'il tente d'exécuter échoue.

1. Pour désactiver l'accès de l'administrateur principal :

À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `4`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que l'accès est activé.

```
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. À l'invite, tapez `y` afin de désactiver le compte, puis appuyez sur `<Entrée>`.

3. Les informations suivantes s'affichent, vous invitant à confirmer le changement.

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. À l'invite, tapez `y`, puis appuyez sur `<Entrée>`. L'accès de l'administrateur principal a été désactivé.

## Définition de la disposition du clavier

Cette option vous permet de changer de disposition de clavier en passant de l'anglais (English) à une variété de langues.

---

**Remarque** – La disposition du clavier devrait correspondre à celle du clavier connecté au KMA afin que celui-ci puisse interpréter correctement les touches activées.

---

Pour définir la disposition du clavier :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `5`, puis appuyez sur `<Entrée>`. Les dispositions de clavier suivantes s'affichent.

```

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. À l'invite `Please enter the number for the keyboard layout` (Saisissez le numéro de la disposition de clavier), tapez le numéro voulu. La nouvelle disposition de clavier est appliquée.
3. Les informations suivantes s'affichent. Press `<Enter>` to continue.

## Déconnexion

Pour vous déconnecter de la session de console KMS active :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **0**, puis appuyez sur <Entrée>.
2. La session active prend fin et l'invite de connexion s'affiche, permettant à l'utilisateur d'accéder à nouveau à la console KMS.

## Fonctions du rôle Security Officer (Responsable de la sécurité)

Cette section décrit les tâches qu'un responsable de la sécurité est habilité à effectuer. Il s'agit des tâches suivantes :

- Connexion du KMA au cluster
- Définition de la phrase de passe d'un utilisateur
- Définition des adresses IP du KMA
- Réinitialisation de l'état par défaut défini en usine du KMA
- Activation/Désactivation du support technique
- Activation/Désactivation de l'administrateur principal
- Définition de la disposition du clavier
- Déconnexion du KMA

Le menu du responsable de la sécurité est présenté ci-dessous.

```
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:
```

## Connexion du KMA au cluster

Cette option de menu permet au responsable de la sécurité de reconnecter le KMA au cluster après la modification de sa phrase de passe. Avant d'effectuer cette tâche :

1. Affichez KMS Manager.
2. Connectez-vous à un KMA existant en tant que responsable de la sécurité.
3. Localisez le panneau KMA List (Liste des KMA).
4. Créez une entrée de KMA.

Pour connecter le KMA au cluster :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `1`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent.

```
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. Connectez-vous à un KMA existant (par ex., 129.80.60.172) en tant que responsable de la sécurité.
3. À l'invite, tapez la phrase de passe initialement configurée pour le KMA afin de rejoindre le cluster, puis appuyez sur `<Entrée>`.

```
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. Saisissez le premier nom d'utilisateur de scission de clés établi lors de la procédure QuickStart pour le premier KMA via la fonction Modify Key Split Credentials (Modifier les références de scission de clés) de KMS Manager (voir « [Modification de la configuration de scissions de clé](#) », page 161).

---

**Remarque** – Le responsable de la sécurité doit connaître le nombre d'utilisateurs de scission de clés à saisir, c'est-à-dire, le seuil de scissions. Dans cet exemple, le seuil est défini sur 2.

---

5. Tapez la phrase de passe de l'utilisateur de la scission de clé, puis appuyez sur <Entrée>.

```
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. Indiquez le nom du deuxième utilisateur de la scission de clé.
7. Tapez la phrase de passe de l'utilisateur de la scission de clé, puis appuyez sur <Entrée>.

```
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. Appuyez sur <Entrée> en regard du troisième nom d'utilisateur de scission de clé afin de mettre un terme à l'autorisation des utilisateurs de scissions de clés.
9. Tapez **n**, puis appuyez sur <Entrée>.

## Définition de la phrase de passe d'un utilisateur

Cette option de menu permet à un responsable de la sécurité de définir la phrase de passe de tout utilisateur, y compris lui-même.

Pour définir la phrase de passe d'un utilisateur :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **2**, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent.

```
Set User's Passphrase
-----
Press Ctrl-c to abort.
Please enter the User Name:
```

2. À l'invite, saisissez le nom de l'utilisateur, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent.

```
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. À l'invite, tapez la phrase de passe, puis appuyez sur `<Entrée>`.
4. À l'invite `Please re-enter the desired Passphrase` (Ressaisissez la phrase de passe), tapez la même phrase de passe, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que la phrase de passe est définie. Appuyez sur `<Entrée>` pour revenir au menu principal.

```
Press Enter to continue:
```

## Définition des adresses IP du KMA

Cette option permet de modifier les paramètres d'adresse IP du KMA. Au départ, ces informations sont définies dans le programme QuickStart (voir « [Définition de l'adresse IP](#) », page 28), mais elles peuvent être modifiées ici.

Vous noterez que dans un grand cluster comptant plusieurs sites, les lecteurs peuvent être connectés à un jeu partiel des KMA du cluster. Cette mise en garde s'applique au jeu de KMA auquel un KMA peut se connecter.

---

**Attention** – Cette fonction doit être utilisée avec précaution. Si vous modifiez les informations relatives à un KMA, ce changement est immédiatement répercuté sur les autres KMA, à condition qu'ils soient connectés. Si le KMA est déconnecté, les autres seront mis à jour une fois qu'il sera reconnecté.

Toutefois, si par exemple vous disposez de deux KMA non connectés entre eux (suite à une panne de réseau) et que vous modifiez les deux adresses IP, ils ne pourront pas se reconnecter lorsque le réseau sera rétabli.

Dans ce cas, vous devez utiliser la fonction *Connexion du KMA au cluster* sur un KMA afin qu'il se reconnecte à l'autre en prenant soin de mettre à jour la phrase de passe au préalable. Par exemple, si les KMA A et B sont déconnectés et que vous modifiez les deux adresses IP, connectez-vous au KMA A et modifiez la phrase de passe du KMA B. Connectez-vous ensuite à la console du KMA B et utilisez la fonction *Connexion du KMA au cluster* afin de le relier au KMA A.

Manipulez également les lecteurs de bande avec précaution. Les lecteurs de bande ne reçoivent pas automatiquement les informations IP actualisées ; ils ne les obtiennent qu'au moment du montage d'un lecteur. Par conséquent, dans un environnement standard où les tâches des lecteurs sont effectuées de nuit et que vous modifiez les adresses IP des KMA de jour, les lecteurs ne pourront pas communiquer avec les KMA. Dans ce cas, ils doivent être réinscrits auprès du cluster KMS. Pour éviter cela, modifiez les adresses IP des KMA une après l'autre, attendez que tous les lecteurs de bande reçoivent la modification, puis passez au changement suivant.

---

Pour définir les adresses IP des KMA :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `3`, puis appuyez sur <Entrée>. Les paramètres actifs s'affichent

```
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. Saisissez le nom de l'hôte réseau de gestion dans le champ Management Network Hostname.
3. Tapez **n** ou **y** à l'invite Do you want to use DHCP to configure the Management Network interface (Voulez-vous utiliser le protocole DHCP pour configurer l'interface réseau de gestion ?). Si vous tapez **n**, passez à l'étape 4. Si vous choisissez **y**, passez à l'étape 6.
4. À l'invite, tapez l'adresse IP réseau de gestion, puis appuyez sur <Entrée>.
5. À l'invite Please enter the Management Network Subnet Mask: (Saisissez l'adresse du masque de sous-réseau), tapez l'adresse appropriée (par exemple, **255.255.254.0**), puis appuyez sur <Entrée>.
6. Indiquez le nom de l'hôte réseau de service dans le champ Service Network Hostname, puis appuyez sur <Entrée>.
7. Tapez **n** ou **y** à l'invite Do you want to use DHCP to configure the Service Network interface (Voulez-vous utiliser le protocole DHCP pour configurer l'interface réseau de service ?). Si vous tapez **n**, passez à l'étape 8. Si vous choisissez **y**, passez à l'étape 10.
8. À l'invite, tapez l'adresse IP réseau de service, puis appuyez sur <Entrée>.
9. À l'invite Please enter the Service Network Subnet Mask (Saisissez le masque de sous-réseau du réseau de service), tapez l'adresse du masque de sous-réseau appropriée (par exemple, **255.255.255.0**), puis appuyez sur <Entrée>.
10. Saisissez l'adresse IP de la passerelle dans le champ Gateway IP Address, puis appuyez sur <Entrée>.
11. À l'invite Please enter the Primary DNS Server IP Address (optional) (Saisissez l'adresse IP du serveur DNS principal (facultatif)), tapez une valeur, puis appuyez sur <Entrée>.
12. Indiquez le domaine DNS dans le champ DNS Domain, puis appuyez sur <Entrée>.
13. Tapez **y** en réponse à l'invite Are you sure that you want to commit these changes? [y/n]: (Voulez-vous vraiment valider ces modifications ?).

---

**Remarque** – Si, à un moment donné, l'utilisateur appuie sur les touches Ctrl+C, aucune modification n'est enregistrée et le menu principal s'affiche à l'écran. Les modifications sont uniquement acceptées après confirmation de l'opération par l'utilisateur via la saisie de **y** (oui) à l'invite finale. Après avoir confirmé l'opération, l'utilisateur revient au menu principal.

---

## Réinitialisation de l'état par défaut défini en usine du KMA

Cette option de menu permet à un responsable de la sécurité de réinitialiser le KMA sur son état par défaut défini en usine.

---

**Avertissement** – La réinitialisation est irrémédiable ; les informations contenues sur le KMA sont définitivement perdues suite à cette opération.

---

Il s'agit d'un processus destructeur aboutissant à la perte de toutes les données stockées sur le disque dur. Le système est forcé de redémarrer et les systèmes de fichiers sont reformatés et préparés à l'utilisation des nouvelles clés de chiffrement.

Pour réinitialiser le KMA sur son état par défaut défini en usine :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **4**, puis appuyez sur <Entrée>. Les informations suivantes s'affichent.

```
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:
```

---

**Avertissement** – Toutes les informations stockées sur ce KMA seront détruites. L'accès à l'ensemble des données protégées sera perdu à moins qu'une sauvegarde des données du KMA n'ait été créée au préalable ou que ses pairs du cluster soient présents.

---

2. À l'invite `Zeroize KMA before resetting` (Mettre à zéro le KMA avant la réinitialisation ?), tapez **n** ou **y**. Si vous tapez **y**, toutes les informations contenues sur le disque dur seront effacées de manière sécurisée.

---

**Remarque** – Cette opération prend environ quatre heures.

---

3. À l'invite `Type RESET to confirm` (Tapez RÉINITIALISER pour confirmer), tapez `RESET`, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que le KMA est en cours de réinitialisation.

Resetting...

4. Une fois l'authentification terminée, vous revenez à QuickStart. Reportez-vous à la section « [Exécution du programme QuickStart](#) », page 26.

## Activation du compte de support technique

L'option de menu Technical Support (Support technique) permet à un opérateur d'activer ou de désactiver le compte support du système d'exploitation et l'accès au shell sécurisé (SSH) correspondant. Par défaut, le compte du support technique comme l'accès SSH sont désactivés. Comme la phrase de passe associée au compte de support est uniquement connue du service de support Sun, l'activation de ce compte n'accorde pas d'accès supplémentaire au KMA à un utilisateur de la console.

1. Pour activer le compte de support technique :

À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `5`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que le compte de support est désactivé.

```
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. À l'invite, tapez `y` afin d'activer le compte, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que l'accès SSH est désactivé. L'activation de l'accès SSH permet au support technique de diagnostiquer un problème à distance.

```
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. À l'invite, tapez `y`, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant la fonction des clés hôte SSH.

```
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. À l'invite, tapez `y`, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, vous invitant à confirmer le changement.

```
Are you sure that you want to commit these changes? [y/n]:
```

5. À l'invite, tapez `y`, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que le compte est activé. Appuyez sur <Entrée> pour revenir au menu principal.

```
Press Enter to continue:
```

## Désactivation du compte de support technique

Pour désactiver le compte de support technique :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `5`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que le compte de support est activé.

```
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. À l'invite, tapez `y` afin de désactiver le compte, puis appuyez sur `<Entrée>`.
3. Les informations suivantes s'affichent, vous invitant à confirmer le changement.  
`Are you sure that you want to commit these changes? [y/n]:`
4. À l'invite, tapez `y`, puis appuyez sur `<Entrée>`. Le service SSH s'arrête automatiquement.

## Activation de l'administrateur principal

L'option de menu Primary Administrator vous permet d'activer ou de désactiver l'accès de l'administrateur principal sur le KMA.

- Pour activer l'accès de l'administrateur principal, commencez par activer le support technique (option 5).
- Cette tâche peut uniquement être *activée* par le responsable de la sécurité ; elle peut être *désactivée* par un opérateur ou un responsable de la sécurité.

---

**Attention** – La fonction d'administrateur principal permet à un utilisateur connecté en tant que personnel du support technique de disposer d'un accès d'administrateur principal (équivalent à l'accès root). Bien que dangereuse, cette procédure peut s'avérer nécessaire dans certaines situations afin de récupérer le système suite à un problème. Toutefois, vous pourrez avoir besoin d'une assistance directe du service de support ou du service d'ingénierie central.

---

1. Pour activer l'accès de l'administrateur principal :

À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **6**, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que l'accès est désactivé.

```

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. À l'invite, tapez **y** afin d'activer le compte, puis appuyez sur <Entrée>.

3. Les informations suivantes s'affichent, vous invitant à confirmer le changement.

```

Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]:

```

4. À l'invite, tapez **y**, puis appuyez sur <Entrée>. L'accès de l'administrateur principal a été activé.

## Désactivation de l'administrateur principal

L'option de menu Primary Administrator vous permet d'activer ou de désactiver l'accès de l'administrateur principal sur le KMA.

---

**Remarque** – Cette tâche peut uniquement être *activée* par le responsable de la sécurité ; elle peut être *désactivée* par un opérateur ou un responsable de la sécurité.

---

La désactivation de l'accès de l'administrateur principal entre en vigueur sur le champ. Si un utilisateur est connecté en tant qu'administrateur principal lorsque son accès est désactivé, la prochaine commande qu'il tente d'exécuter échoue.

1. Pour désactiver l'accès de l'administrateur principal :

À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **6**, puis appuyez sur <Entrée>. Les informations suivantes s'affichent, indiquant que l'accès est activé.

```
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. À l'invite, tapez **y** afin de désactiver le compte, puis appuyez sur <Entrée>.

3. Les informations suivantes s'affichent, vous invitant à confirmer le changement.

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. À l'invite, tapez **y**, puis appuyez sur <Entrée>. L'accès de l'administrateur principal a été désactivé.

## Définition de la disposition du clavier

Cette option vous permet de changer de disposition de clavier en passant de l'anglais (English) à une variété de langues.

---

**Remarque** – La disposition du clavier devrait correspondre à celle du clavier connecté au KMA afin que celui-ci puisse interpréter correctement les touches activées.

---

Pour définir la disposition du clavier :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `7`, puis appuyez sur `<Entrée>`. Les dispositions de clavier suivantes s'affichent.

```

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. À l'invite `Please enter the keyboard layout [ US-English ]` (Choisissez la disposition du clavier [Américain]), indiquez la langue voulue.
3. À l'invite, tapez `y`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que la modification a été effectuée. Appuyez sur `<Entrée>` pour revenir au menu principal.

```
The keyboard layout has been applied successfully.
```

```
Press Enter to continue:
```

## Déconnexion

Pour vous déconnecter de la session de console KMS active :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **0**, puis appuyez sur <Entrée>.
2. La session active prend fin et l'invite de connexion s'affiche, permettant à l'utilisateur d'accéder à nouveau à la console KMS.

## Fonctions associées aux autres rôles

Cette section décrit les fonctions pouvant être exécutées par les autres rôles (Compliance Officer, Backup Operator et Auditor). Il s'agit des tâches suivantes :

- Définition de la disposition du clavier
- Déconnexion du KMA

```
Key Management System Version xxx (col)
```

```
-----
```

```
(1) Set Keyboard Layout
```

```
(0) Logout
```

```
-----
```

```
Please enter your choice:
```

## Définition de la disposition du clavier

Cette option vous permet de changer de disposition de clavier en passant de l'anglais (English) à une variété de langues.

---

**Remarque** – La disposition du clavier devrait correspondre à celle du clavier connecté au KMA afin que celui-ci puisse interpréter correctement les touches activées.

---

Pour définir la disposition du clavier :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez `1`, puis appuyez sur `<Entrée>`. Les dispositions de clavier suivantes s'affichent.

```
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. À l'invite `Please enter the keyboard layout [ US-English ]` (Choisissez la disposition du clavier [Américain]), indiquez la langue voulue.
3. À l'invite, tapez `y`, puis appuyez sur `<Entrée>`. Les informations suivantes s'affichent, indiquant que la modification a été effectuée. Appuyez sur `<Entrée>` pour revenir au menu principal.

The keyboard layout has been applied successfully.

Press Enter to continue:

## Déconnexion

Pour vous déconnecter de la session de console KMS active :

1. À l'invite `Please enter your choice` (Indiquez votre choix) dans le menu principal, tapez **0**, puis appuyez sur <Entrée>.
2. La session active prend fin et l'invite de connexion s'affiche, permettant à l'utilisateur d'accéder à nouveau à la console KMS.



---

# Glossaire

---

---

## A

**AC** Voir Autorité de certification (AC).

**Accélérateur cryptographique** Périphérique matériel (carte) permettant d'augmenter la vitesse de chiffrement et de déchiffrement des données, optimisant ainsi les performances système dans les conditions de pics de demandes.

**Activé pour le chiffrement** Lecteur de bande doté d'une fonction de chiffrement ayant été activée.

**Adresse IP** Valeur de quatre octets permettant d'identifier un périphérique et de le rendre accessible par le biais d'un réseau. Les adresses IP suivent un format numérique de 32 bits écrit sous la forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. Exemple d'adresse IP possible : 129.80.145.23.  
Également appelée Adresse TCP/IP.

**Advanced Encryption Standard (AES)** Norme de chiffrement NIST approuvée par FIPS conçue pour protéger les données électroniques.

**AES** Voir Advanced Encryption Standard.

**Agent** Il est possible de créer différents types d'agents de chiffrement devant interagir avec le logiciel KMS afin de générer et d'obtenir des clés. Les modèles StorageTek T10000 A et B, T9840D de même que les lecteurs de bande HP LTO4 sont des types d'agents de chiffrement lorsqu'ils sont activés dans ce but.

**Algorithme de Rijndael** Algorithme sélectionné par le NIST (National Institute of Standards and Technology) aux États-Unis comme norme de chiffrement avancé (AES, Advanced Encryption Standard). Prononcé « rain-dahl », cet algorithme a été conçu par deux cryptologistes belges, Vincent Rijmen et Joan Daemen, dont les noms de famille composent l'intitulé du chiffrement.

**Algorithmes de hachage sécurisés (SHA)** Les algorithmes de hachage sécurisés sont des fonctions de hachage cryptographiques conçues par la NSA (National Security Agency, agence de sécurité nationale américaine) et publiées par le NIST comme norme de traitement des informations fédérales aux États-Unis.

## B

<b>API d'agent</b>	Voir API de bibliothèque d'agents.
<b>API de bibliothèque d'agents</b>	API fournie par la bibliothèque d'agents. Les agents appellent cette API.
<b>Audit</b>	Voir Journal d'audit.
<b>Auditor (Responsable des audits)</b>	Rôle de l'utilisateur habilité à afficher les pistes de vérification du système (événements de la liste d'audit et paramètres de sécurité du KMA).
<b>Autorité de certification (AC)</b>	Une autorité de certification enregistre les utilisateurs finaux, émet leurs certificats et peut également créer des AC sous-jacentes. Dans KMS 2.0, les KMA eux-mêmes agissent en tant qu'autorité de certification chargée d'émettre des certificats pour les utilisateurs, les agents et d'autres KMA.

---

## B

<b>Backup Operator (Opérateur des sauvegardes)</b>	Rôle de l'utilisateur chargé de la sécurisation et du stockage des données et des clés.
<b>Baie de jetons</b>	KMS version 1.x requise. Châssis hébergeant les jetons physiques et offrant l'alimentation et les connexions pour un ou deux jetons via le connecteur de branchement en aveugle arrière. La baie de jetons est compatible avec un rack de 19 pouces standard (de facteur de forme 1U). Elle est déclinée en deux styles : unité de bureau et montée en rack.
<b>Bibliothèque d'agents</b>	La bibliothèque d'agents est utilisée par un agent afin de récupérer des clés à partir d'une application KMS.
<b>BOT</b>	Beginning of Tape (début de la bande).

---

## C

<b>Certificat</b>	Document signé numériquement servant à valider l'autorisation et le nom de son détenteur. Ce document se compose d'un bloc de données d'un format spécial qui contient le nom du détenteur du certificat (DN, nom distinctif) du sujet, un numéro de série, les dates de validité, la clé publique du détenteur, le DN de l'émetteur et la signature numérique de l'émetteur à des fins d'authentification. L'émetteur atteste que le nom du détenteur correspond bien à celui associé à la clé publique contenue dans le document.
<b>Chiffrement</b>	Conversion des données en un code secret. Le chiffrement est l'une des méthodes de protection des données les plus efficaces. Pour lire un fichier chiffré, vous devez avoir accès à une clé ou un mot de passe spécial permettant de le déchiffrer.

- Clé** Dans ce contexte, il s'agit d'une clé de chiffrement de données symétrique. Les agents peuvent demander de nouvelles clés de chiffrement de données correspondant à une ou plusieurs unités de données. Une clé fait partie d'un groupe de clés unique de sorte que seuls les agents associés à ce groupe peuvent y accéder. Les clés sont dotées de durées de validité de chiffrement et de déchiffrement régies par la stratégie de clés associée au groupe de cette clé. Le type de la clé (c.-à-d., sa longueur et son algorithme) est défini par l'agent de chiffrement.
- Clé** Chaîne aléatoire de bits générée par le système de gestion des clés, saisie à partir du clavier ou achetée. Les types de clés disponibles sont les suivants :
- Les clés de périphérique permettent d'activer la fonction de chiffrement sur les lecteurs de bande.
  - Les clés de support permettent de chiffrer et de déchiffrer les données client sur une cartouche de bande.
  - Les clés de PC permettent de préparer les lecteurs de bande au chiffrement.
  - Les clés de communication ajoutent une couche de chiffrement (d'authentification) supplémentaire à la clé de support lors des transmissions effectuées entre le jeton et le lecteur par le biais du réseau local (LAN).
  - Les clés scindées sont spécifiques à chaque lecteur et fonctionnent de pair avec la clé d'habillage à des fins de protection.
  - Les clés d'habillage chiffrent la clé de support sur le LAN et le jeton.
- Clé d'activation** Clé unique composée de 64 caractères destinée à activer le lecteur de bande. Voir aussi Clé de PC.
- Clé d'écriture** Il s'agit d'une clé de support permettant d'écrire des données stockées sur une bande.
- Clé d'habillage** Chiffre les clés de support sur le LAN et sur le jeton.
- Clé de communication** Ajoute une couche supplémentaire de chiffrement et d'authentification lors des transmissions effectuées entre le jeton et le lecteur via un réseau local (LAN).
- Clé de lecture** Il s'agit d'une clé de support permettant de lire des données stockées sur une bande.
- Clé de PC** Permet au lecteur de bande de lire et d'écrire en mode chiffré.
- Clé de périphérique** Active la fonction de chiffrement sur le lecteur de bande. KMS version 1.x requise.
- Clé de support** Permet de chiffrer et de déchiffrer les données client sur une cartouche de bande.
- Cluster** Un cluster est un ensemble de dispositifs de gestion des clés (KMA) regroupés au sein d'un seul système en vue d'optimiser la tolérance de pannes, la disponibilité et l'évolutivité.
- Cluster KMS** Ensemble d'un ou de plusieurs KMA interconnectés. Tous les KMA faisant partie d'un cluster KMS doivent disposer des mêmes informations. Les seules exceptions à cette règle sont les suivantes : un KMS est hors service ou une nouvelle information n'a pas encore été diffusée à tous les KMA du cluster KMS. Une mesure prise au niveau de n'importe quel KMA du cluster KMS se propage systématiquement aux autres KMA du cluster KMS.

**Compliance Officer  
(Responsable de la  
conformité)**

Rôle de l'utilisateur chargé de gérer le flux de données à l'échelle de l'entreprise et habilité à définir et à déployer les contextes de données (groupes de clés) et les règles déterminant le mode de protection et, en dernier lieu, de destruction des données (stratégies de clés).

**Cryptographie**

Art de protéger des informations en les transformant (chiffrant) dans un format illisible appelé texte chiffré. Seules les personnes possédant une *clé* spéciale sont capables de déchiffrer (décrypter) le message en restituant sa forme initiale.

---

## D

**Durées de validité**

Laps de temps pendant lequel une clé peut servir à des fins de chiffrement. Cette période débute lorsque la clé est assignée au lecteur. Cette valeur correspond à la « période d'utilisation de l'initiateur » de la spécification NIST 800-57.

---

## E

**EKT** Enabling key token, activation du jeton de clé (clé de périphérique). KMS version 1.x requise.

---

## F

**Fichier de clé de  
sauvegarde**

Fichier généré au cours de l'opération de sauvegarde et contenant la clé utilisée pour chiffrer le fichier de sauvegarde. Ce fichier est chiffré au moyen de la clé principale du système. La clé principale est extraite du fichier de sauvegarde de sécurité principal à l'aide d'un quorum des références de scission de clés.

**Fichier de sauvegarde**

Fichier créé lors d'une opération de sauvegarde et contenant toutes les informations nécessaires à la restauration d'un KMA. Il est chiffré au moyen d'une clé générée tout particulièrement pour la sauvegarde. La clé est contenue dans le fichier de clé de sauvegarde correspondant.

**Fichier de transfert  
de clés**

Fichier contenant des clés et les unités de données associées (le cas échéant) utilisées pour déplacer des clés d'un cluster KMS vers un autre. Les deux parties du transfert doivent configurer un partenaire de transfert de clés correspondant à l'autre partie de l'opération. Le fichier de transfert de clés est signé et chiffré afin d'assurer à la fois la confidentialité et l'intégrité des informations transférées.

**Fin de tâche anormale**

**(abend)**

Problème logiciel ou matériel terminant une tâche en cours de traitement sur l'ordinateur.

**FIPS** Federal Information Processions Standards. L'institut national des normes et des technologies, le NIST (National Institute of Standards and Technology), est une agence fédérale américaine non réglementée faisant partie du service Technology Administration and Laboratories du Ministère du Commerce, lequel développe et fait la promotion des normes et des technologies, notamment :

- le CSRC (Computer Security Division and Resource Center) ;
- les normes FIPS (Federal Information Processing Standards).

Pour plus d'informations, rendez-vous sur :  
<http://www.nist.gov/>

---

## G

**Groupe de clés** Permet d'organiser les clés et de les associer à une stratégie. Les groupes de clés servent également à forcer l'accès aux clés des agents de chiffrement.

---

## H

**HMAC (Hash Message Authentication Code)**

En cryptographie, un code HMAC (Hash Message Authentication Code, code d'authentification d'une empreinte cryptographique de message avec clé) est un type de code d'authentification de message (MAC, Message Authentication Code) calculé à l'aide d'une fonction de hachage cryptographique associée à une clé secrète.

---

## I

**IG** Interface graphique.

**IP (Internet Protocol)** Protocole utilisé pour acheminer les données de leur source vers leur destination au sein d'un environnement Internet.

---

## J

**Jeton** KMS version 1.x requise.  
 Les jetons sont des périphériques de poche intelligents conçus pour se connecter à une baie de jetons au moyen d'une connexion Ethernet. Les deux rôles des jetons sont les suivants :

- Activation d'un jeton à clé
- Clé à jeton opérationnel

**Jeton de clé opérationnel** OKT (Operational Key Token) pour clés de support. KMS version 1.x requise.

**Journal d'audit** Le cluster KMS conserve un journal de tous les événements pouvant être audités qui surviennent en tout point du système. Les agents peuvent consigner des entrées dans ce journal afin d'enregistrer des événements à auditer.

---

## K

### Key Management System

**(KMS)** Système de gestion des clés. Le système Sun/StorageTek dispose d'un composant KMS permettant de gérer les clés au nom des agents de chiffrement.

### KMA (Key Management Appliance)

Dispositif de gestion des clés. Serveur Sun Fire X2100-M2 sur lequel le logiciel KMS 2.0 est préchargé. Il s'agit d'un processeur à deux noyaux éprouvé doté d'un système d'exploitation Solaris 10 proposant une gestion des clés basée sur les stratégies et des services de provisioning de clés.

**KMA** Voir Dispositif de gestion des clés.

**KMS** Voir Système de gestion des clés.

---

## L

**Lecteur de bande T10000** Le lecteur de bande T10000 est un modèle hautes performances, modulaire, de petit format, conçu pour stocker de gros volumes de données (jusqu'à 500 gigaoctets (Go) de données non compressées).

---

## M

**Mettre à zéro** Permet d'effacer des données stockées électroniquement, les clés de chiffrement et les paramètres de sécurité critiques en modifiant ou en supprimant le contenu de l'espace de stockage des données en vue d'empêcher la récupération de ces dernières.

---

## N

**NIST** National Institute of Standards and Technology (Institut national des normes et des technologies aux États-Unis).

### Numéro de série du

**volume** Étiquette alphanumérique de six caractères permettant d'identifier un volume de bande.

---

## O

**Operator (Opérateur)** Rôle de l'utilisateur chargé de la gestion des opérations quotidiennes effectuées sur le système.

---

## P

**Paramètre de sécurité critique** Informations de sécurité (clés cryptographiques secrètes et privées, données d'authentification telles que les mots de passe et les numéros d'identification personnelle PIN, par exemple) dont la divulgation ou la modification peuvent compromettre la sécurité d'un module cryptographique.

**Partage du secret de Shamir** En cryptographie, algorithme selon lequel un secret est divisé en plusieurs parties, donnant à chaque participant sa propre partie unique, et nécessitant une partie ou l'ensemble de ces éléments pour reconstituer le secret. Étant donné qu'il serait peu pratique de compter sur l'ensemble des participants pour combiner les différentes parties d'un secret, un quorum (ou schéma à seuil) est appliqué.

**Partenaire de transfert de clés** Le partenaire de transfert de clés désigne le destinataire des clés exportées d'un KMS vers un autre.

**Prêt pour le chiffrement** Lecteur de bande doté de la capacité de chiffrement de données et pouvant l'activer.

---

## R

**Réseau** Disposition de nœuds et de branches reliant entre eux des périphériques de traitement des données par le biais de liaisons logicielles et matérielles destinées à faciliter l'échange d'informations.

**RSA** En cryptographie, **RSA** est un algorithme de cryptographie à clé publique créé par Ron Rivest, Adi Shamir et Leonard Adleman à l'institut MIT aux États-Unis. Les lettres qui composent le nom de cet algorithme (**RSA**) sont les initiales des noms de ces cryptologistes.

---

## S

### **Security Officer (Responsable de la sécurité)**

Rôle de l'utilisateur chargé de gérer les paramètres de sécurité, les utilisateurs, les sites et les partenaires de transfert.

**Site** Attribut de chaque KMS et agent de chiffrement indiquant la proximité réseau ou la localité. Les agents de chiffrement doivent d'abord tenter de contacter un KMA situé sur le même site, puis un KMA d'un autre site en l'absence de réponse de la part d'un KMA du site local.

**Stratégie de clés** Fournit les paramètres des durées de validité applicables aux clés. Chaque groupe de clés dispose d'une stratégie de clés ; chaque stratégie de clés peut s'appliquer à aucun, à un ou à plusieurs groupes. Les durées de validité de chiffrement et de déchiffrement indiquées dans la stratégie limitent l'utilisation de clés et déclenchent des événements de cycle de vie des clés, tels que la désactivation ou la destruction de clés.

Les stratégies de clés contrôlent également les cibles d'exportation (autres partenaires de transfert) ou les sources d'importation (autres partenaires de transfert) des clés régies par la stratégie.

**Stratégie de sécurité** Déclaration rigoureuse de la sensibilité des données organisationnelles, des accès potentiels aux données et des règles régissant et contrôlant les accès.

---

## T

### **Transport Layer Security**

**(TLS)** Protocole de chiffrement assurant la sécurisation de communications via Internet lors d'opérations spécifiques : navigation Web, messagerie électronique, envoi de fax par Internet, messagerie instantanée et autres transferts de données.

---

## U

**UID** Chaîne servant d'identificateur unique pour une entité KMS, par ex., un agent de chiffrement ou un utilisateur.

### **Ultra Tape Drive Encryption Agent**

Logiciel utilisé par les lecteurs de bande de chiffrement compatibles Ultra 2.0 pour la gestion des clés. Ces lecteurs obtiennent les informations sur les clés auprès du KMS à utiliser avec les volumes de clés. Chaque opération d'écriture du début de la bande entraîne l'utilisation de nouvelles informations de clés pour le chiffrement des données sur le volume. Par conséquent, la définition d'une unité de données est mappée à un volume de bande avec l'ID externe de l'unité correspondant au numéro de série du volume.

**Unité de données** Entité abstraite au sein du KMS qui représente les objets de stockage associés aux stratégies du KMS et aux clés de chiffrement. La définition concrète d'une unité de données est fournie par l'agent de chiffrement qui la crée. Pour les lecteurs de bande, une unité de données correspond à une cartouche de bande.

**UTC** Coordinated Universal Time, temps universel.

---

## V

**Verrou autonome** Lorsque le déverrouillage autonome est activé, un quorum de responsables de la sécurité (Security Officer) est requis pour le déverrouillage d'un KMA verrouillé. Lorsque cette fonction est désactivée, le KMA peut être déverrouillé par n'importe quel responsable de la sécurité.

**Vidage système** Opération lancée par l'utilisateur entraînant la collecte de toutes les données pertinentes dans un fichier unique, lui-même téléchargé sur la machine de l'utilisateur. Une fois le téléchargement terminé, ce fichier est supprimé du KMA.



# Index

---

## A

Accélérateur de chiffrement, définition 297

Activation

Administrateur principal, console KMS 289

Compte de support technique, console KMS 272, 286

Activé pour le chiffrement, définition 297

Adjust System Time (régler l'heure système), menu 172

Administrateur principal, désactivation 274, 290

Adresse IP, définition 297

Advanced Encryption Standard (AES), définition 297

AES, définition 297

Affichage

Assignations de groupes de clés à des partenaires de transfert 208

Assignations de partenaires de transfert à des groupes de clés 212

Gestionnaires SNMP d'un KMA 114

Groupes de clés 187

Historique des fichiers de sauvegarde 256

Historique des sauvegardes 143

Informations détaillées sur les clés publiques de transfert 140

Informations détaillées sur un fichier de sauvegarde 146, 257

Journal d'audit 216

KMA 84

Liste de clés publiques de transfert 137

Liste des agents 228

Opérations 105

Références de scission de clés 159

Rôles 103

Sites 107

Stratégies de clés 176, 182

Unités de données 241

Utilisateurs 95

Affichage des détails

Agent 234

Gestionnaire SNMP 119

Groupe de clés 192

Journal d'audit 221

KMA 90

Site 112

Unité de données 245

Utilisateur 100

Agent Assignment to Key Groups (Assignation d'un agent à des groupes de clés), menu 194

Agent List (Liste des agents), menu 227

Agents

Affichage ou modification des détails d'un agent 234

Affichage, liste des agents 228

Assignation à un groupe de clés 196

Assignation d'un groupe de clés 203

Création 231

Définition 1, 297

Définition d'une phrase de passe 235

Suppression 236

Suppression d'un agent dans un groupe de clés 198

Suppression d'une groupe de clés 205

Aide en ligne, utilisation 13, 61

Aide, support technique xxvii

Algorithme de Rijndael, définition 297

Algorithmes de hachage sécurisés (SHA), définition 297

API de bibliothèque d'agents, définition 298

Appel de KMS Manager 54

Application d'une mise à niveau logicielle 252

Arrêt du KMA 271

Assignation

Agent à un groupe de clés 196

Groupe de clés à un agent 203

Groupe de clés à un partenaire de transfert 209

Partenaire de transfert à un groupe de clés 213

Assistance technique xxvii  
Audit Event List (Liste des événements d'audit),  
menu 216  
Auditor (Responsable des audits)  
Définition 298  
Description 13  
Opérations 263  
Rôle 263  
Autonomous Unlock Option (Option de  
déverrouillage autonome), menu 163  
Autorité de certification, définition 298

## B

Backup List (Liste des sauvegardes), menu 142, 255  
Backup Operator (Opérateur des sauvegardes)  
Définition 298  
Description 13  
Opérations 255  
Rôle 255  
Baie de jetons, définition 298  
Bibliothèque d'agents, définition 298  
Boutons de barre d'outils 60

## C

Centre des ressources client (CRC) xxvii  
Certificat, définition 298  
Chiffrement, définition 298  
Clé  
D'activation, définition 299  
D'écriture, définition 299  
D'habillage, définition 299  
De communication, définition 299  
De lecture, définition 299  
De PC, définition 299  
De périphérique, définition 299  
De support, définition 299  
Définition 299  
Destruction des clés post-opérationnelles 251  
Exportation et importation 124  
Importation à partir d'un fichier de transfert de  
clés 238  
Clés post-opérationnelles, destruction 251  
Clés publiques de transfert  
Affichage de la liste 137  
Affichage des informations détaillées 140  
Création 141  
Cluster  
Connexion 71  
Définition 1, 299  
Intégration, programme QuickStart 38  
KMS, définition 299  
Rétablissement de la connexion du KMA 278

Compliance Officer (Responsable de la conformité)  
Définition 300  
Description 13  
Opérations 173  
Rôle 174  
Compte du support technique  
Activation 272  
Désactivation 273  
Configuration  
Cluster, programme QuickStart 31  
Définition des paramètres 77  
Logicielle requise, KMS 13  
Partenaires de transfert de clés 122  
Confirmation d'une destruction de fichier de  
sauvegarde 260  
Connexion  
À KMS 71  
Au dispositif de gestion des clés 266  
Distante à la console, ELOM 20  
Console KMS  
Auditor (Responsable des audits), options 269  
Backup Operator (Opérateur des sauvegardes),  
options 269  
Compliance Officer (Responsable de la  
conformité), options 269  
Description 265  
Fonctions associées aux autres rôles  
Déconnexion 295  
Définition de la disposition du clavier 294  
Fonctions de l'opérateur  
Activation du compte de support technique 272  
Arrêt du KMA 271  
Déconnexion 276  
Définition de la disposition du clavier 275  
Désactivation de l'administrateur principal 274  
Désactivation du compte de support  
technique 273  
Redémarrage du KMA 271  
Fonctions du responsable de la sécurité  
Activation de l'administrateur principal 289  
Activation du compte de support technique 286  
Déconnexion 292  
Définition de la disposition du clavier 291  
Définition de la phrase de passe d'un  
utilisateur 280  
Définition des adresses IP du KMA 281  
Désactivation de l'administrateur principal 290  
Désactivation du compte de support  
technique 288  
Réinitialisation de l'état par défaut défini en  
usine du KMA 284  
Rétablissement de la connexion du KMA au  
cluster 278  
Options pour l'opérateur 267  
Security Officer (Responsable de la sécurité),  
options 268

- Utilisation 265
- Console, connexion distante (ELOM) 20
- Contact du support Sun Microsystems pour StorageTek xxviii
- Conventions typographiques xxxi
- Core Security (Sécurité principale), menu 156
- Création
  - Agent 231
  - Clé publique de transfert 141
  - Fichier de sauvegarde 259
  - Gestionnaire SNMP 117
  - Groupe de clés 190
  - KMA 87
  - Partenaire de transfert 130
  - Profil de cluster 71
  - Sauvegarde de sécurité principale 157
  - Site 110
  - Stratégie de clés 180
  - Utilisateur 98
  - Vidage système 150
- Cryptographie, définition 300

## D

- Data Unit List (Liste des unités de données), menu 240
- Déconnexion
  - KMA 75
  - Session de console KMS 276, 292, 295
- Définition adresse IP
  - KMA, console KMS 281
  - Programme QuickStart 28
- Définition de la disposition du clavier 275
  - Console KMS 275, 291, 294
- Définition de la phrase de passe
  - Agent 235
  - KMA 92
  - Utilisateur 101
  - Utilisateur, console KMS 280
- Démarrage
  - KMA, programme QuickStart 30
  - KMS Manager 54
  - Programme QuickStart 27
- Dépannage xxvii
- Désactivation
  - Administrateur principal, console KMS 274, 290
  - Compte de support technique, console KMS 273, 288
- Destruction des clés post-opérationnelles 251
- Détails d'un utilisateur, affichage ou modification 100
- Déverrouillage
  - Autonome, option à utiliser avec précaution 36
  - KMA 166
  - Sécurité principale du KMA 167

- Dimensions, lecteur de bande T10000 302
- Disposition du clavier, définition 275
- Durées de validité 300

## E

- EKT (Enabling Key Token), définition 300
- ELOM *Voir* Embedded Lights Out Manager
- Embedded Lights Out Manager (ELOM)
  - Connexion via ELOM 20
  - Utilisation d'une connexion réseau 22
- États et transitions disponibles dans KMS 6
- Exportation
  - Clés 124
  - Clés, importation d'un fichier KMS 1.0 215
  - Journal d'audit 222

## F

- Fichier
  - Clé de sauvegarde, définition 300
  - Sauvegarde, définition 300
  - Transfert de clés, définition 300
- Fin de tâche anormale (abend), définition 300
- FIPS (Federal Information Processions Standards), définition 301
- Fonctions associées aux autres rôles
  - Déconnexion 295
  - Définition de la disposition du clavier 294
- Fonctions de l'opérateur
  - Activation du compte de support technique 272
  - Arrêt du KMA 271
  - Déconnexion de la session de console KMS 276
  - Définition de la disposition du clavier 275
  - Désactivation de l'administrateur principal 274
  - Désactivation du compte de support technique 273
  - Redémarrage du KMA, console KMS 271
- Fonctions du responsable de la sécurité
  - Activation de l'administrateur principal 289
  - Activation du compte de support technique 286
  - Définition de la disposition du clavier 291
  - Définition de la phrase de passe d'un utilisateur 280
  - Définition des adresses IP du KMA 281
  - Désactivation de l'administrateur principal 290
  - Désactivation du compte de support technique 288
  - Réinitialisation de l'état par défaut défini en usine du KMA 284
  - Rétablissement de la connexion du KMA au cluster 278

## G

- Gestionnaire SNMP
  - Affichage ou modification des détails 119
  - Affichage pour un KMA 114
  - Création 117
  - Suppression 120
- Glossaire 297
- Groupes de clés
  - Affichage 187
  - Affichage des assignations de groupes de clés à des partenaires de transfert 208
  - Affichage des partenaires de transfert assignés 212
  - Affichage ou modification des détails 192
  - Assignation à un agent 203
  - Assignation à un partenaire de transfert 209
  - Assignation d'un partenaire de transfert 211
  - Assignation d'un agent 196
  - Assignation d'un partenaire de transfert 213
  - Création 190
  - Définition 184, 301
  - Suppression 193
  - Suppression d'un agent 198
  - Suppression d'un partenaire de transfert 210, 214
  - Suppression pour un agent 205

## H

- Heure système, récupération 170
- HMAC (Hash Message Authentication Code), définition 301
- Horloge
  - Locale, réglage 172
  - Réglage de l'horloge locale 172

## I

- IG (interface graphique), définition 301
- Import Keys (Importer des clés), menu 238
- Importation
  - Clés 124
  - Fichier d'exportation de clés KMS 1.0 215
- Initialisation du KMA, programme QuickStart 30
- Intégration à un cluster existant, programme QuickStart 38
- IP (Internet Protocol), définition 301

## J

- Jeton
  - Clé opérationnel, définition 301
  - Définition 301
- Journal d'audit
  - Affichage 216
  - Affichage des informations détaillées 221
  - Définition 302
  - Exportation 222

## K

- Key Group Assignment to Agents (Assignation d'un groupe de clés à un agent), menu 200
- Key Group Assignment to Transfer Partners (Assignation d'un groupe de clés à un partenaire de transfert), menu 207
- Key Group List (Liste des groupes de clés), menu 186
- Key Groups (Groupes de clés), menu 186, 226
- Key Management System (KMS)
  - Appel de KMS Manager
    - Solaris, démarrage 54
    - Windows, démarrage 54
  - Cluster, définition 1
  - Concepts
    - Agents 2
    - Clusters KMS 2
    - Configuration initiale, connexion directe ou console distante 3
    - Configuration initiale, programme QuickStart 4
    - Connexions réseau 2
    - Cycle de vie des clés 4
    - KMS, états et transitions 6
    - Transition d'état 5
    - Unités de données, clés, groupes de clés et stratégies de clés 10
    - Utilisateurs et contrôle d'accès basé sur les rôles 9
  - Déploiement réseau standard 12
  - Description 47
  - États
    - Actif 6
    - Compromis 7
    - Désactivé 7
    - Destroyed and Compromised (Détruit et compromis) 8
    - Détruit 7
    - Préactivation 6
  - Installation 48
  - Introduction 1
  - Rôles d'utilisateur 13
- Key Policy List (Liste des stratégies de clés), menu 175

- Key Split Configuration (Configuration de scissions de clé), menu 159
- KMA (Key Management Appliance)
  - Affichage 84
  - Affichage des gestionnaires SNMP 114
  - Affichage ou modification des détails 90
  - Arrêt 271
  - Configuration et gestion 18
  - Connexion 20, 266
  - Création 87
  - Déconnexion 75
  - Définition 1, 302
  - Définition d'une phrase de passe 92
  - Définition des adresses IP 281
  - Déverrouillage de la sécurité principale 167
  - Redémarrage 271
  - Réglage de l'horloge locale 172
  - Réinitialisation de l'état par défaut défini en usine 284
  - Rétablissement de la connexion au cluster 278
  - Suppression 93
  - TCP/IP, connexions 11
  - Verrouillage de la sécurité principale du KMA 166
  - Verrouillage ou déverrouillage de la sécurité principale 166
- KMA *Voir* Dispositif de gestion des clés
- KMS (Key Management System)
  - Définition 302
- KMS Manager
  - Barre d'état 65
  - Configuration logicielle requise 13
  - Connexion au cluster KMS 71
  - Création d'un profil de cluster 71
- IG
  - Barre d'outils, boutons 60
  - Définition 1
  - Menu Help (Aide) 58
  - Présentation 55
  - Raccourcis clavier 60
  - System (Système), menu 56
  - Touches d'accès rapide aux menus 60
- Modification de la phrase de passe 76
- Paramètres de configuration 77
- Quitter 79
- Suppression d'un profil de cluster 75
- Utilisation de l'aide en ligne 61
- Utilisation du menu System (Système) 71
- View (Affichage), menu 57
- Volet de l'arborescence des opérations 62
- Volet des détails des opérations 63
- Volet du journal d'audit des sessions 64
- Volets de l'IG 62
- KMS *Voir* Système de gestion des clés

## L

- Lecteur de bande T10000
  - Définition 302
  - Description 302
  - Taille 302
- Liste des clés publiques de transfert de clés, menu 137
- Local Configuration (Configuration locale), menu 165
- Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA), menu 166
- Logiciel, téléchargement et application d'une mise à niveau 252

## M

- Maintenance demandée par le client (CIM) xxviii
- Menu
  - Adjust System Time (Régler l'heure système) 172
  - Agent Assignment to Key Groups (Assignment d'un agent à des groupes de clés) 194
  - Agent List (Liste des agents) 227
  - Audit Event List (Liste des événements d'audit) 216
  - Autonomous Unlock (Déverrouillage autonome) 163
  - Backup List (Liste des sauvegardes) 142, 255
  - Core Security (Sécurité principale) 156
  - Data Unit List (Liste des unités de données) 240
  - Groupes de clés 186
  - Help (Aide) 58
  - Import Keys (Importer des clés) 238
  - Key Group Assignment to Agents (Assignment d'un groupe de clés à un agent) 200
  - Key Group Assignment to Transfer Partners (Assignment d'un groupe de clés à un partenaire de transfert) 207
  - Key Group List (Liste des groupes de clés) 186
  - Key Groups (Groupes de clé) 226
  - Key Policy List (Liste des stratégies de clés) 175
  - Key Split Configuration (Configuration de scissions de clé) 159
  - Key Transfer Public Key List (Liste des clés publiques de transfert) 137
  - KMA List (Liste des KMA) 83
  - Local Configuration (Configuration locale) 165
  - Lock/Unlock KMA (Verrouiller/Déverrouiller le KMA) 166
  - Paramètres de sécurité 152
  - Role List (Liste des rôles) 103
  - Site List (Liste des sites) 106
  - SNMP Manager List (Liste des gestionnaires SNMP) 114

- Software Upgrade (Mise à niveau du logiciel) 252
- System (Système) 56, 71
- System (Système), utilisation 71
- System Time (Heure système) 170
- Transfer Partner Assignment to Key Groups (Assignation d'un partenaire de transfert à des groupes de clés) 211
- Transfer Partners (Partenaires de transfert) 125
- Transfer Partners List (Liste des partenaires de transfert) 126
- User List (Liste des utilisateurs) 94
- Vidage système 150
- View (Affichage) 57
- Mettre à zéro
  - Définition 302
  - Réinitialisation de l'état par défaut défini en usine du KMA 284
- Modification
  - Paramètres de sécurité 154
  - Phrase de passe 76
  - Références de scission de clés 161
  - Stratégie de clés 182
- Modification détails
  - Agent 234
  - Gestionnaire SNMP 119
  - Groupe de clés 192
  - KMA 90
  - Site 112
  - Unité de données 245
  - Utilisateur 100

## N

- NIST, définition 302
- Numéro de série du volume, définition 302

## O

- Opérateur, définition 303
- Opération basée sur le rôle 14
- Operator (Opérateur)
  - Description 13
  - Opérations 225
  - Rôle 225

## P

- Paramètres de configuration 77
- Paramètres de sécurité
  - Critique, définition 303
  - Modification 154
  - Récupération 152

- Partage de clés, présentation 121
- Partage du secret de Shamir, définition 303
- Partenaires de transfert de clés
  - Configuration 122
  - Définition 303
  - Description de la fonction 121
- Partenaires, site Web de SUN xxvi
- Phrase de passe
  - Définition 101
  - Définition pour un KMA 92
  - Définition pour un utilisateur 280
  - Modification 76
  - Utilisateur, définition 101
- Préface xxv
- Préférence de déverrouillage autonome, programme QuickStart 36
- Prêt pour le chiffrement, définition 303
- Profil de cluster
  - Création 71
  - Suppression 75
- Public cible xxv

## Q

- QuickStart, programme
  - Configuration du cluster 31
  - Définition de l'adresse IP 28
  - Démarrage 27
  - Exécution 26
  - Initialisation du KMA 30
  - Intégration à un cluster existant 38
  - Préférence de déverrouillage autonome 36
  - Références initiales de l'utilisateur responsable de la sécurité 35
  - Restauration d'un cluster à partir d'une sauvegarde 41
  - Saisie des références de scission de clés 32
  - Synchronisation horaire des KMA 37
- Quitter KMS Manager 79

## R

- Raccourcis clavier 60
- Récupération
  - Heure système 170
  - Paramètres de sécurité 152
- Redémarrage du KMA, console KMS 271
- Références de scission de clés
  - Affichage 159
  - Modification 161
  - Programme QuickStart 32
- Références initiales de l'utilisateur responsable de la sécurité, programme QuickStart 35

- Réinitialisation de l'état par défaut défini en usine du KMA 284
  - Console KMS 284
- Réseau, définition 303
- Restauration
  - Cluster à partir d'une sauvegarde, programme Quickstart 41
  - Sauvegarde 148
- Rétablissement de la connexion du KMA au cluster, console KMS 278
- Role List (Liste des rôles), menu 103
- Rôles
  - Affichage 103
  - Affichage des opérations associées 105
  - Key Management System 13
  - Requis pour effectuer une opération 14
- RSA, définition 303

## S

- Sauvegarde de la sécurité principale 157
- Sauvegarde, fichiers
  - Affichage de l'historique 143, 256
  - Affichage des informations détaillées 146, 257
  - Confirmation de destruction 260
  - Création 259
  - Restauration 148
- Sécurité principale
  - Création d'une sauvegarde 157
  - Description 155
- Security Officer (Responsable de la sécurité)
  - Définition 304
  - Description 13
  - Opérations 81
  - Rôle 82
- Security Parameters (Paramètres de sécurité), menu 152
- Sièges internationaux de SUN xxix
- Site
  - Affichage 107
  - Affichage ou modification des détails 112
  - Création 110
  - Définition 304
  - Suppression 113
  - Web de SUN xxvi
- Site List (Liste des sites), menu 106
- SNMP Manager List (Liste des gestionnaires SNMP), menu 114
- Software Upgrade (Mise à niveau du logiciel), menu 252
- Stratégie de sécurité, définition 304
- Stratégies de clés
  - Affichage 176, 182
  - Création 180

- Définition 304
- Description 175
- Modification 182
- Suppression 183
- Support
  - Client xxvii
  - Technique xxvii
- Suppression
  - Agent 236
  - Agent dans un groupe de clés 198
  - Gestionnaire SNMP 120
  - Groupe de clés 193
  - Groupe de clés d'un partenaire de transfert 210
  - Groupe de clés pour un agent 205
  - KMA 93
  - Partenaire de transfert d'un groupe de clés 214
  - Profil de cluster 75
  - Site 113
  - Stratégie de clés 183
  - Utilisateur 102
- Synchronisation horaire des KMA, programme QuickStart 37
- System Dump (Vidage système), menu 150
- System Time (Heure système), menu 170

## T

- Taille du lecteur de bande 302
- Téléchargement d'une mise à niveau logicielle 252
- Touches d'accès rapide aux menus 60
- Transfer Partner Assignment to Key Groups ((Assignation d'un partenaire de transfert à des groupes de clés), menu 211
- Transfer Partners (Partenaires de transfert)
  - Affichage des assignations à des groupes de clés 212
  - Affichage des assignations de groupes de clés 208
  - Affichage et modification des détails 133
  - Assignation à un groupe de clés 211, 213
  - Assignation d'un groupe de clés 207, 209
  - Création 130
  - Importation des clés et d'unités de données à partir d'un fichier de transfert 238
  - Liste 126
  - Suppression 136
  - Suppression d'un groupe de clés 210, 214
- Transfer Partners (Partenaires de transfert), menu 125
- Transfert de clés
  - Présentation 121
  - Processus 122
- Transport Layer Security (TLS), définition 304

## U

- UID, définition 304
- Ultra Tape Drive Encryption Agent, définition 304
- Unités de données
  - Affichage 241
  - Affichage des informations détaillées 245
  - Définition 305
  - Description 240
  - Destruction des clés post-opérationnelles 251
  - Modification des détails 245
- User List (Liste des utilisateurs), menu 94
- UTC, définition 305
- Utilisateur
  - Affichage 95
  - Création 98
  - Rôles dans Key Management System 13
  - Suppression 102
- Utilisation
  - Aide en ligne 61
  - Console KMS 265
  - Menu System (Système) 71

## V

- Verrou autonome, définition 305
- Verrouillage
  - KMA 166
  - Sécurité principale du KMA 166
- Vidage système
  - Création 150
  - Définition 305