Oracle Key Manager

Administration Guide

Version 2.3

November 2010
Revision AA

Submit comments about this document by clicking the Feedback [+] link at: http://docs.sun.com

Oracle Key Manager (OKM) Administration Guide

Copyright ©2007, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Please
Recycle

Revision History

Date	Revision	Description
November, 2010	AA	*Oracle Key Manager 2.3 Administration Guide*

Contents

Revision History iii

Contents v

Figures xv

Tables xvii

What's New? xix

Preface xxi

1. Introduction 1

Overview 1

OKM Concepts 2

OKM Clusters 2

Agents 2

Network Connections 2

Initial Setup - Direct Connection or Remote Console 3

Initial Setup - QuickStart Program 4

Key Lifecycle 4

State Transition 5

OKM Key States and Transitions 6

Pre-activation 6

Active 6

Deactivated 7

Compromised 7

Destroyed/Destroyed Compromised 7
Users and Role-based Access Control 9
Allowed Operations for Each Role 9
Quorum Protection 9
Data Units, Keys, Key Groups, and Key Policies 10
TCP/IP Connections and the KMA 11
OKM in the Network 13
OKM Manager Software Requirements 14
Using Online Help 14
Role-Based Access Control 14
Role-Based Operations 15
Setting Up and Managing the Key Management Appliance 20

2. Getting Started 21

Accessing the KMA Through the Service Processor 22
Connecting to the KMA 22
Using a Network Connection - ELOM 24
Using a Network Connection - ILOM 27
Launching the OKM Console 30
Running the QuickStart Program 31
Starting QuickStart 32
Specifying the Network Configuration 33
Initializing the KMA 39
Configuring the Cluster 39
Entering Key Split Credentials 40
Entering Initial Security Officer User Credentials 42
Specifying the Autonomous Unlocking Preference 43
Setting the Key Pool Size 44
Synchronizing KMA Time 45
Joining an Existing Cluster 46
Restoring a Cluster From a Backup 52
Adding Agents and Enrolling Tape Drives 59

3. Using the OKM Manager 61

What is the OKM Manager? 61
Installing the OKM Manager Software 62
Starting the OKM Installation 63
Invoking the OKM Manager 70
Starting the OKM Manager with Windows 70
Starting the OKM Manager with Solaris 70
OKM Manager GUI Overview 71
System Menu 72
View Menu 73
Help Menu 74
Toolbar Buttons 76
Shortcut Keys 76
Menu Accelerator Keys 76
Using Online Help 77
OKM Manager GUI Panes 78
OKM Management Operations Tree Pane 78
OKM Management Operation Details Pane 79
Session Audit Log Pane 80
Status Bar 81
Panels 82
Uninstalling the OKM Manager Software 84
Invoking the Executable File 84
Invoking Add/Remove Programs (Windows Only) 84
Completing the Uninstall Process 85

4. Using the System Menu 87
Connecting to the Cluster 87
Creating a Cluster Profile 87
Deleting a Cluster Profile 91
Disconnecting from the KMA 91
Changing the Passphrase 92
Saving Certificates 93
Converting PKCS12 Format to PEM Format 95
Specifying the Configuration Settings 96

IPv6 Addresses with Zone IDs 98
Exiting from the OKM Manager 100

5. Security Officer Operations 101

Security Officer Role 102
KMA List Menu 103
Viewing KMAs 104
Checking the SCA 6000 Card 107
Creating a KMA 109
Viewing/Modifying a KMA's Details 112
Setting a KMA Passphrase 115
Deleting a KMA 117
User List Menu 118
Viewing Users 119
Creating a User 122
Viewing/Modifying a User's Details 125
Setting a User's Passphrase 128
Deleting Users 130
Role List Menu 131
Viewing Roles 132
Viewing Operations for a Role 134
Site List Menu 135
Viewing Sites 136
Creating a Site 139
Viewing/Modifying a Site's Details 141
Deleting a Site 142
SNMP Manager List Menu 143
Viewing a KMA's SNMP Managers 144
Creating a New SNMP Manager 147
Viewing/Modifying an SNMP Manager's Details 149
Deleting an SNMP Manager 150
Key Transfer 151
Overview 151
Key Transfer Partners Feature 151

Key Transfer Process 152
Configuring Key Transfer Partners 152
Exporting/Importing Keys 154
Transfer Partners Menu 156
Transfer Partner List Menu 157
Creating a Transfer Partner 161
Viewing/Modifying Transfer Partner Details 165
Deleting a Transfer Partner 169
Key Transfer Public Key List Menu 170
Viewing the Key Transfer Public Key List 171
Viewing the Key Transfer Public Key Details 174
Creating a Key Transfer Public Key 175
Backup List Menu 176
Viewing Backup Files History 177
Viewing Backup Details 180
Restoring a Backup 182
System Dump Menu 186
Creating a System Dump 187
Security Parameters Menu 188
Retrieving the Security Parameters 189
Modifying the Security Parameters 192
Core Security 193
Core Security Management Menu 194
Backup Core Security 195
Creating a Core Security Backup 195
Key Split Configuration 197
Viewing the Key Split Configuration 197
Modifying the Key Split Configuration 198
Autonomous Unlock Option 201
Local Configuration Menu 203
Lock/Unlock KMA 204
Locking the KMA 204
Unlocking the KMA 205

Network Configuration Information 208
Displaying the Network Configuration 208
System Time Menu 210
Retrieving the Local Clock Information 211
Adjusting the KMA's Local Clock 212

6. Compliance Officer Operations 213

Compliance Officer Role 213
Key Policies 214
Key Policy List Menu 214
Viewing Key Policies 214
Creating a Key Policy 218
Viewing/Modifying a Key Policy 220
Deleting a Key Policy 221
Key Groups 222
Key Groups Menu 224
Key Group List Menu 224
Viewing Key Groups 225
Creating a Key Group 228
Viewing/Modifying a Key Group's Details 230
Deleting a Key Group 231
Agent Assignment to Key Groups Menu 232
Assigning an Agent to a Key Group 234
Removing an Agent from a Key Group 236
Key Group Assignment to Agents Menu 238
Assigning a Key Group to an Agent 241
Removing a Key Group from an Agent 243
Key Group Assignment to Transfer Partners Menu 245
Viewing Key Group Assignments 246
Adding a Key Group to a Transfer Partner 247
Removing a Key Group from a Transfer Partner 248
Transfer Partner Assignment to Key Groups Menu 249
Viewing Transfer Group Assignments 250
Adding a Transfer Partner to a Key Group 251

Removing a Transfer Partner from a Key Group 252
Importing a KMS 1.0 Key Export File 253
Audit Event List Menu 255
Viewing Audit Logs 256
Viewing Audit Log Details 261
Exporting an Audit Log 262
Data Unit List Menu 262
Compromising Keys 262
Other Functions 265

7. Operator Operations 267

Operator Role 267
Key Groups Menu 268
Key Group List 268
Agent Assignment to Key Groups 268
Transfer Partner Assignment to Key Groups 268
Agent List Menu 269
Viewing the Agent List 270
Creating an Agent 273
Viewing/Modifying an Agent 276
Setting an Agent's Passphrase 277
Deleting Agents 278
Key Group Assignment to Agents Menu 279
Import Keys Menu 280
Data Units 282
Data Unit List Menu 282
Viewing Data Units 283
Viewing/Modifying Data Unit Details 287
Destroying Post-operational Keys 293
Software Upgrade Menu 294
Guidelines for Performing Software Upgrades 294
Uploading and Applying Software Upgrades 295
Backup List Menu 299
Audit Event List Menu 299

KMA List Menu 299
Site List Menu 299
SNMP Manager List Menu 299
System Time Menu 299
Lock/Unlock KMA Menu 299

8. Backup Operator Operations 301

Backup Operator Role 301
Backup List Menu 301
Viewing Backup Files History 302
Viewing Backup Details 303
Creating a Backup 305
Confirming a Backup's Destruction 306
KMA List Menu 307
Modifying a Key Pool Size 307
Other Functions 309

9. Auditor Operations 311

Auditor Role 311
Audit List Menu 311
Security Parameters Menu 311
Other Functions 312

10. Quorum Member Operations 313

Quorum Member Role 313
Pending Quorum Operation List Menu 314
Viewing Pending Operations Details 317
Approving Pending Quorum Operations 318
Deleting Pending Quorum Operations 320
Related Operations 321

11. Using the OKM Console 323

What is the OKM Console? 323
Logging into the KMA 324
Operator 325

Security Officer 326
Other Roles 327
Operator Role Functions 328
Rebooting the KMA 329
Shutting Down the KMA 329
Disabling the Technical Support Account 330
Disabling the Primary Administrator 331
Setting the Keyboard Layout 332
Logging Out 333
Security Officer Role Functions 334
Logging the KMA Back into the Cluster 335
Setting a User's Passphrase 337
Setting the KMA Management IP Address 339
Setting the KMA Service IP Addresses 341
Viewing/Adding/Deleting Gateways 343
Specifying the DNS Settings 345
Resetting the KMA to the Factory Default 346
Enabling the Technical Support Account 348
Disabling the Technical Support Account 350
Enabling the Primary Administrator 351
Disabling the Primary Administrator 353
Setting the Keyboard Layout 354
Logging Out 355
Other Role Functions 356
Setting the Keyboard Layout 357
Logging Out 358

12. Command Line Utilities 359

OKM Command Line Utility 360
Solaris/Windows Syntax 361
Parameter Descriptions 363
Examples 370
Exit Values 375
Sample Perl Scripts 375

Backup Command Line Utility 377

Solaris Syntax 377

Windows Syntax 377

Parameter Descriptions 377

Example 378

A. SNMP Management Information Base (MIB) Data 379

Glossary 381

Index 389

Figures

FIGURE 1-1 Connections to the KMA 3

FIGURE 1-2 Key Lifecycle Periods 4

FIGURE 1-3 State Transition Diagram 5

FIGURE 1-4 Typical Deployment of OKM Solution 13

FIGURE 2-1 Embedded Lights Out Manager Login Screen 24

FIGURE 2-2 Power Control 25

FIGURE 2-3 Launch Redirection (ELOM) 26

FIGURE 2-4 Integrated Lights Out Manager Login Screen 27

FIGURE 2-5 Power Control 28

FIGURE 2-6 Launch Redirection (ILOM) 29

FIGURE 2-7 Remote Console 30

FIGURE 6-1 Key Group Relationship with Key Policies, Agents, Data Units 223

Tables

TABLE 1-1 KMA Port Connections 11

TABLE 1-2 Other Services 11

TABLE 1-3 System Operations/User Roles 15

TABLE 2-1 Supported ELOM Compatible Web Browsers and Java Versions 22

TABLE 2-2 Supported ILOM Compatible Web Browsers and Java Versions 23

TABLE 5-1 Export Format Settings 154

TABLE 12-1 OKM Command Line Utility - User Role Access 360

TABLE A-1 KMA Object Identifiers 379

What's New?

OKM Release 2.3 includes the following enhancements, updates, and clarifications:

Revision AA:

Enhancement/Update	Primary Location
The product name, Key Management System (KMS), has been renamed to Oracle Key Manager (OKM). References to the KMS and most of its components and concepts have been changed accordingly.	Whole document.
The Oracle Key Manager GUI and command line utilities are now supported on a Microsoft® Windows 7 and Windows 2008 server.	"OKM Manager Software Requirements" on page 14.
The KMA can be accessed through a separate service processor, the Integrated Lights Out Manager (ILOM), which manages and monitors servers. KMAs are now manufactured on Sun Fire X4170 M2 servers and use an ILOM instead of an ELOM. Sun Fire X2100 or X2200 KMAs can be upgraded to run OKM 2.3.	"Accessing the KMA Through the Service Processor" on page 22 and "Using a Network Connection - ILOM" on page 27.
When you enter Key Split Credentials in the QuickStart program, note two additional requirements: ■ The Key Split Threshold must be less than or equal to the Key Split Size. ■ Key split user names should be different from KMA user names.	"Entering Key Split Credentials" on page 40.
The new KMA can join the Cluster without downgrading to an earlier release if the new KMA runs OKM 2.3 and the existing KMA runs an earlier KMS release.	"Joining an Existing Cluster" on page 46.
You can specify to accelerate your initial updates after you successfully join an existing Cluster. The KMA joining the Cluster identifies another KMA that has the largest cached backup in this Cluster, downloads that backup, and applies it to its local database. This process is the equivalent of replicating the data but at a much faster rate.	Step 9 on page 49 in "Joining an Existing Cluster".
After you set up the KMA, you can add agents and enroll tape drives to use that KMA; however, you must assign the Key Group as the default or the drive cannot write. If you do not specify a default, the drive is read-only for the assigned group(s).	"Adding Agents and Enrolling Tape Drives" on page 59.

Revision AA:

Enhancement/Update	Primary Location
You must uninstall any previous OKM Manager version before installing the new OKM Manager.	"Starting the OKM Installation" on page 63.
The Save Certificates function, initiated from the System menu, exports certificates that can be used by the new OKM Command Line Utility (see page 360).	"Saving Certificates" on page 93.
A note has been added specifying where configuration settings are stored.	"Specifying the Configuration Settings" on page 96.
The "IPv6 Addresses with Zone IDs" topic has been moved from the *Backup Operator Operations* chapter to the *Using the System Menu* chapter.	"IPv6 Addresses with Zone IDs" on page 98.
Before you export keys, keys must meet a number of criteria. Keys that do not are not exported when an Operator issues an Export Keys request.	"Exporting/Importing Keys" on page 154
The Create Transfer Partner dialog box includes an Export Format field.	"Creating a Transfer Partner" on page 161
The Entity ID, Entity Network Address, and KMA ID parameter descriptions have been updated.	"Viewing Audit Logs" on page 256.
KMAs running KMS 2.1 or earlier must be upgraded to KMS 2.2 before they can be upgraded to OKM 2.3.	"Software Upgrade Menu" on page 294.
The *Command Line Utilities* chapter describes the new OKM Command Line Utility that allows users to launch backups, export keys, import keys, and list data units from the command line instead of from the OKM Manager GUI.	"Command Line Utilities" on page 359.
The "Backup Command Line Utility" description has been moved from the *Backup Operator Operations* chapter to the new *Command Line Utilities* chapter.	"Command Line Utilities" on page 359.

Preface

This guide provides configuration and administration information for the Oracle Key Manager (OKM) software. It is intended for storage administrators, system programmers and operators responsible for configuring and maintaining the OKM software at their site.

Note – The product name, Key Management System (KMS), has been renamed to Oracle Key Manager (OKM). References to the KMS, most of its components and concepts, have been changed accordingly.

Related Documentation

The following list contains the names and order numbers of publications that provide additional information about OKM.

The online documentation is available at:

http://www.oracle.com/technetwork/indexes/documentation/index.html

Function	Title
	Hardware Publications
Installation planning for the encryption solution	*Systems Assurance Guide*
	Software Publications
OKM software configuration and maintenance	*Administration Guide*
Interface between the OKM and IBM Integrated Cryptography Service Facility (ICSF)	*Integration Guide*

Documentation, Support, and Training

Function	URL
Documentation ■ Customer: ■ Employee: ■ Partner:	 ■ `http://docs.sun.com` ■ `http://docs.sfbay.sun.com/` ■ `https://spe.sun.com/spx/control/Login`
Downloads ■ Customer: ■ Employee:	 ■ `http://www.sun.com/download/index.jsp` ■ https://dlrequest-zn-dlapps1.sfbay.sun.com/usr/login
Support	■ `http://www.sun.com/support/`
Training	■ http://www.oracle.com/global/us/education/sun_select_country.html
Sun Online Account	■ `https://reg.sun.com/register`

Oracle Welcomes Your Comments

Oracle is interested in improving its documentation and welcomes your comments and suggestions. Submit your comments by clicking the Feedback[+] link at:

`http://docs.sun.com`

Please include the title of your document with your feedback:

OKM 2.3 Administration Guide

CHAPTER 1

Introduction

Overview

The Oracle Key Manager (OKM) creates, stores, and manages encryption keys. It consists of the following components:

- **Key Management Appliance (KMA)** – A security-hardened box that delivers policy-based Lifecycle Key Management, authentication, access control, and key provisioning services. As a trust authority for storage networks, the KMA ensures that all storage devices are registered and authenticated, and that all encryption key creation, provisioning and deletion is in accordance with prescribed policies.
- **OKM Manager GUI** – A Graphical User Interface that is executed on a workstation and communicates with the KMA over an IP network to configure and manage the OKM. The OKM Manager GUI must be installed on a customer-provided workstation.
- **OKM Cluster** – The full set of KMAs in the system. All of these KMAs are aware of each other and replicate information to each other.
- **Agent** – A device or software that performs encryption, using keys managed by the OKM Cluster. These are the StorageTek encrypting tape drives. Agents communicate with KMAs via the Agent API. The Agent API is a set of software interfaces that are incorporated into the agent hardware or software.

OKM Concepts

OKM Clusters

OKM supports clustering of multiple KMAs, which provides load balancing and failover. All KMAs in a OKM Cluster act in an active/active manner. All KMAs can provide all capabilities to any agent. Actions performed on one KMA are quickly replicated to all other KMAs in the Cluster.

Agents

Agents perform cryptographic operations, specifically, encrypting data as it is written and decrypting data as it is read. Agents contact the OKM Cluster in order to create and retrieve keys used to perform the cryptography.

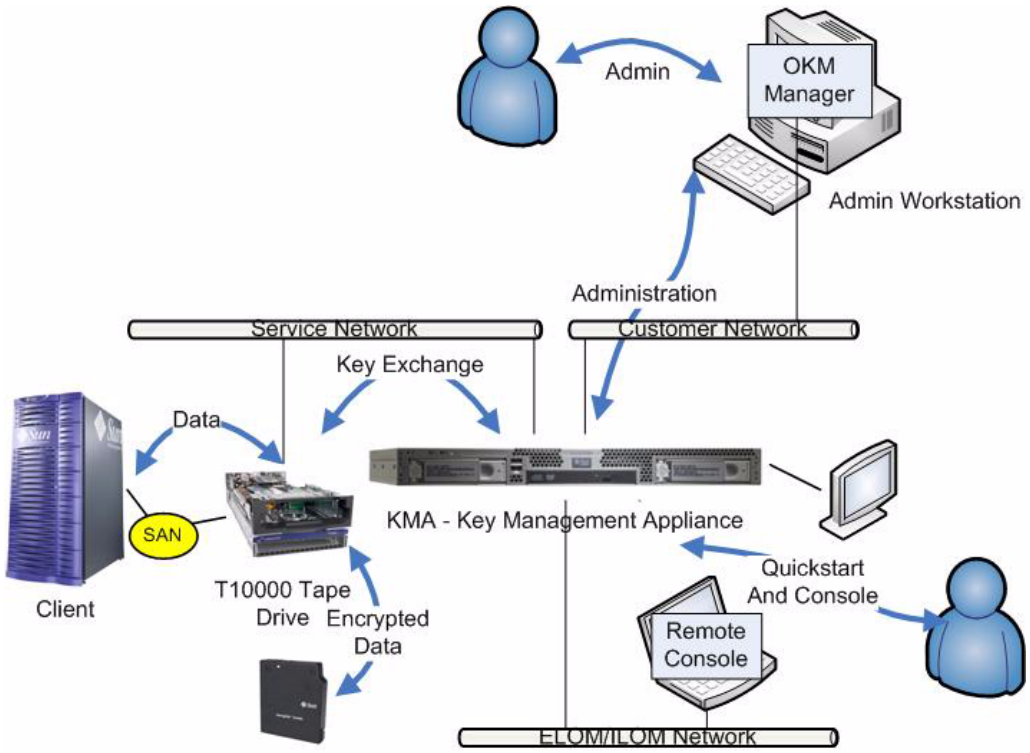
Network Connections

The OKM uses TCP/IP networking for the connections between KMAs, Agents, and machines where the OKM Manager GUI is running. In order to provide flexible network connections, two interfaces are provided for network connections on the KMA:

- The management connection, intended for connection to the customer network
- The service connection, intended for connection to the tape drives.

With production KMA installation, library-specific accessory kits are available that include switches and cables for connecting to the drives and the KMA. This is shown in FIGURE 1-1 on page 3.

FIGURE 1-1 Connections to the KMA



Initial Setup - Direct Connection or Remote Console

KMA initial setup is performed through the console connection. This can be done by using a monitor and keyboard connected directly to the KMA or by the remote console function in the Embedded Lights Out Manager (ELOM) or Integrated Lights Out Manager (ILOM). The ELOM or ILOM provides a remote connection to the console allowing you to perform server functions.

The ELOM/ILOM remote console function requires a third network connection, labeled the "ELOM/ILOM Network" in FIGURE 1-1. The ELOM's or ILOM's IP address must be configured as described in "Accessing the KMA Through the Service Processor" on page 22 in order to use the remote console function.

Note – Usually, the ELOM/ILOM Network is the same network as the customer network.

Initial Setup - QuickStart Program

When a KMA in the factory default state is powered on, a wizard function called QuickStart will run on the console to perform the initial setup. Once complete, most other functions can be done from the OKM manager GUI. A limited function console interface remains active for a small set of functions.

Key Lifecycle

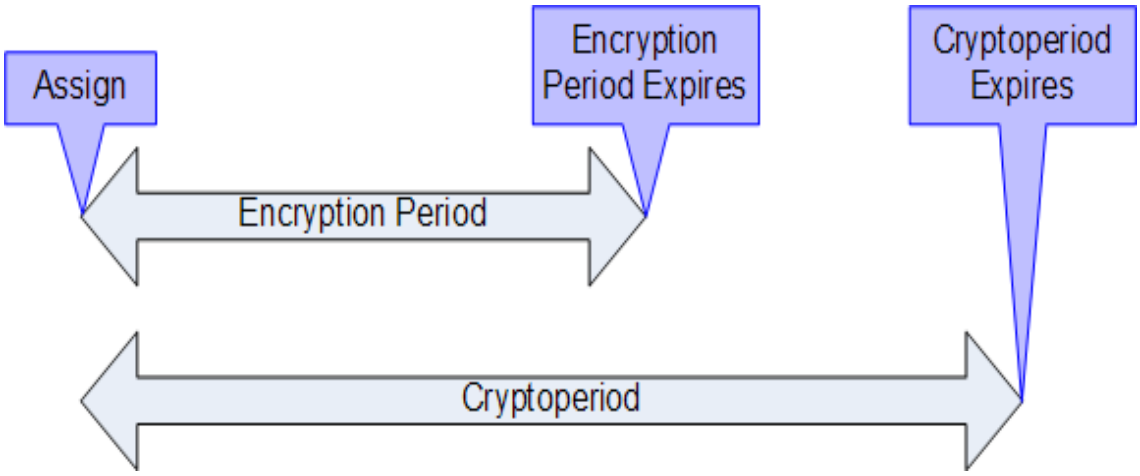
Keys undergo a lifecycle based on the key policy. The lifecycle imposed by the OKM is based on the NIST 800-57 guidelines. A few additional states are added to deal with nuances of the OKM.

The key lifecycle is based on two time periods (see FIGURE 1-2) defined in the key policies:

- Encryption period
- Cryptoperiod

The encryption period is the period after a key is assigned that can be used to encrypt data. The cryptoperiod is the period that can be used for decryption. The two periods start at the same time when the key is assigned.

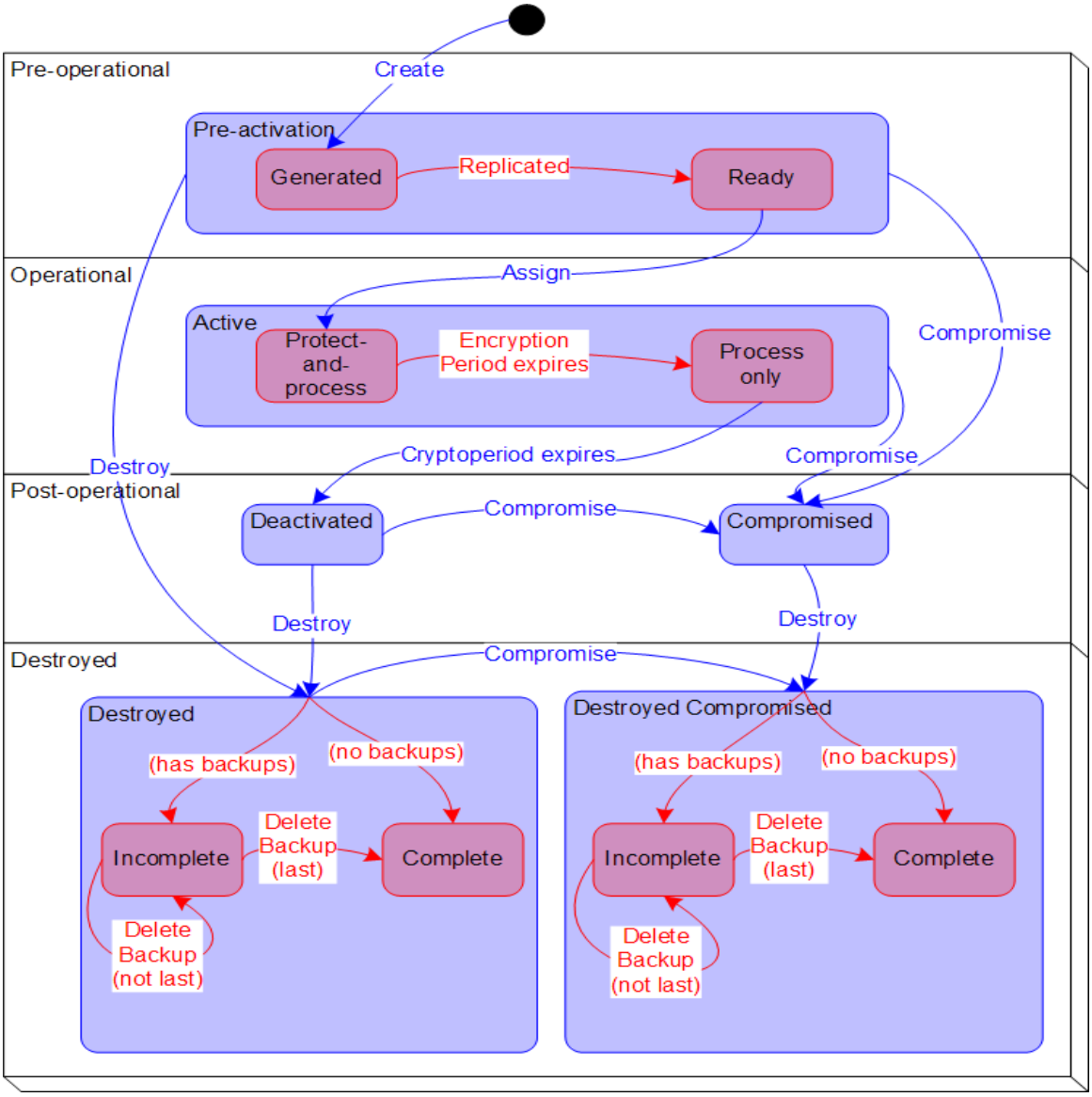
FIGURE 1-2 Key Lifecycle Periods



State Transition

These encryption period and cryptoperiod, combined with other functions of the OKM, define a state transition for keys as shown in FIGURE 1-3. In this diagram, states and transitions shown in blue are defined by NIST 800-57.

FIGURE 1-3 State Transition Diagram



OKM Key States and Transitions

In FIGURE 1-3, states and transitions shown in red are added by the OKM. When examining keys in the OKM Manager, only the innermost state is listed. OKM states are listed below.

Pre-activation

This state indicates that the key has generated but is not yet available for use. Within the pre-activation state, the key can take two further states, generated and ready.

Generated

A generated state indicates a key that has been created on one KMA in a OKM Cluster. It remains generated until it has been replicated to at least one other KMA in a multi-OKM Cluster. In a Cluster with only a single KMA, a key must be recorded in at least one backup to transition out of the generated state.

Ready

A ready state indicates that the key has been protected against loss by replication or a backup. A ready key is available for assignment. The “replicated” transition occurs when the key is replicated or (for a single OKM Cluster) backed up.

Active

This state indicates that the key may be used to protect information (encrypt) or to process previously protected information (decrypt) NIST states that an active key may be designated to protect only, process only, or protect and process. Further, it specifically states that for symmetric data encryption keys, a key may be used for some time period to protect and process information and once this time period expires, the key may continue to be used for processing only.

Within the active state, the OKM adds two substates. These states are described in NIST, but are not specifically identified as states.

Protect-and-process

A key in this state can be used for both encryption and decryption. A key is placed into this state when it is assigned. The assignment is done when an encryption agent requests a new key to be created.

Process only

A key in this state can be used for decryption but not encryption. When an agent determines that none of the keys available to it for a specific data unit that is being read or written are in the protect-and-process state, it should create a new key.

Keys move from the protect-and-process state to the process only state when the encryption period for the key expires.

Deactivated

This state indicates that the key has passed its cryptoperiod but may still be needed to process (decrypt) information. NIST specifically states that keys in this state may be used to process data.

The NIST guidelines state that if post-operational keys, including deactivated and compromised keys, need to remain accessible, they should be archived. This is a key recovery process that allows keys to be recalled from an archive and made available for use.

The OKM provides archives in the form of KMA backups but cannot recall a single key from a backup. Therefore, the OKM retains post-operational phase keys in the OKM Cluster and delivers them upon request from an agent.

Compromised

Keys are in the compromised state when they are released to or discovered by an unauthorized entity. Compromised keys should not be used to protect information, but may be used to process information.

Destroyed/Destroyed Compromised

Destroyed and Destroyed Compromised keys (keys that are compromised before or after destruction) no longer exist. However, information about the key may be retained. Key material from destroyed keys is removed from the OKM Cluster. Destroyed keys will not be delivered to an agent.

Note – The only way to destroy a key is through the GUI or the management API.

The NIST guidelines do not provide any basis for destroying keys based on time.

Within the Destroyed and Destroyed Compromised states, the OKM defines two substates, incomplete and complete. These states are created because the OKM does not control the backups that it creates. A customer administrator must inform the OKM when a backup has been destroyed. Only after all backups have been destroyed can a key be considered truly destroyed.

Incomplete

This substate indicates that at least one backup still exists that contains the destroyed key. In this substate, the key does not exist in any KMA in the OKM Cluster. Keys in this state cannot be delivered to agents.

Complete

This substate indicates that all backups containing the key have been destroyed. The key does not exist in any KMA, nor in any backup. Strictly speaking, backups that contain the key may well still exist. Although the OKM identifies the backups as destroyed, it is the responsibility of the user to ensure these backups have actually been destroyed.

It is worth noting again that the “destroyed” transition occurs only as the result of an administrative command. Further, keys may still be delivered to an encryption agent when the key is in the post-operational phase (Deactivated and Compromised states.) This interpretation is consistent with NIST's descriptions for the post-operational phase. The NIST guidelines specify that a post-operational key should be destroyed when it is “no longer needed.” We believe that only you can determine when a key is “no longer needed,” so only an external entity can initiate the destroyed transition.

Users and Role-based Access Control

The OKM provides the ability to define multiple users, each with a user ID and passphrase. Each user is given one or more pre-defined roles. These roles are:

- **Security Officer** – performs OKM setup and management
- **Operator** – performs agent setup and day-to-day operations
- **Compliance Officer** – defines Key Groups and controls agent access to Key Groups
- **Backup Operator** – performs backup operations
- **Auditor** – can view system audit trails
- **Quorum Member** – views and approves pending quorum operations.

A Security Officer is defined during the QuickStart process. Additional users may be defined using the OKM Manager GUI after QuickStart is complete.

Allowed Operations for Each Role

TABLE 1-3 on page 15 lists the functions for each role. It displays only the allowed operations for the GUI and the console. Although you may see an operation, it may fail when you attempt it. This can occur if roles are removed from a user between the time of display and when the operation is attempted.

All roles except the Auditor's must create a functioning encryption system. A user can have one or multiple roles.

Quorum Protection

The OKM also provides quorum protection for certain operations. You can define a quorum of up to 10 users and a threshold from one to the number of quorum users . This information is called the *Key Split Credentials* (see "Entering Key Split Credentials" on page 40).

The user IDs and passphrases are different from the user IDs and passphrases used to log into the system. When you attempt an operation that requires quorum approval, a screen is displayed that allows all quorum users to input their userid and passphrase. At a minimum, you must supply the specified threshold of userids and passphrases for the operation to be allowed.

Data Units, Keys, Key Groups, and Key Policies

Data units are used to represent data that is encrypted by agents. For tape drives, a data unit is a tape cartridge, and data units are always present. This is not a fundamental requirement, and future agents may operate without defining data units.

Keys are the actual key values (key material) and their associated metadata.

Key policies define parameters that govern keys. This includes lifecycle parameters (such as encryption period and cryptoperiod) and export/import parameters (for example, import allowed, export allowed.)

Key Groups associate keys and key policies. Key Groups have a specific key policy and are assigned to agents. Each agent has a list of allowed Key Groups. Agents are allowed to retrieve only the keys that are assigned to one of the agent's allowed Key Groups. Agents also have a default Key Group. When an agent creates a key (more specifically, assigns it to a data unit), the key is placed into the agent's default Key Group. There is functionality in place to allow more sophisticated control of Key Groups by agents. However, existing agents cannot leverage this functionality.

In order for the system to function, at least one key policy and one Key Group must be defined. That Key Group must be assigned as the default Key Group for all agents.

TCP/IP Connections and the KMA

If a firewall exists between the entities (OKM Manager, Agents, and other KMAs in the same Cluster) and the KMA, the firewall must allow the entity to establish TCP/IP connections with the KMA on the following ports:

- OKM Manager-to-KMA communication requires ports 3331, 3332, 3333, 3335.
- Agent-to-KMA communication requires ports 3331, 3332, 3334, 3335.
- KMA-to-KMA communication requires ports 3331, 3332, 3336.

TABLE 1-1 lists the ports KMAs explicitly use or ports at which KMAs provide services.

TABLE 1-1 KMA Port Connections

Port Number	Protocol	Direction	Description
22	TCP	Listening	SSH (only when Technical Support is enabled)
123	TCP/UDP	Listening	NTP
3331	TCP	Listening	OKM CA Service
3332	TCP	Listening	OKM Certificate Service
3333	TCP	Listening	OKM Management Service
3334	TCP	Listening	OKM Agent Service
3335	TCP	Listening	OKM Discovery Service
3336	TCP	Listening	OKM Replication Service

TABLE 1-2 shows other services listening at ports that might not be used.

TABLE 1-2 Other Services

Port Number	Protocol	Direction	Description
53	TCP/UDP	Connecting	DNS (only when KMA is configured to use DNS)
68	UDP	Connecting	DHCP (only when KMA is configured to use DHCP)
111	TCP/UDP	Listening	RPC (KMAs respond to rpcinfo queries). This port is open only on KMS 2.1 and earlier
161	UDP	Connecting	SNMP (only when SNMP Managers are defined)
546	UDP	Connecting	DHCPv6 (only when KMA is configured to use DHCP and IPv6)
4045	TCP/UDP	Listening	NFS lock daemon (KMS 2.0 only)

Notes –

Port 443 must be open to enable customers to access the Service Processor web interface and the OKM Console through the firewall.

Refer to the *Oracle Key Manager Installation and Service Manual* to see ELOM and ILOM ports

OKM in the Network

FIGURE 1-4 shows a typical deployment of the OKM solution.

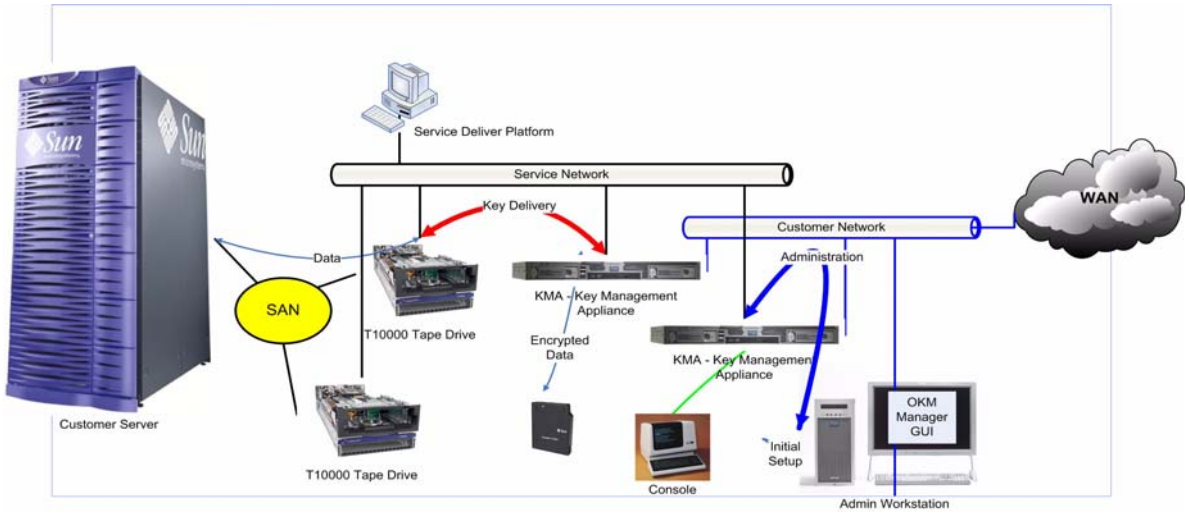


FIGURE 1-4 Typical Deployment of OKM Solution

OKM Manager Software Requirements

To run the OKM Manager, you need a workstation that runs one of the following:

- Microsoft® Windows XP, Vista, 7, 2003, and 2008
- Solaris 10 Update 3 or higher (x86 and SPARC).

You do not need to have Administrator (on Windows) or root (on Solaris) privileges to install and invoke the GUI.

Using Online Help

The OKM Manager includes comprehensive online help. To display help on any OKM Manager screen,

- Click the **Help** button that is located at the top of the panel for general help.

or

- Navigate to a panel by either pressing the **Tab** key or by clicking somewhere within the panel. Then, click **F1** to view context-sensitive help.

Role-Based Access Control

OKM defines the following roles:

- **Security Officer –** manages security settings, users, sites, and Transfer Partners
- **Compliance Officer –** manages key policies and Key Groups and determines which agents and Transfer Partners can use Key Groups
- **Operator** – manages agents, data units, and keys
- **Backup Operator –** performs backups
- **Auditor** – views information about the OKM Cluster
- **Quorum Member** – views and approves pending quorum operations.

A single KMA user account may be assigned membership to one or more roles. The KMA verifies that the requesting user entity has permission to execute an operation based on the user's role(s). For more information on the roles, refer to"Logging into the KMA" on page 324.

Role-Based Operations

TABLE 1-3 shows the system operations that each user role can perform. In the "Roles" columns,

- **Yes** – the role is allowed to perform the operation.
- **Quorum –** the role is allowed to perform the operation but must also provide a quorum.
- A blank means the role is not allowed to perform the operation.

TABLE 1-3 System Operations/User Roles

Entity	Operation	Roles					
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor	Quorum Member
Console							
	Log In	Yes	Yes	Yes	Yes	Yes	Yes
	Set KMA Locale	Yes					
	Set KMA IP Address	Yes					
	Enable Tech Support	Yes					
	Disable Tech Support	Yes		Yes			
	Enable Primary Administrator	Yes					
	Disable Primary Administrator	Yes		Yes			
	Restart KMA			Yes			
	Shutdown KMA			Yes			
	Log OKM into Cluster	Quorum					
	Set User's Passphrase	Yes					
	Reset KMA	Yes					
	Zeroize KMA	Yes					
	Logout	Yes	Yes	Yes	Yes	Yes	Yes
Connect							
	Log In	Yes	Yes	Yes	Yes	Yes	Yes
	Create Profile	Yes	Yes	Yes	Yes	Yes	Yes
	Delete Profile	Yes	Yes	Yes	Yes	Yes	Yes
	Set Config Settings	Yes	Yes	Yes	Yes	Yes	Yes
	Disconnect	Yes	Yes	Yes	Yes	Yes	Yes
Key Split Credentials							
	List	Yes					
	Modify	Quorum					
Autonomous Unlock							

TABLE 1-3 System Operations/User Roles

Entity	Operation	Roles					
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor	Quorum Member
	List	Yes					
	Modify	Quorum					
Lock/Unlock KMA							
	List Status	Yes	Yes	Yes	Yes	Yes	
	Lock	Yes					
	Unlock	Quorum					
Site							
	Create	Yes					
	List	Yes		Yes			
	Modify	Yes					
	Delete	Yes					
Security Parameters							
	List	Yes	Yes	Yes	Yes	Yes	
	Modify	Yes					
KMA							
	Create	Quorum					
	List	Yes		Yes			
	Modify	Quorum					
	Delete	Yes					
User							
	Create	Quorum					
	List	Yes					
	Modify	Yes					
	Modify Passphrase	Quorum					
	Delete	Yes					
Role							
	Add	Quorum					
	List	Yes					
Key Policy							
	Create		Yes				
	List		Yes				
	Modify		Yes				
	Delete		Yes				
Key Group							
	Create		Yes				

TABLE 1-3 System Operations/User Roles

Entity	Operation	Roles					
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor	Quorum Member
	List		Yes	Yes			
	List Data Units		Yes	Yes			
	List Agents		Yes	Yes			
	Modify		Yes				
	Delete		Yes				
Agent							
	Create			Yes			
	List		Yes	Yes			
	Modify			Yes			
	Modify Passphrase			Yes			
	Delete			Yes			
Agent/Key Group Assignment							
	List		Yes	Yes			
	Modify		Yes				
Data Unit							
	Create						
	List		Yes	Yes			
	Modify			Yes			
	Modify Key Group		Yes				
	Delete						
Keys							
	List Data Unit Keys		Yes	Yes			
	Destroy			Yes			
	Compromise		Yes				
Transfer Partners							
	Configure	Quorum					
	List	Yes	Yes	Yes			
	Modify	Quorum					
	Delete	Yes					
Key Transfer Keys							
	List	Yes					
	Update	Yes					
Transfer Partner Key Group Assignments							
	List		Yes	Yes			
	Modify		Yes				

TABLE 1-3 System Operations/User Roles

Entity	Operation	Roles					
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor	Quorum Member
Backup							
	Create				Yes		
	List	Yes	Yes	Yes	Yes		
	List Backups with Destroyed Keys		Yes	Yes			
	Restore	Quorum					
	Confirm Destruction				Yes		
Core Security Backup							
	Create	Yes					
SNMP Manager							
	Create	Yes					
	List	Yes		Yes			
	Modify	Yes					
	Delete	Yes					
Audit Event							
	View	Yes	Yes	Yes	Yes	Yes	
	View Agent History		Yes	Yes			
	View Data Unit History		Yes	Yes			
	View Data Unit Key History		Yes	Yes			
System Dump							
	Create	Yes		Yes			
System Time							
	List	Yes	Yes	Yes	Yes	Yes	
	Modify	Yes					
NTP Server							
	List	Yes	Yes	Yes	Yes	Yes	
	Modify	Yes					
Software Version							
	List	Yes	Yes	Yes	Yes	Yes	
	Upgrade			Quorum			
Network Configuration							
	Display	Yes	Yes	Yes	Yes	Yes	

TABLE 1-3 System Operations/User Roles

Entity	Operation	Roles					
		Security Officer	Compliance Officer	Operator	Backup Operator	Auditor	Quorum Member
Pending Quorum Operation							
	Approve						Quorum
	Delete	Yes					

Setting Up and Managing the Key Management Appliance

For procedures on getting your OKM solution installed and configured, refer to the *OKM 2.3 Installation and Service Manual*.

CHAPTER 2

Getting Started

This chapter describes the following topics:

- Accessing the KMA Through the Service Processor – the Embedded Lights Out Manager (ELOM) and Integrated Lights Out Manager (ILOM) provide a remote connection to the console (page 22)
- Running the QuickStart program – QuickStart is a utility that a customer (Security Officer or qualified representative) can use to configure a new KMA (page 31).

Note – A service representative can also run QuickStart, however, since this program establishes critical security parameters, customers may prefer to do it themselves, following their corporate security policies.

Accessing the KMA Through the Service Processor

The Embedded Lights Out Manager (ELOM) and Integrated Lights Out Manager (ILOM) contain a separate Service Processor from the main server. These Service Processors provide a remote connection to the KMA, allowing you to perform server functions, such as the *QuickStart* program.

Notes –
KMAs that are Sun Fire X2100 or X2200 servers use an ELOM as the Service Processor, whereas KMAs that are Sun Fire X4170 M2 servers employ an ILOM as their service processor.

Refer to the *Embedded Lights Out Manager Administration Guide* or the *Integrated Lights Out Manager Web Interface Procedures Guide* for configuration information.

Connecting to the KMA

Connect to the KMA through the ELOM or ILOM using either:

- The network connection, LAN 1 NET MGT ELOM or ILOM interface (suggested), or
- The keyboard and monitor attached to the KMAs.

Popup blockers will prevent Windows from launching in the following procedures. Disable the popup blockers before beginning.

If the window appears, but a console window does not, the Web browser or Java version is incompatible with the Service Processor. Upgrade to the latest versions of the browser and Java. See TABLE 2-1 for a list of compatible versions.

TABLE 2-1 Supported ELOM Compatible Web Browsers and Java Versions

Client OS	Supports These Web Browsers	Java Runtime Environment Including Java Web Start
■ Microsoft Windows XP ■ Microsoft Windows 2003 ■ Microsoft Windows Vista	■ Internet Explorer 6.0 and later Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0	JRE 1.5 (Java 5.0 Update 7 or later)
■ Red Hat Linux 3.0 and 4.0	■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0	
■ Solaris 9 ■ Solaris 10 ■ Solaris Sparc ■ SUSE Linux 9.2	■ Mozilla 1.7.5	
You can download the Java 1.5 runtime environment at: http://java.com The current version of the ELOM guide is located at: http://dlc.sun.com/		

TABLE 2-2 Supported ILOM Compatible Web Browsers and Java Versions

Client OS	Supports These Web Browsers	Java Runtime Environment Including Java Web Start
■ Microsoft Windows 98 ■ Microsoft Windows 2000 ■ Microsoft Windows XP ■ Microsoft Windows Vista	■ Internet Explorer 6.0 and later ■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0 or later ■ Opera 6.*x* or later	JRE 1.5 (Java 5.0 Update 7 or later)
■ Linux (Red Hat, SuSE, Ubuntu)	■ Mozilla 1.7.5 or later ■ Mozilla Firefox 1.0 or later ■ Opera 6.*x* or later	
■ Solaris 9 ■ Solaris 10	■ Mozilla 1.7.5 or later ■ Firefox 1.0 or later	
You can download the Java 1.5 runtime environment at: http://java.com The current version of the ILOM guide is located at: http://dlc.sun.com/		

Using a Network Connection - ELOM

1. Using another workstation on the network, launch a Web browser.
2. Connect to the KMA ELOM using the IP Address or hostname of LAN 1 (NET MGT), which is the address just configured.

Note – Because the certificate in the ELOM will not match the assigned name or IP, you will receive one or more warnings from your web browser.

---

3. Click OK or Yes to bypass these warnings.

   Once past the warnings, you will receive the ELOM login prompt.

FIGURE 2-1 Embedded Lights Out Manager Login Screen

4. Log in using:
   Userid = `root`
   Password = `changeme`

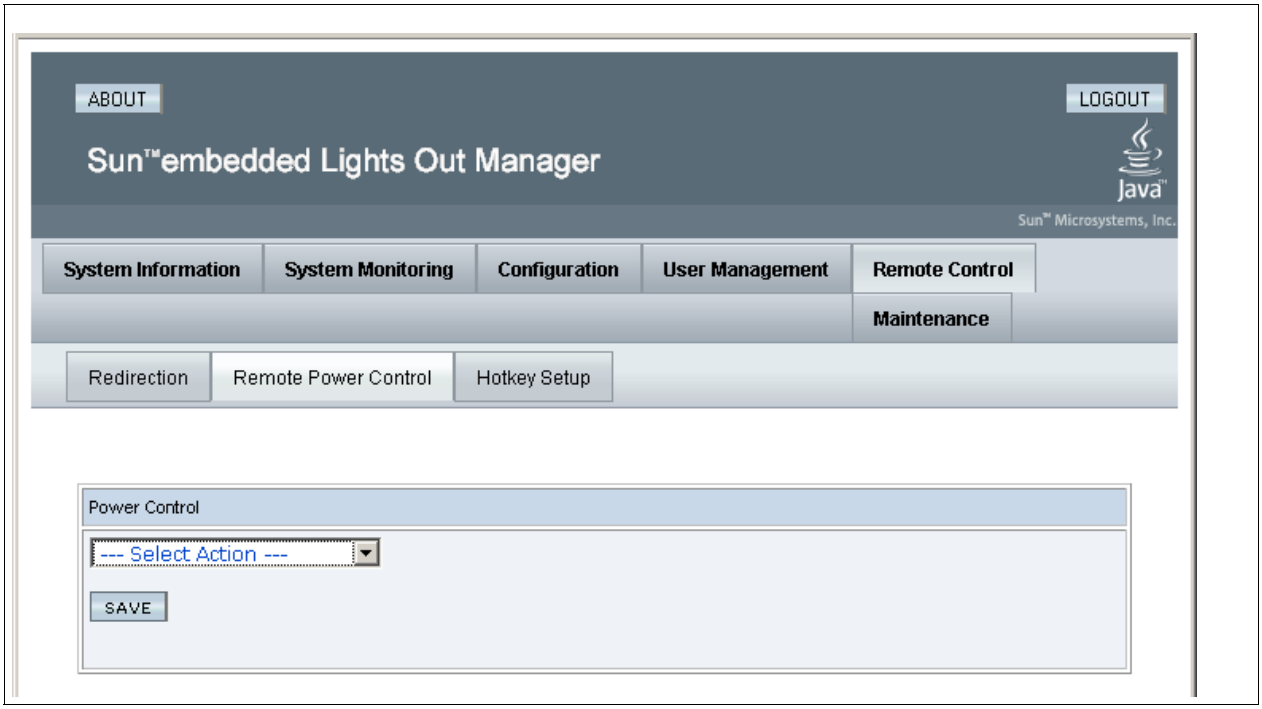
   The next screen is the Manager Screen. If the server has just been connected to power, and it has not been powered on, it will not have completed a system boot.

   KMAs are configured to boot up automatically when initially powered on and should boot up to the QuickStart prompt within a few minutes of being powered on.

5. Check the power status by clicking on the **System Monitoring** tab.

6. If the Power Status shows "power off," click the **Remote Control** tab to the far right of the upper row of tabs.
7. Click the **Remote Power Control** tab in the second row of tabs.
8. In the Select Action drop-down, choose **Power On** and click the **Save** button.
   The KMA will begin powering up. This will take a few minutes; however, you can continue with the KMA configuration.

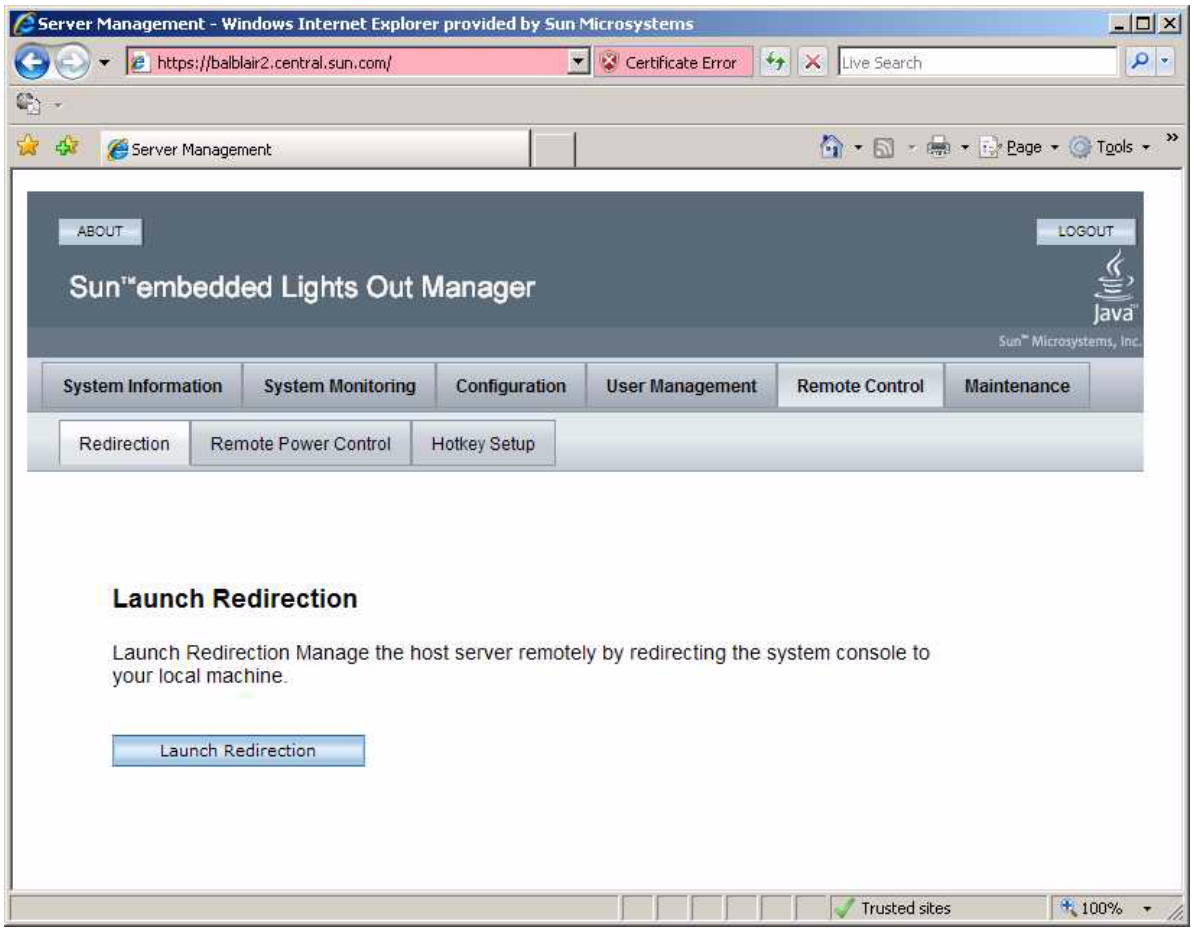
FIGURE 2-2 Power Control



9. Click the **Remote Control** tab in the first row of tabs.
10. Click the **Redirection** tab in the second row of tabs.
11. Click the **Launch Redirection** button.

A Java applet will be downloaded before starting the remote console window.

FIGURE 2-3 Launch Redirection (ELOM)



This launches the remote console screen in a new window.

12. Save the javaRKVM.jnlp file when requested, then open it to start the remote console. Click past any warnings that may be displayed.
13. Go to "Launching the OKM Console" on page 30 for the next steps in the process.

Using a Network Connection - ILOM

1. Using another workstation on the network, launch a Web browser.
2. Connect to the KMA ILOM using the IP Address or hostname of LAN 1 (NET MGT), which is the address just configured.

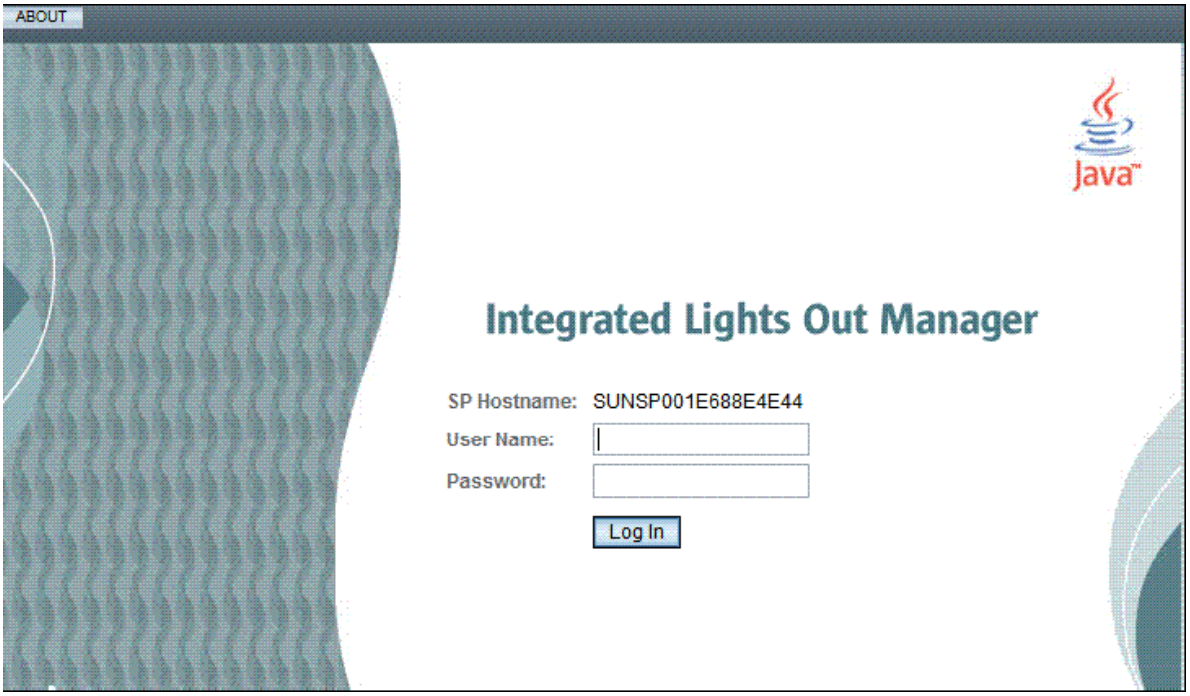
Note – Because the certificate in the ILOM will not match the assigned name or IP, you will receive one or more warnings from your web browser.

---

3. Click OK or Yes to bypass these warnings.

   Once past the warnings, you will receive the ILOM login prompt.

FIGURE 2-4 Integrated Lights Out Manager Login Screen



4. Log in using:

   Userid = `root`

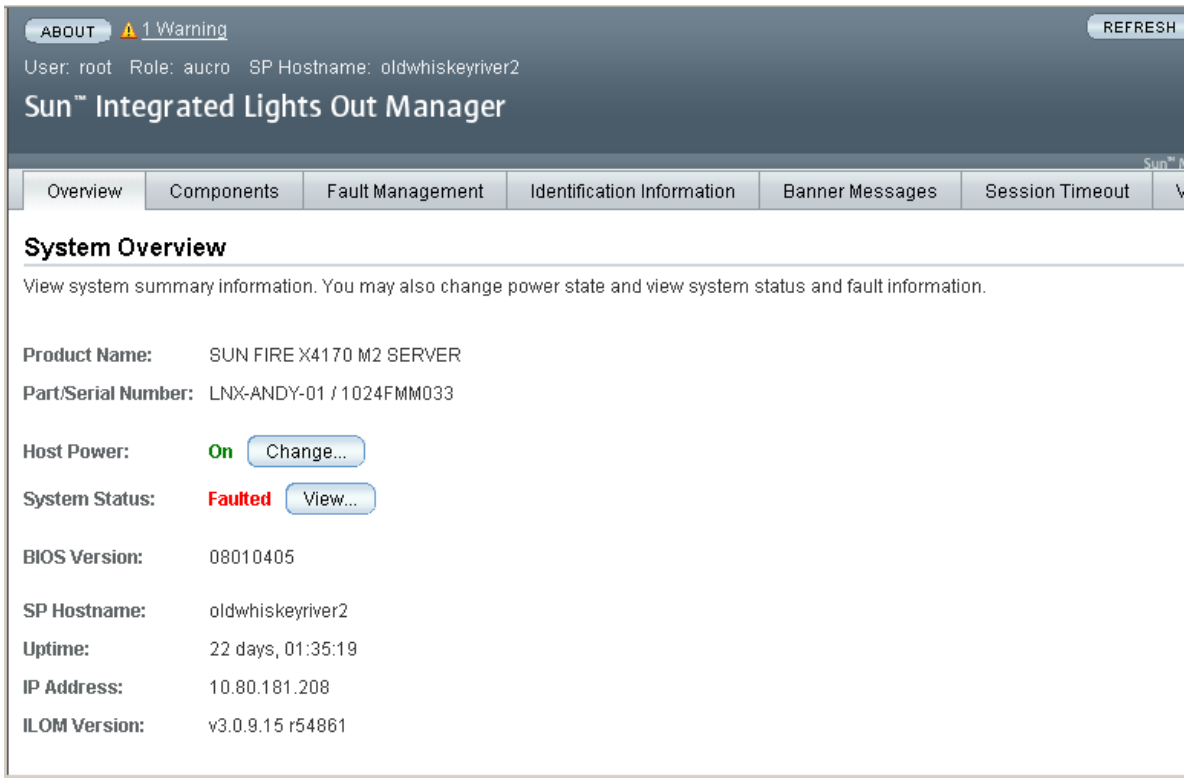
   Password = `changeme`

   The next screen is the Manager Screen. If the server has just been connected to power, and it has not been powered on, it will not have completed a system boot.

   KMAs are configured to boot up automatically when initially powered on and should boot up to the QuickStart prompt within a few minutes of being powered on.

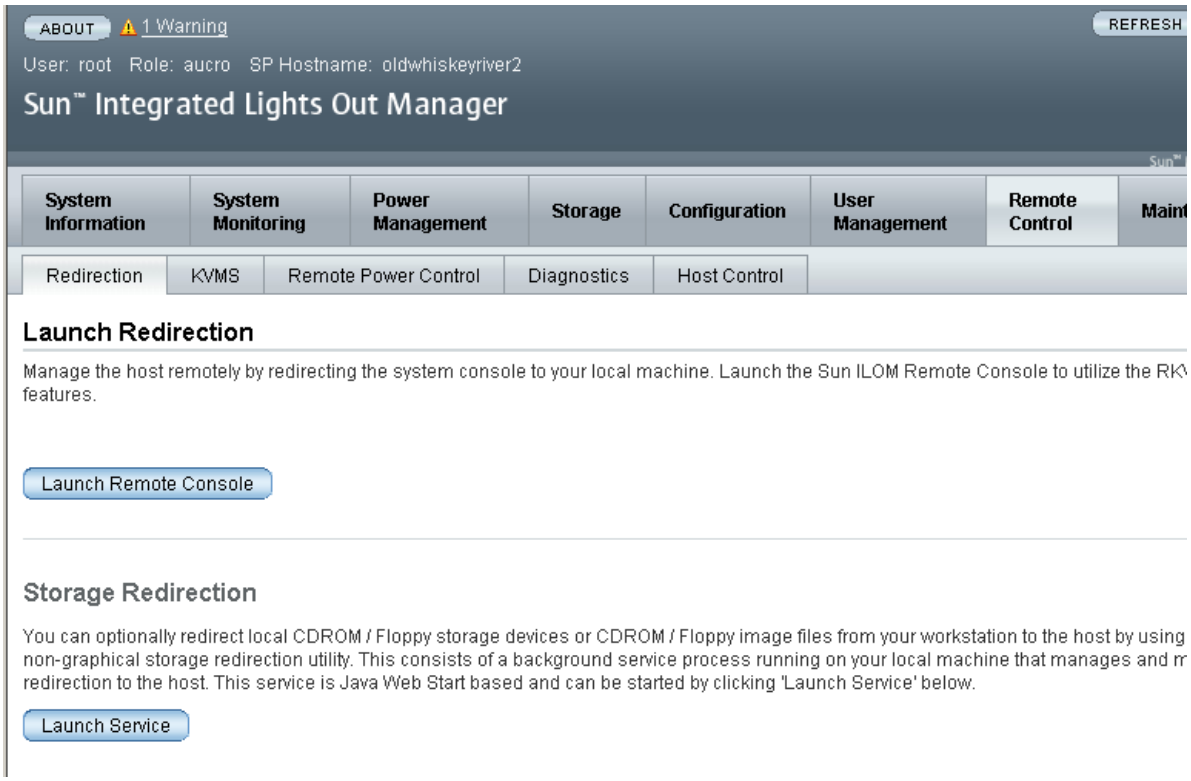
5. Check the power status shown next to Host Power.

FIGURE 2-5 Power Control



6. If Host Power shows that the power is off, click the Change drop-down.
7. In the Select Action drop-down, choose **Power On** and click the **Save** button. The KMA will begin powering up. This will take a few minutes; however, you can continue with the KMA configuration.
8. Click the **Remote Control** tab in the first row of tabs.
9. Click the **Redirection** tab in the second row of tabs.

FIGURE 2-6 Launch Redirection (ILOM)



10. Click the **Launch Remote Console** button.

    A Java applet will be downloaded before starting the remote console window. This launches the remote console screen in a new window.

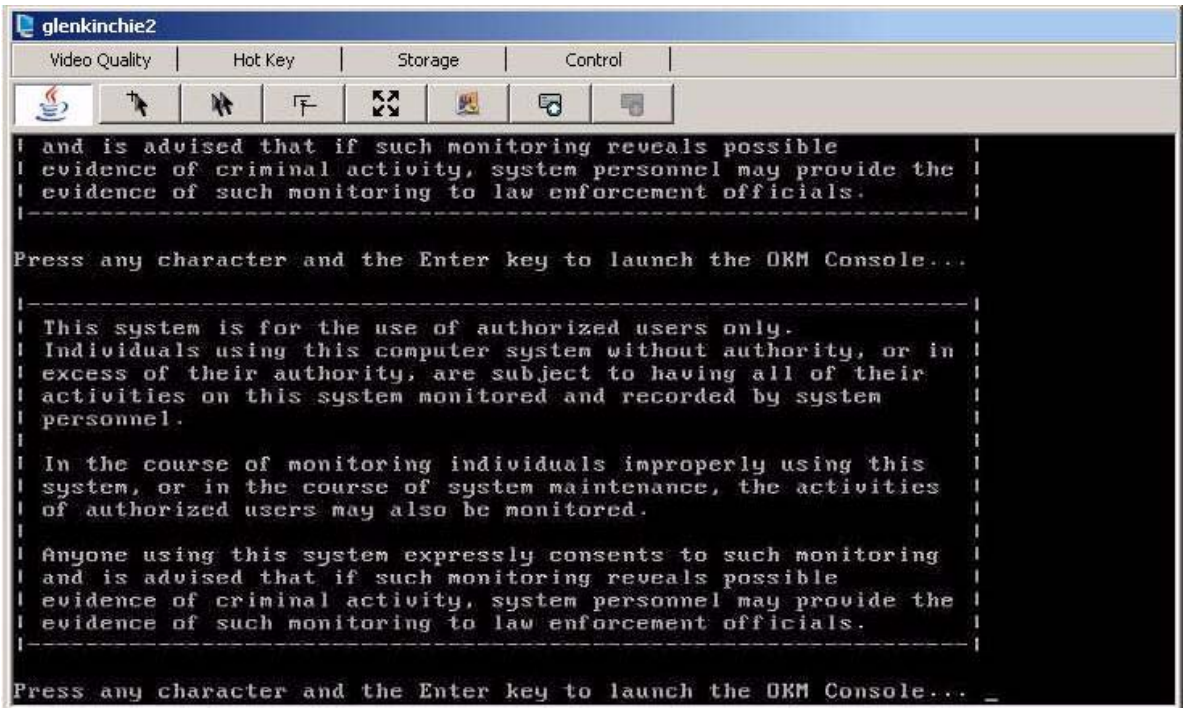
11. Save the javaRKVM.jnlp file when requested, then open it to start the remote console. Click past any warnings that may be displayed.

12. Go to "Launching the OKM Console" on page 30 for the next steps in the process.

Launching the OKM Console

1. Press any key and press <Enter> to continue. The KMA checks the SCA 6000 card and reports its status.

FIGURE 2-7 Remote Console



2. Press <Enter>.

You now proceed to the QuickStart program prompt described in "Starting QuickStart" on page 32.

Running the QuickStart Program

When a KMA in the factory default state is powered on, a special mode of the KMA Configuration Menu called QuickStart is automatically executed. QuickStart collects the minimal configuration information required for initializing the KMA. Once the QuickStart program has been successfully completed, it cannot be re-executed. The only way to access the QuickStart program again is to reset the KMA to its factory default state (refer to "Resetting the KMA to the Factory Default" on page 346.)

Note – In the following screen examples, entries in **bold** represent areas where you respond.

Starting QuickStart

To run the QuickStart Program:

Power on the KMA. When you power up the KMA for the first time, QuickStart is executed, and the Welcome to QuickStart! screen is displayed.

```
Copyright (c) 2007, 2010, Oracle and/or its affiliates. All rights
reserved.
Oracle Key Manager Version 2.3 (Build1036)
------------------------------------------------------------
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:
```

Note – If you press Ctrl-c, the QuickStart program resets and the Welcome to QuickStart! screen is redisplayed.

Specifying the Network Configuration

The following procedures allow you to establish the network configuration.

Setting the KMA Management IP Addresses

To set the KMA Management IP addresses:

1. Press <Enter> to continue. The following information is displayed.

```
Set KMA Management IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other KMAs or Users in your system.


Do you want to configure the Management Network interface to have
an IPv6 address? [y/n]:

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

Please enter the Management Network IP Address [10.80.180.39]:

Please enter the Management Network Subnet Mask [255.255.254.0]:
```

2. At the `Please enter your choice:` prompt on the main menu, type **3** and press <Enter>.
3. Type either **n** or **y** at the `Do you want to configure the Management Network interface to have an IPv6 address` prompt.
4. Type either **n** or **y** at the `Do you want to use DHCP to configure the Management Network interface` prompt. If you type **n**, go to Step 5. If you type **y**, you go to the procedure "Setting the KMA Service IP Addresses" on page 35.
5. At the prompt, type the Management Network IP address and press <Enter>.
6. At the `Please enter the Management Network Subnet Mask:` prompt, type the subnet mask address, (for example **255.255.254.0**) and press <Enter>.

Enabling the Technical Support Account

To enable the Technical Support account:

1. Press <Enter> to continue. The following information is displayed.

```
To assist in troubleshooting your network configuration,
you might want to enable the technical support account for the
network configuration steps of the QuickStart process.

Do you want to enable this support account for the network
configuration steps of the QuickStart process? [y/n]: y

Press Enter to continue:
```

2. If you want to enable the technical support account in QuickStart, type **y** at the `Do you want to enable this support account for the network configuration steps of the QuickStart process?` prompt. Otherwise, type **n**, and you proceed to Step 3.

Note – If you type **y**, you see the same prompts that are described in "Enabling the Technical Support Account" on page 348. After answering these prompts, you move to Step 3.

---

3. Press <Enter> to continue.

Note – If you have enabled the Technical Support account, QuickStart disables it after you complete the *Specifying the DNS Settings* process shown on page 38. The following screen is displayed.

```
The support account is now being disabled.

Technical Support configuration changes have been completed.

Press Enter to continue:
```

Setting the KMA Service IP Addresses

To set the KMA Service IP addresses:

1. Press <Enter> to continue. The following information is displayed.

```
Set KMA Service IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other Agents in your system.


Do you want to configure the Service Network interface to have an
IPv6 address?
[y/n]: y

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

Please enter the Service Network IP Address [192.168.1.39]:

Please enter the Service Network Subnet Mask [255.255.255.0]:
```

2. At the `Please enter your choice:` prompt on the main menu, type **4** and press <Enter>.
3. Type either **n** or **y** at the `Do you want to configure the Service Network interface to have an IPv6 address` prompt.
4. Type either **n** or **y** at the `Do you want to use DHCP to configure the Service Network interface` prompt. If you type **n**, go to Step 5. If you type **y**, you go to the procedure "Viewing/Adding/Deleting Gateways" on page 36.
5. At the prompt, type the Service Network IP address and press <Enter>.
6. At the `Please enter the Service Network Subnet Mask:` prompt, type the subnet mask address, (for example **255.255.255.0**) and press <Enter>.

Viewing/Adding/Deleting Gateways

This menu option shows the current gateway settings (five to a page) on the Management (M) and Service (S) interfaces.

1. Press <Enter> to continue. The following information is displayed, indicating that you can add a gateway, remove a gateway, or accept the current gateway configuration.

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                    Netmask         IF
---- -------------------------- -------------------------- --------------- --
   1 default                    10.80.181.254               0.0.0.0         M
   2 default                    10.80.181.21                0.0.0.0         M
   3 default                    192.168.1.119               0.0.0.0         S
   4 10.0.0.0                   10.80.180.25                255.255.254.0   M
*  5 10.80.180.0                10.80.180.39                255.255.254.0   M

Press Enter to continue:

Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                    Netmask         IF
---- -------------------------- -------------------------- --------------- --
*  6 192.168.1.0                192.168.1.39                255.255.255.0   S
   7 192.168.25.0               10.80.180.25                255.255.255.0   M
   8 192.168.26.0               10.80.180.25                255.255.255.0   M
*  9 127.0.0.1                  127.0.0.1                   255.255.255.255
* 10 fe80::                     fe80::216:36ff:feca:15b6    10              M

(1) Continue
(2) Back
1
```

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                     Netmask         IF
---- -------------------------- -------------------------- --------------- --
* 11 fe80::                     fe80::216:36ff:feca:15b9    10              S

You can add a route, delete a route, or exit the gateway configuration.
Please choose one of the following:

(1)  Add a gateway
(2)  Remove a configured gateway (only if modifiable)
(3)  Exit gateway configuration
(4)  Display again
3
```

2. At the `Please enter your choice:` prompt on the main menu, type **5** and press <Enter>.
3. At the `(1) Continue (2) Back` prompt, type **1** to display the next gateway setting or **2** to return to the previous gateway setting.
4. At the `Please choose one of the following:` prompt, type **1**, **2**, **3,** or **4** and press <Enter>.

Note – If at any time you press Ctrl+c, no changes are saved and you are returned to the main menu.

Specifying the DNS Settings

This menu option shows the DNS settings, and prompts you for a new DNS domain (if you want to configure one) and the DNS server IP addresses.

1. Press <Enter> to continue. The following information is displayed.

```
Set DNS Configuration
------------------------------------------------------------

Press Ctrl-c to abort.

DNS configuration is optional, but necessary if this KMA
will be configured using hostnames instead of IP addresses.

Current DNS configuration:

Domain:
Nameservers:

Please enter the DNS Domain (blank to unconfigure DNS):
central.sun.com

Up to 3 DNS Name Servers can be entered. Enter each name
server separately, and enter a blank name to finish.

Please enter DNS Server IP Address #1: 10.80.0.5

Please enter DNS Server IP Address #2:
```

2. At the `Please enter your choice:` prompt on the main menu, type **6** and press <Enter>.
3. Enter the DNS domain name at the `Please enter the DNS Domain (blank to unconfigure DNS):` prompt.
4. Enter the DNS server IP address at the `Please enter DNS Server IP address` prompt. You can enter up to three IP addresses.
5. Press `<Enter>`, without specifying an IP address, to finish.

Initializing the KMA

1. Press <Enter> to continue. The following information is displayed.

```
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:
```

2. At the prompt, type a unique identifier for the KMA.

Note – A KMA Name cannot be altered once it is set using the QuickStart program. It can only be changed by resetting the KMA to the factory default and running QuickStart again.

Configuring the Cluster

1. At the prompt, press <Enter>. The following information is displayed, indicating that you can use this KMA to create a new Cluster, join an existing Cluster, or restore a Cluster from a backup of this 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. At the prompt, type **1**, **2**, or **3** and press <Enter>.

If you type 1, go to "Entering Key Split Credentials" on page 40.

If you type 2, go to "Joining an Existing Cluster" on page 46.

If you type 3, go to "Restoring a Cluster From a Backup" on page 52.

Entering Key Split Credentials

Key Split Credentials user IDs and passphrases should be entered by the individual who owns that user ID and passphrase. Using one person to collect and enter this information defeats the purpose of having the Key Split Credentials.

If it is impractical for all members of the Key Split Credentials to enter this information at this time, enter a simple set of credentials now, and then enter the full credentials later in the OKM Manager.

However, doing this creates a security risk. If a Core Security backup is created with simple Key Split Credentials, it can then be used to restore a backup.

1. At the `Please enter your choice:` prompt, type 1. The following information is displayed.

```
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: 2


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

Please enter the Key Split Threshold: 1

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.
```

Notes –
The Key Split Size and Key Split Threshold can be changed using "Modifying the Key Split Configuration" on page 198.

The Key Split Threshold must be less than or equal to the Key Split Size.

User IDs and passphrases should be entered only by an authorized user to keep them secure. These items also can be changed after running the QuickStart program.

2. At the `Please enter the Key Split Size:` prompt, type the number of key splits that will be generated and press <Enter>.
3. At the `Please enter the Key Split Threshold:` prompt, type the number of required keys splits to obtain a quorum and press <Enter>.
4. At the `Please enter the Key Split User Name #1:` prompt, type the user name for the first Key Split user and press <Enter>.
5. At the `Please enter Key Split Passphrase #1:` prompt, type the passphrase for the first Key Split user and press <Enter>.
6. At the `Please re-enter Key Split Passphrase #1:` prompt, type the same passphrase that you previously entered and press <Enter>.
7. Repeat Step 4 through Step 6 until all user names and passphrases have been entered for the selected Key Split size.

Notes –
The Key Split user names and passphrases are independent of other user accounts that are established for KMA administration.

Key split user names should be different from KMA user names.

Entering Initial Security Officer User Credentials

1. At the `Press Enter to continue:` prompt, press <Enter>. The following information is displayed.

```
The initial Security Officer User is the first User that can
connect to the KMA via the Oracle Key Manager GUI.  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 Oracle Key Manager GUI.
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.
```

Note – This initial Security Officer user account will be used to logon to the KMA using the OKM Manager.

---

2. At the prompt, type the Security Officer's user name and press <Enter>. The following information is displayed.
3. At the prompt, type the Security Officer's passphrase and press <Enter>.
4. At the Please re-enter the Security Officer Passphrase: prompt, re-type the same passphrase and press <Enter>.

Important – All KMAs have their own passphrases that are independent of passphrases assigned to users and Agents. The first KMA in a Cluster is assigned a random passphrase. If this KMA's certificate expires, and you want to retrieve its entity certificate from another KMA in the Cluster, you would have to use the OKM Manager to set the passphrase to a known value. For procedures, refer to "Setting a KMA Passphrase" on page 115.

Specifying the Autonomous Unlocking Preference

Caution – While it is more convenient and increases the availability of the OKM Cluster, enabling autonomous unlocking creates security risks. When autonomous unlocking is enabled, a powered-off KMA must retain sufficient information to boot up fully and begin decrypting stored keys.

This means a stolen KMA can be powered up, and an attacker can begin extracting keys for the KMA. While it is not easy to extract keys, a knowledgeable attacker will be able to dump all keys off the KMA. No cryptographic attacks will be needed.

If autonomous unlocking is disabled, cryptographic attacks will be required to extract keys from a stolen KMA.

You should carefully consider potential attacks and security concerns before choosing to enable autonomous unlocking.

1. At the `Press Enter to continue:` prompt, press <Enter>. The following information is displayed.

```
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
```

Note – The Autonomous Unlocking feature allows the KMA to enter a fully operational state after a hard or soft reset without requiring the entry of a quorum of passphrases using the OKM Manager. You can change this option from the OKM Manager at a later time.

2. At the prompt, type **y** or **n** and press <Enter>.

Setting the Key Pool Size

1. At the `Press Enter to continue:` prompt, press <Enter>. The following information is displayed.

```
Enter Key Pool Size
------------------------------------------------------------

Press Ctrl-c to abort.

Each KMA pre-generates and maintains a pool of keys. These
pre-operational keys must be backed up or replicated before
a KMA will provide them to an Agent for use in protecting
data. This helps to ensure that a key will never be
permanently lost, even in disaster scenarios.

A smaller key pool size prevents unnecessary initial
database (and backup) size, but requires frequent backups
or a reliable network to ensure that activation-ready keys
are always available. Conversely, a large key pool size is
more tolerant of infrequent backups or unreliable network
connections between KMAs, but the large number of pre-
generated keys causes the database (and backups) to be
quite large.


Please select the key pool size (1000 - 200000):
```

2. At the prompt, enter the key pool size. The value entered determines the initial size that the new KMA generates and maintains.

Synchronizing KMA Time

KMAs in a Cluster **must** keep their clocks synchronized. Internally, all KMAs use UTC time (Coordinated Universal Time).

You can also use the OKM Manager to adjust date and time settings to local time.

```
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 cluster has been created.

Press Enter to continue:
Oracle Key Manager Version (Build1036)
_____________________________________________________________
KMA initialization complete!

You may now connect to the KMA via the Oracle Key Manager GUI in
order to continue with Cluster configuration.

Press Enter to exit:

Copyright (c) 2007, 2010, Oracle and/or its affilitates. All rights
reserved.
Oracle Key Manager Version 2.3 (Build1036)
_____________________________________________________________

Please enter your User Name:
```

1. If an NTP server is available in your network environment, at the `Please enter the NTP Server Hostname or IP Address (optional):` prompt, enter the NTP server hostname or IP address.
2. If an NTP server is not available, press <Enter>. Then, at the `Please enter the date and time for this KMA` prompt, enter the date and time in one of the specified formats, or press <Enter> to use the displayed date and time.
3. At the prompt, press <Enter>. KMA initialization is complete.
4. Press <Enter> to exit. The QuickStart program terminates and a login prompt is displayed (refer to "Logging into the KMA" on page 324). The KMA now has the minimum system configuration that is required to communicate with the OKM Manager.
5. Your next step is to use the OKM Manager to connect to the Cluster. For procedures, refer to "Connecting to the Cluster" on page 87.

Joining an Existing Cluster

Important –

- Before performing this task, the Security Officer must first log into the OKM Cluster using the OKM Manager and create a KMA. See "Creating a KMA" on page 109.

  The KMA Name specified in the KMA initialization process (see "Initializing the KMA" on page 39) must match the KMA name you enter when you create the KMA.

- When you add a new KMA to an existing OKM Cluster, the OKM Cluster begins to propagate Cluster information to the new KMA. It takes time for the Cluster to finish circulating this information to the new KMA, and as a result, the Cluster becomes busy during this time period.

  Add KMAs to the Cluster during times of light loads so that this propagation activity does not interfere with normal operations. To avoid problems caused by Agents attempting to use the new KMA during the synchronization period, the KMA remains locked after it has been added to the Cluster. Wait until the KMA has been synchronized (that is, until it has "caught up" with other KMAs in the Cluster) before you unlock it.

- In earlier KMS releases, if the release running on a new KMA was different from an existing KMA in the Cluster, then the new KMA was automatically upgraded or downgraded to the release of the existing KMA when the new KMA joined the Cluster. For OKM 2.3, if the new KMA runs OKM 2.3 and the existing KMA runs an earlier KMS release, then the new KMA can join the Cluster without downgrading to the earlier release.

To join a new KMA to an existing Cluster:

1. When you complete the KMA initialization process (see "Initializing the KMA" on page 39), at the prompt, press <Enter>.

   The following information is displayed, indicating that you can use this KMA to create a new Cluster, join an existing Cluster, or restore a Cluster from a backup of this 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. At the `Please enter your choice:` prompt, type **2**. The following information is displayed.

```
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...

This KMA has joined the Cluster.

Press Enter to continue:

Oracle Key Manager Version 2.3 (Build1036)
-------------------------------------------------------------

KMA initialization complete!

You may now connect to the KMA via the Oracle Key Manager GUI
in order to continue with Cluster configuration.

Press Enter to exit:
```

Note – Before this new KMA can communicate with an existing KMA in the Cluster, you must use the OKM Manager to create an entry for this KMA in the existing KMA's database. For procedures, refer to "Creating a KMA" on page 109.

---

3. At the prompt, type the network address of one KMA in the existing Cluster and press <Enter>.
4. At the prompt, type the passphrase for the KMA and press <Enter>.
5. Enter the first Key Split user name for the first KMA.

6. Type the passphrase for the Key Split user, and press <Enter>.

Important – Enter Key Split user names and passphrases carefully. Any errors cause this process to fail with a non-specific error message. To limit information exposed to an attacker, no feedback is given as to which Key Split user name or passphrase is incorrect.

---

7. Repeat Steps 5 and 6 until you have entered a sufficient number of Key Split user names and passphrases to form a quorum.
8. At the next `Please enter Key Split User Name` prompt, press <Enter>. Enter a blank name to finish.

   The initialization is complete.

   At the end of a successful Join Cluster session, QuickStart displays the following prompt if the Cluster's replication version is at least 12.

```
It might take some time for this KMA to be updated with
information from other KMAs in the Cluster.  This amount of
time can be greater in Clusters that have more KMAs or when
the KMAs have been online for a long time.

To accelerate these initial updates (that is, to catch up now),
you can choose now to download a backup from another KMA in
the Cluster and then restore from it.  There will not be an
opportunity to accelerate these updates later.

Catch up now? [y/n]:
```

9. Type **y** to accelerate initial updates. Otherwise, type **n** to go to step 10.

Note – Before you type **y** at the above prompt, create a backup on a peer KMA if you have switched the Cluster's replication version to 12. Also, ensure that the peer KMA on which you created a backup is currently responding on the network. These steps help the new KMA find a cached backup to download and apply.

   The KMA you specified identifies another KMA that has the largest cached backup in this Cluster, downloads that backup, and then applies it to its local database. This process is equivalent to replicating the data but at a much faster rate. Informational messages appear during this process.

   For example:

```
Waiting 10 seconds for the join to propagate to Peer KMAs...

Querying Peer KMAs to find the active ones...

Querying active Peer KMAs to find cached backup sizes...

Peer KMA at IP Address 10.80.180.39 has a cached backup size of
729136 bytes.

Downloading the cached backup from this Peer KMA...

Downloaded the cached backup from this Peer KMA.

Initialized the Key Store.

Performed maintenance on the Key Store.

Applying the cached backup to the local database...

.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.........................................................

Applied the cached backup to the local database.

Successfully accelerated initial updates on this KMA.
```

Later, the newly joined KMA automatically replicates any data that is not in the backup.

If an error occurs during this process, QuickStart displays the above prompt again (in case the error is due to a temporary condition). QuickStart also displays the above prompt again if the KMA cannot find a peer KMA that has a cached backup.

However, if more than 5 minutes has elapsed since the first time the above prompt was displayed, then QuickStart displays the following message and no longer displays the above prompt:

```
Failed to accelerate initial updates on this KMA after 300 seconds.
This KMA will gradually be updated with information from other
KMAs.
```

Regardless of whether you typed **y** or **n** at step 9, or even if the process timed out, these messages appear:

```
This KMA has joined the Cluster.

Press Enter to continue:
```

10. Press <Enter> to exit. The QuickStart program terminates and a login prompt is displayed (refer to "Logging into the KMA" on page 324). The KMA now has the minimum system configuration that is required to communicate with the OKM Manager.
11. Your next step is to use the OKM Manager to connect to the Cluster. For procedures, refer to "Connecting to the Cluster" on page 87.
12. The OKM Cluster begins to propagate information to the newly added KMA. This causes the new KMA to be very busy until it has caught up with the existing KMAs in the Cluster. The other KMAs will also be busy. You can observe this activity from the OKM Manager by viewing the KMAs as described by "Viewing KMAs" on page 104.
13. Observe the Replication Lag Size value of the new KMA. Initially, this value will be high. Periodically refresh the information displayed in this panel by pulling down the View menu and selecting Refresh or by pressing the F5 key. Once the Replication Lag Size value of this KMA drops to a similar value of other KMAs in the Cluster, then you can unlock the KMA as described by "Unlocking the KMA" on page 205.

Restoring a Cluster From a Backup

This option allows you to create a Security Officer account that can be used to restore the Backup image to the KMA using the OKM Manager. You can use a Backup to restore a KMA's configuration in the event a KMA experiences a failure (for example, hard disk damage). This, however, is not typically required since a KMA that is restored to the factory default state can readily join an existing Cluster and build up its database by receiving replication updates from Cluster peers. Restoring a KMA from a Backup is still useful in the event that all KMAs in a Cluster have failed.

Notes –

You first must create a Backup. For procedures on creating Backups using the OKM Manager, refer to "Creating a Backup" on page 305.

Oracle recommends you specify a new Security Officer name that did not exist in the OKM Cluster when the last backup was performed. If you specify an existing Security Officer name and provide a different passphrase, the old passphrase is overwritten.

If you specify an existing Security Officer name and other roles were added to that user before the last backup was performed, these other roles will no longer be assigned to this User.

To restore the backup image:

1. When you complete the KMA initialization process (see "Initializing the KMA" on page 39), at the prompt, press <Enter>.

   The following information is displayed, indicating that you can use this KMA to create a new Cluster, join an existing Cluster, or restore a Cluster from a backup of this 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. At the `Please enter your choice:` prompt, type **3**. The following information is displayed.

```
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 Oracle Key Manager GUI. 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. At the prompt, type the Security Officer's user name and press <Enter>.

Best Practice – Enter a **temporary** restore Security Officer user ID (for example, RestoreSO) instead of the Security Officer user ID that existed prior to the restore.

---

4. At the prompt, type the Security Officer's passphrase and press <Enter>.

Steps 5 through 7 are optional.

If you choose to define initial quorum user credentials in QuickStart, you can enter a quorum login name and passphrase at this time so that the restore operation from the OKM Manager GUI (Step 13) is pended.

Quorum members can then use this login and passphrase later to log in to the OKM Manager GUI and enter their credentials to approve the restore (see "Restoring a Backup" on page 182).

If you do not enter a quorum login user ID here, the only user that exists at the end of QuickStart is the Security Officer created in Step 3. In this case, all Key Split Credentials must be entered at once for the restore to occur (Step 15).

The following information is displayed:

```
Enter Initial Quorum Login User Credentials
------------------------------------------------------------

Press Ctrl-c to abort.

The initial Quorum Login User is an optional user that
will allow the restore operation to be pended until quorum
members can connect to the KMA via the Oracle Key Manager GUI and
enter their credentials.  If this user is not created here,
then a quorum of credentials must be entered at the time
the restore operation is requested.

Please enter a Quorum Login User ID (optional): Q

Passphrases must be at least 8 characters and at most 64
characters in length.
Passphrases must not contain the User's User ID.
Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter the Quorum Login Passphrase:

Please re-enter the Quorum Login Passphrase:
```

5. At the prompt, either press <Enter> or type the quorum login user ID and press <Enter>.
6. At the prompt, either press <Enter> or type the quorum login passphrase and press <Enter>.
7. At the Please re-enter the Quorum Login Passphrase: prompt, either press <Enter> or re-type the same passphrase and press <Enter>.

8. At the `Please re-enter the Security Officer's Passphrase:` prompt, retype the passphrase you entered in Step 4 and press <Enter>.

```
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:
```

9. If an NTP server is available in your network environment, at the `Please enter the NTP Server Hostname or IP Address (optional):` prompt, enter the NTP server hostname or IP address.

10. If an NTP server is not available, press <Enter>. Then, at the `Please enter the date and time for this KMA` prompt, enter the date and time in one of the specified formats, or press <Enter> to use the displayed date and time.

    Ensure the date and time are accurate. Key lifecycles are based on time intervals, and the original creation times for the keys are contained in the backup. An accurate time setting on the replacement KMA is essential to preserve the expected key lifecycles.

11. At the prompt, press <Enter>. The following information is displayed, indicating that initialization is complete.

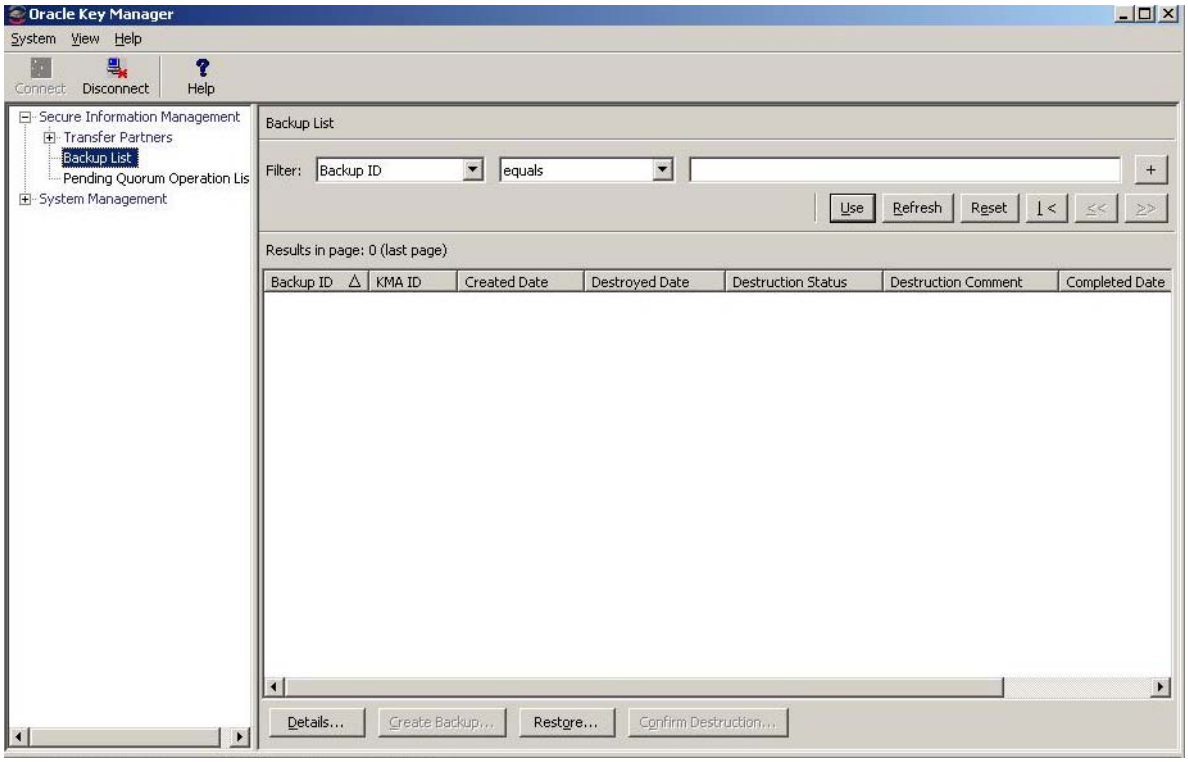
```
Oracle Key Manager Version 2.3 (Build1036)
------------------------------------------------------------

KMA initialization complete!

You may now connect to the KMA via the Oracle Key Manager GUI
in order to continue with Cluster configuration.

Press Enter to exit:
```

12. Press <Enter> to exit. The QuickStart program terminates and a login prompt is displayed.

Best Practice – Log in to the OKM Manager GUI as the temporary restore Security Officer user ID you established in Step 3.

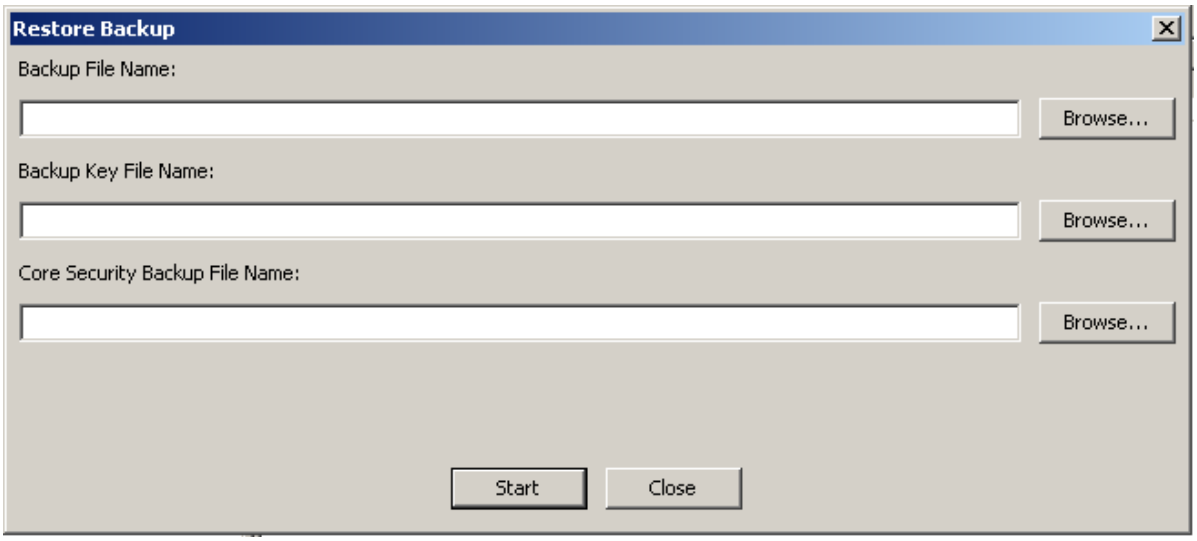
---

13. Login as the Security Officer on the OKM Manager and select **Backup List**. From the Backup List screen, click the **Restore** button to upload and restore the backup to the KMA.

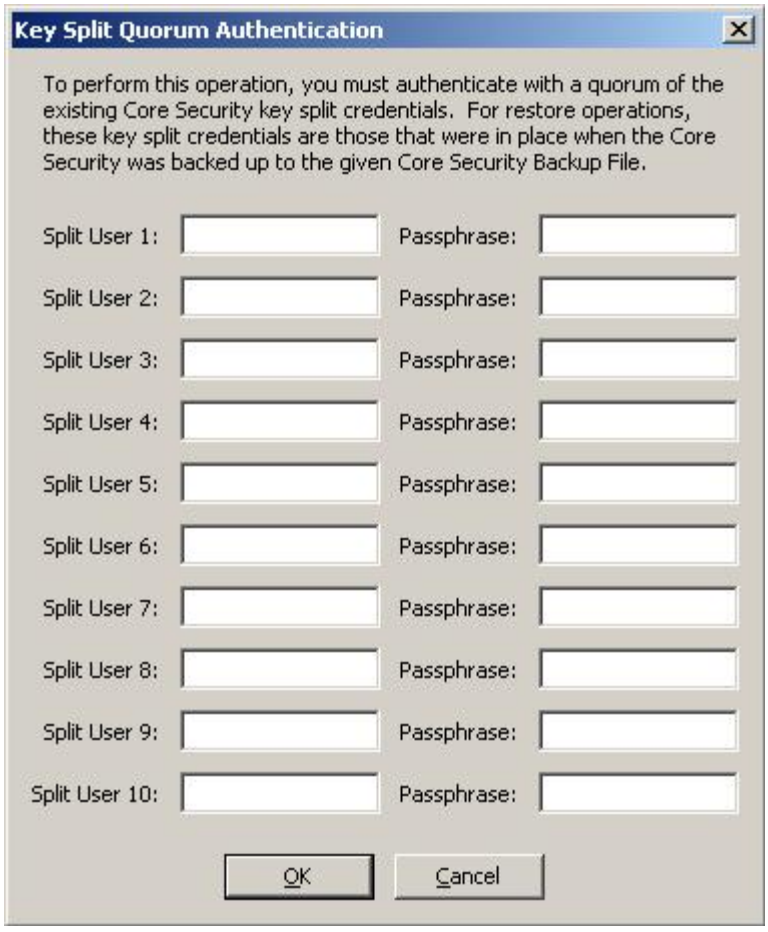


14. To complete the restore operation, the OKM Manager prompts for a Backup File that corresponds to the Backup Key file, a Backup Key file, and a Core Security backup file.

    The Backup Key file and Backup file must match, but any Core Security Backup file can be used.



15. The OKM Manager then prompts for a quorum of Key Split users. These must be Key Split Credential users that were in effect when the Core Security Backup was performed.



Once the restore is complete, the Key Split Credentials that were in effect when the backup (not the Core Security Backup) was completed, will be restored.

Important – Enter Key Split user names and passphrases carefully. Any errors cause this process to fail with a non-specific error message. To limit information exposed to an attacker, no feedback is given as to which Key Split user name or passphrase is incorrect.

---

16. When the restore process is completed, a new Cluster is created.

Best Practice – Log in to the OKM Manager GUI using the original Security Officer user ID (the one that existed prior to the restore), and delete the temporary restore Security Officer user ID as a cleanup step. Refer to "Deleting Users" on page 130.

Adding Agents and Enrolling Tape Drives

After you set up the KMA, you can add agents and enroll tape drives to use that KMA:

1. Log into the OKM Manager GUI as an Operator and create an agent (refer to "Creating an Agent" on page 273).
2. Using the Virtual Operator Panel (VOP), perform the following operations. Refer to the VOP documentation if you do not know how to connect to and use the VOP.
   a. Ask the service representative to license the tape drive(s) (refer to "License the Tape Drives" in chapter 3 of the *OKM Installation and Service Manual*). Use the Virtual Operator Panel (VOP) to perform this function.
   b. With guidance from the service representative, enroll the tape drive(s) (refer to "Enroll the Tape Drives" in chapter 3 of the *OKM Installation and Service Manual*).

      You must supply this information:

      - Is the drive going to use a permanently encrypting tape drive?
      - What is the agent ID, passphrase, and OKM IP address of the appliance?
3. Log into the OKM Manager GUI as a Compliance Officer, create at least one Key Group (refer to "Creating a Key Group" on page 228), and assign the tape drives (agents) to this Key Group (refer to "Assigning a Key Group to an Agent" on page 241 and to "Enroll the Tape Drives" in the *OKM Installation and Service Manual*).

   You must assign this Key Group as the default or the drive cannot write. If you do not specify a default, the drive is read-only for the assigned group(s).

CHAPTER 3

Using the OKM Manager

This chapter describes the OKM Manager and explains procedures for:

- Installing the OKM Manager software (page 62)
- Invoking the OKM Manager (page 70)
- Uninstalling the OKM Manager software (page 84).

The chapter also provides a brief description of the menus and panes.

What is the OKM Manager?

The OKM Manager is an application that serves as a client to the KMA. It can be used to configure, control, and monitor the KMA. Depending on the assigned user roles, users can perform different operations.

Installing the OKM Manager Software

To download the installer for the OKM Manager software:

1. Go to the Oracle download website at the following location:
   `http://www.oracle.com/technetwork/indexes/downloads/index.html`

Note – There are a number of ways to access the OKM installer. The following procedure describes one method.

---

2. Scroll down, and click the **Sun Downloads: A-Z Listing** link.
3. Scroll down, and search under "O" for the **Oracle Key Manager** link.
4. From there, follow the instructions to complete the download.

Starting the OKM Installation

Important – Uninstall any previous OKM Manager version before installing the new OKM Manager.

1. Depending on whether you are running a Windows or Solaris system, select the applicable process to invoke the installer program.

- For Windows, double-click the shortcut to start the installer program.
- For Solaris,

   a. Set your DISPLAY environment to identify the system to which this installer should be displayed.

      i. If you start the installer program on the local Solaris system, set your DISPLAY environment variable to ":0.0."

      ii. Navigate to the directory where you downloaded the installer.

      iii. Invoke the installer.

      For example, if you downloaded the installer to the /tmp directory, and you plan to invoke it on your local Solaris system, you start the installer by entering the following commands at a shell prompt:

```
DISPLAY=:0.0
export DISPLAY
cd /tmp
ls install.bin
sh ./install.bin
```

Note – If you invoke the installer on one Solaris system and want it to be displayed on another Solaris system, set your DISPLAY environment variable to identify the system on which it should be displayed. On the display system, first run the xhost(1) utility to allow access from the system from which you will invoke the installer.

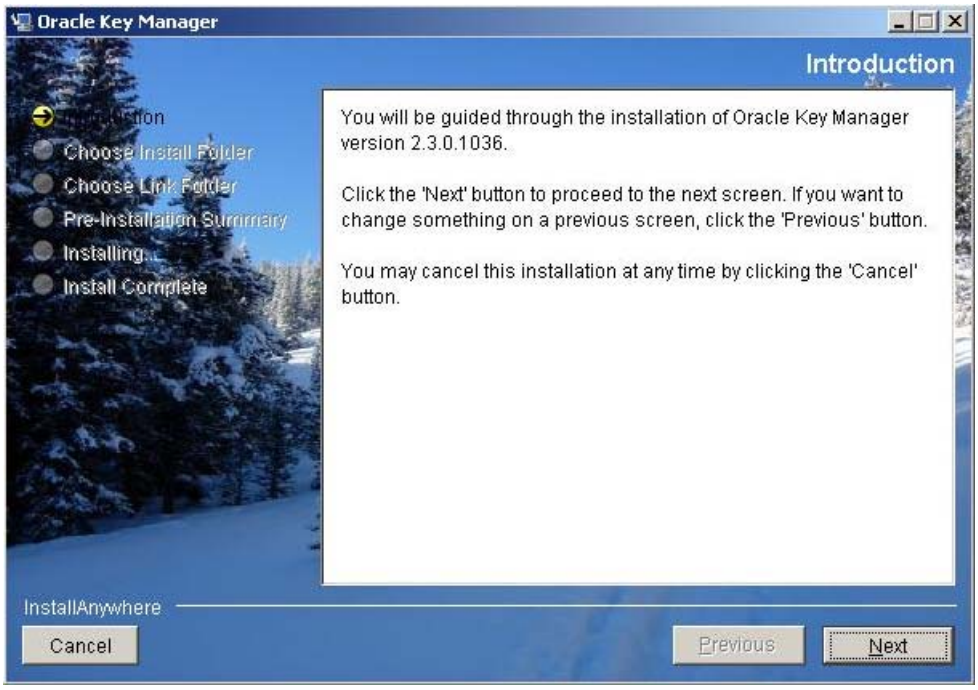
For example, on the system (named "hosta") where you wish to display the installer, enter:

```
xhost +
```

On the system where you start the installer, enter:

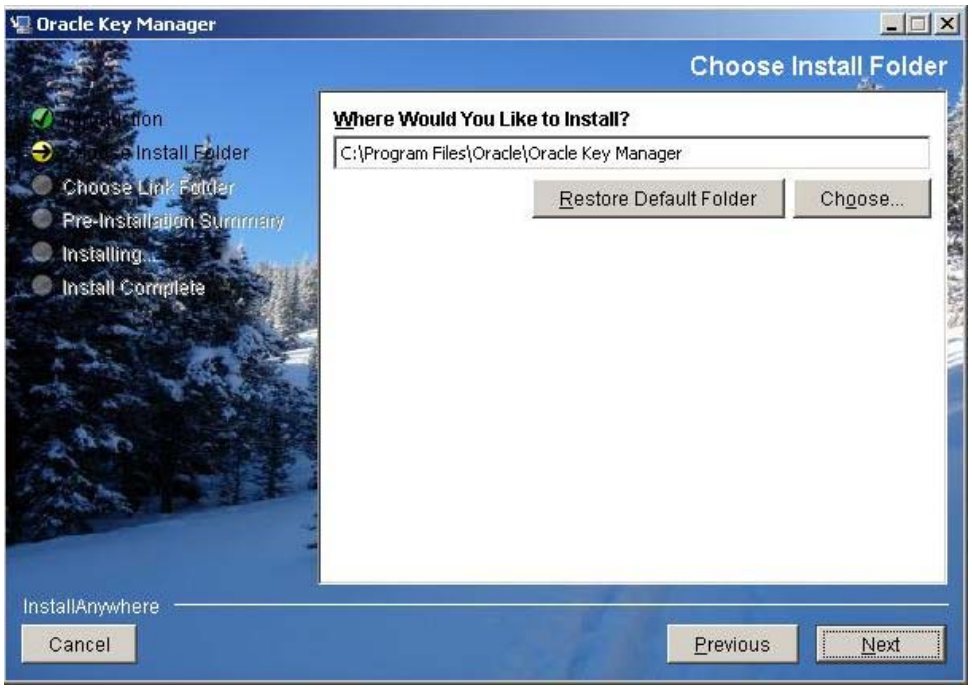
```
ping hosta
DISPLAY=hosta:0.0
export DISPLAY
cd /tmp
ls install.bin
sh ./install.bin
```

The Introduction window is displayed. The following screen examples are for a Windows system.



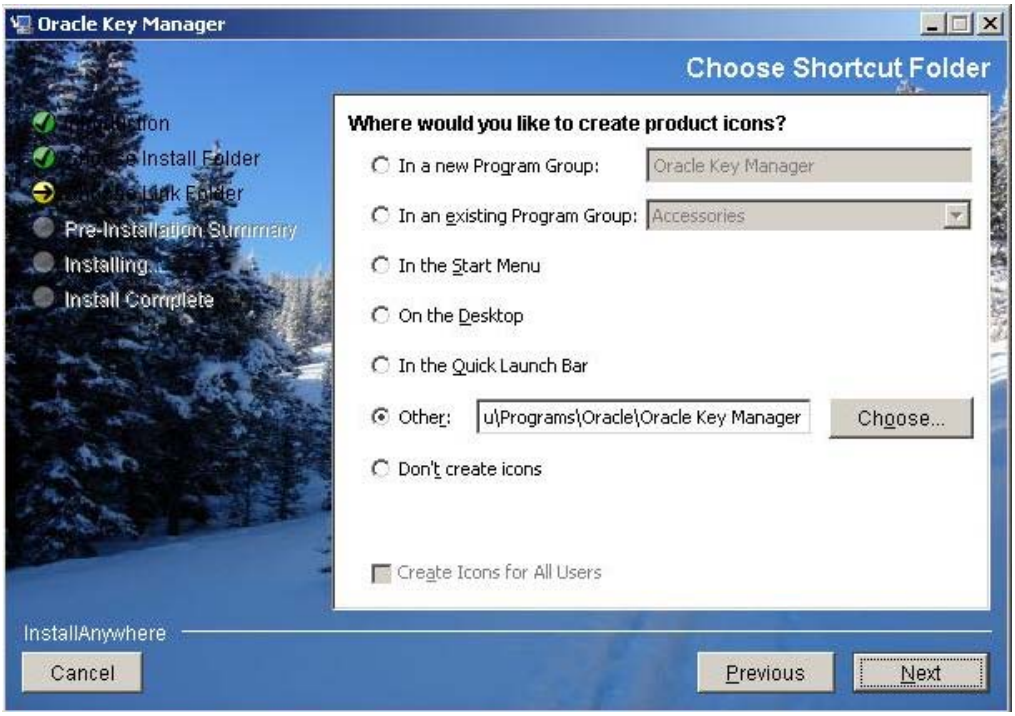
2. Select Next.

3. The Choose Install Folder window is displayed.



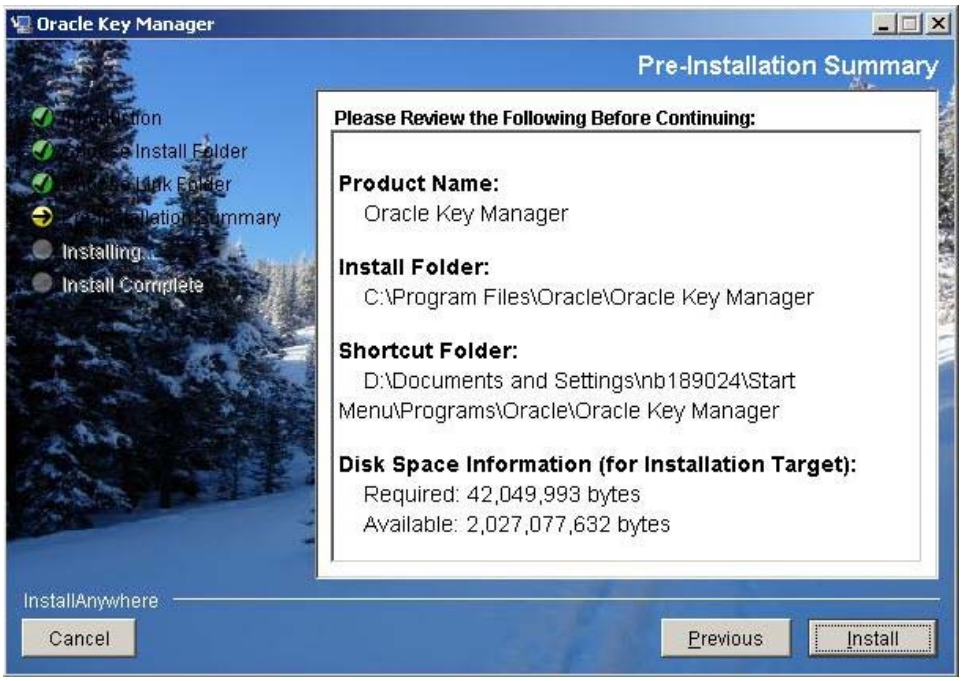
4. To select the default folder, select Next, or supply your own installation folder, and select Next.

5. The Choose Shortcut Folder window is displayed, allowing you to create the product icons where you desire.

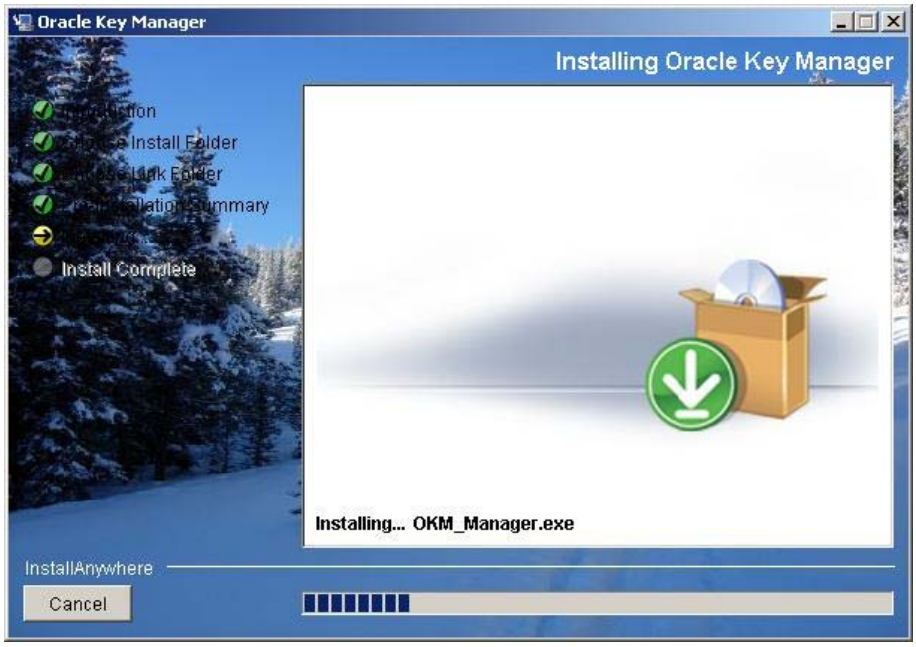


6. Select Next after you make your choice.

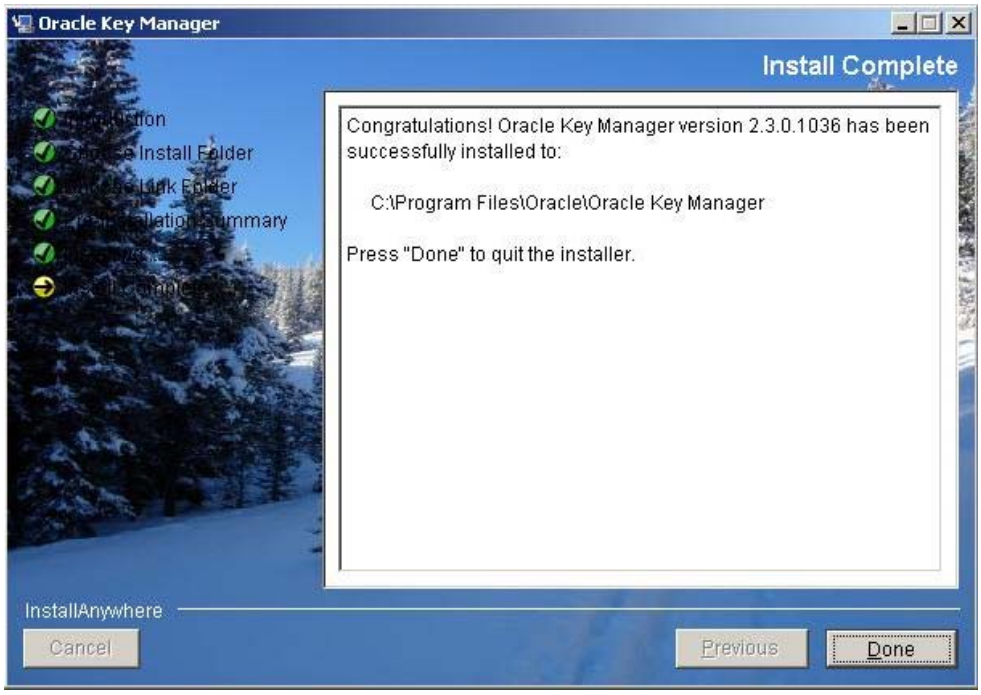
7. The Pre-Installation summary screen is displayed.



8. Select Install to install the OKM Manager, or select Previous to revise your setup.


Oracle Key Manager
Installing Oracle Key Manager
Install Complete
Installing... OKM_Manager.exe
InstallAnywhere
Cancel

9. The installation process is now complete. Select Done to exit.



Invoking the OKM Manager

Two methods can be used to invoke the OKM Manager, depending on your environment:

- Startup with Windows
- Startup with Solaris

Starting the OKM Manager with Windows

If you instructed the installation program to create a shortcut, double-click it to launch the OKM Manager application.

Otherwise, launch Windows Explorer, navigate to where you installed the OKM Manager, and invoke OKM_Manager.exe.

Starting the OKM Manager with Solaris

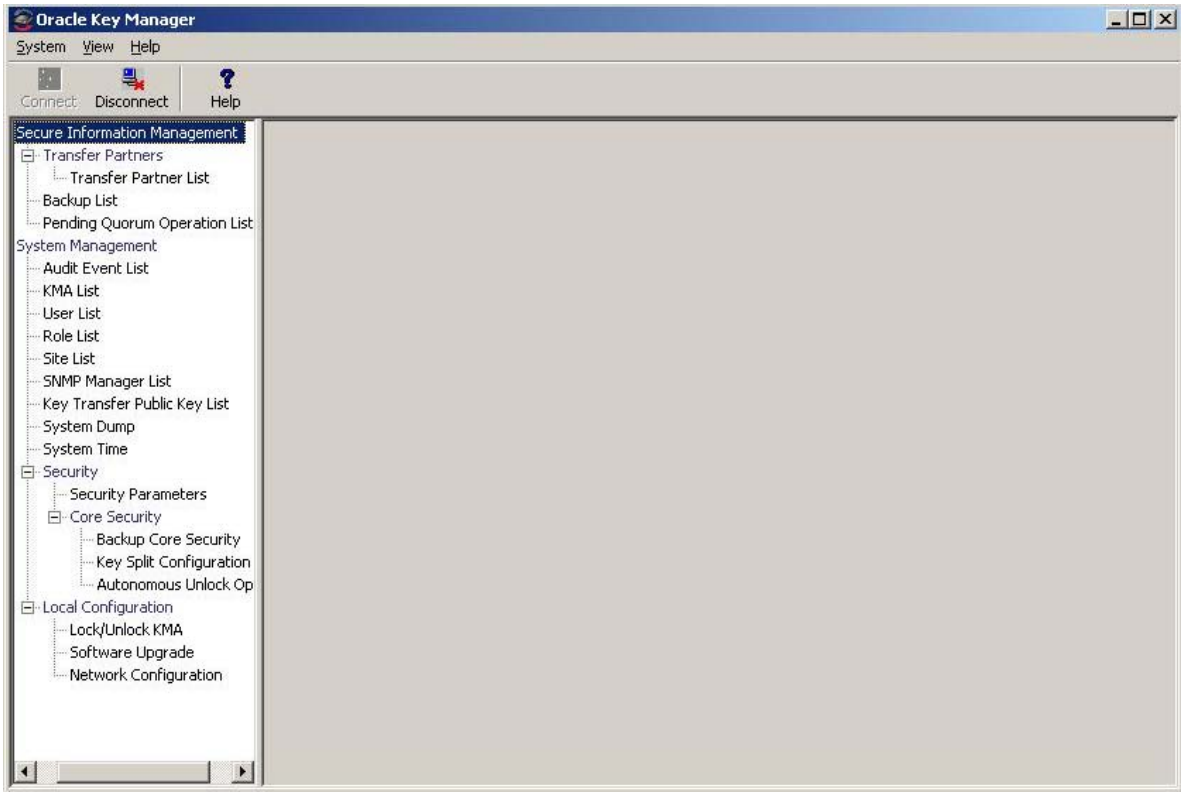
As with Windows, you can direct the installation program to create a shortcut. For example, if you create the shortcut in your home directory, you can invoke it at a shell prompt by entering:

```
~/OKM_Manager
```

Alternatively, you can navigate to where you installed the OKM Manager and invoke OKM_Manager exe.

OKM Manager GUI Overview

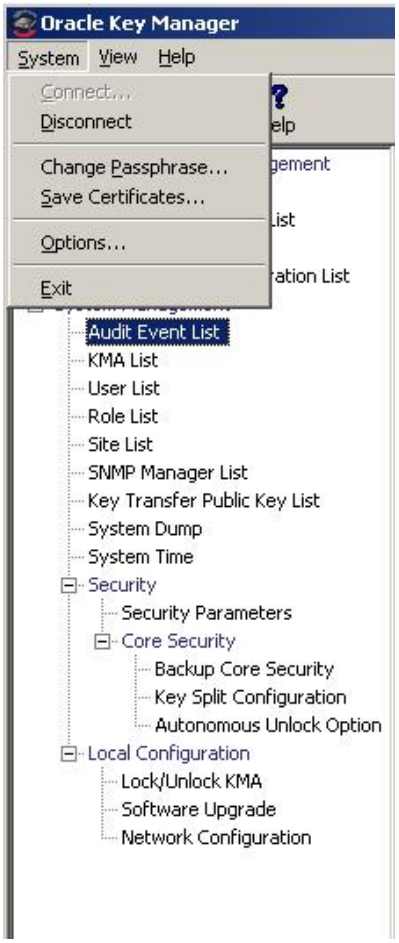
The OKM Manager GUI is shown below with a sample menu.



The OKM Manager GUI contains a System menu, View menu, and Help menu. Click the appropriate action bar item to display a menu and then select a menu item.

Toolbar buttons provide shortcuts to several menu options.

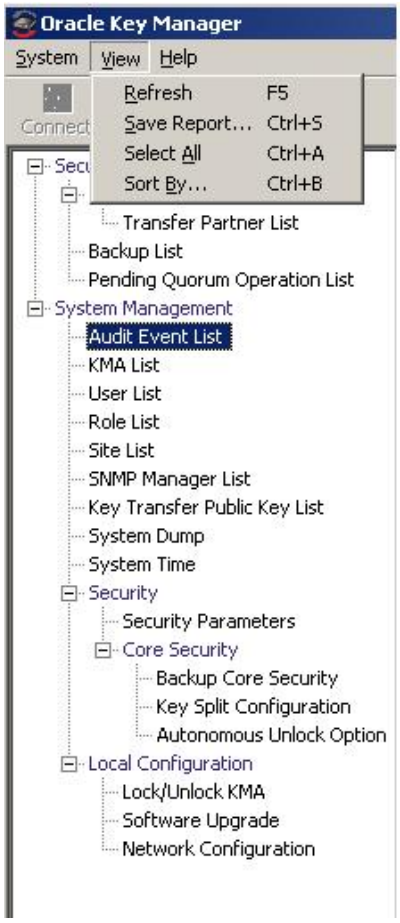
System Menu



System Menu Options

- **Connect**: Displays the Connect to Cluster dialog box that allows you to connect to a pre-existing Cluster using a Profile or to create a new Cluster profile.
- **Disconnect**: Displays the Disconnect from KMA dialog box that disconnects you from the KMA.
- **Change Passphrase**: Displays the Change passphrase dialog box that lets you modify the passphrase.
- **Save Certificates:** Displays the Save Certificates dialog box that permits you to edit the CA Certificate and Client Certificate file names.
- **Options**: Displays the Options dialog box that is used to specify various configuration settings.
- **Exit:** Closes the OKM Manager GUI.

View Menu



View Menu Options

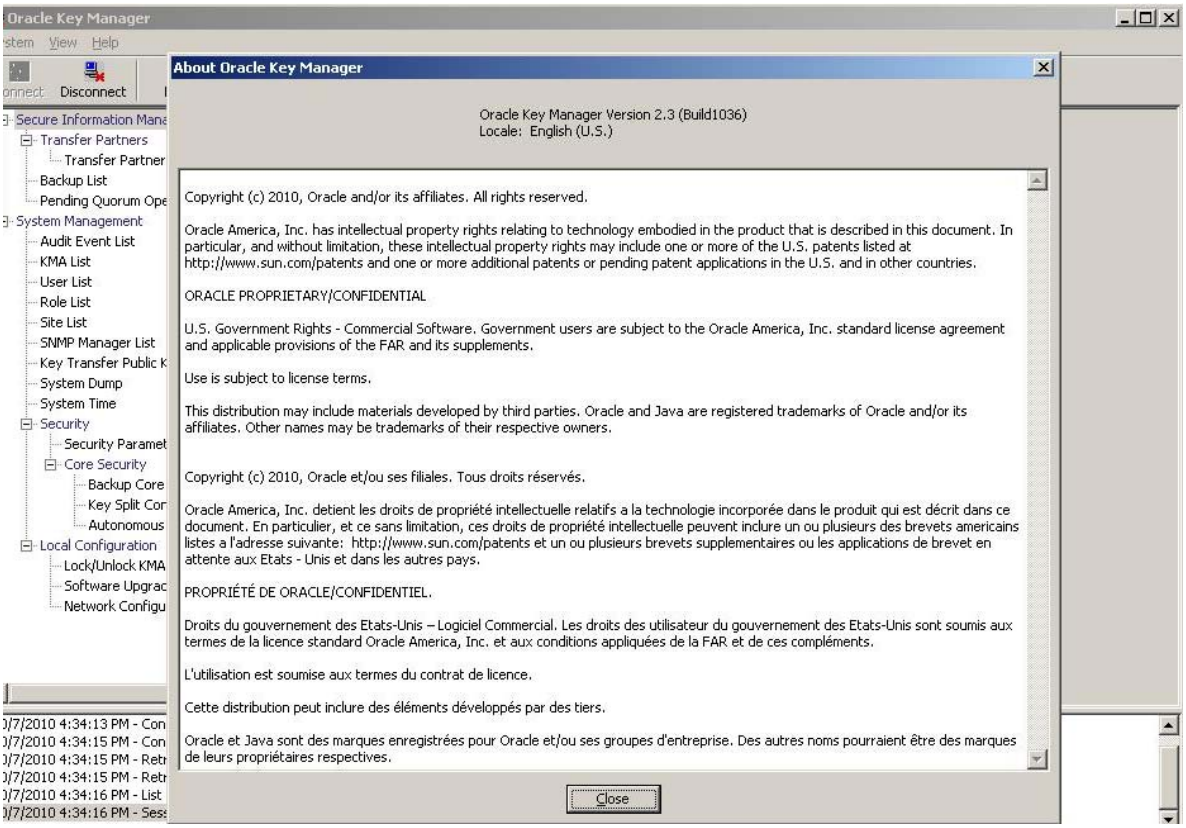
- **Refresh:** Refreshes the screen.
- **Save Report:** Save Report allows you to download the contents of any List screen. to a text file on the system where the OKM Manager is running.
- **Select All:** Select All selects all items on a List screen.
- **Sort By:** Sorts a list of items on a List screen. This is equivalent to clicking on column headings in a list.

Help Menu

Oracle Key Manager
System
View
Help
Oracle Key Manager Help... F1
About Oracle Key Manager...
Connect
Disc
Secure Information Management
Transfer Partners
Transfer Partner List
Backup List
Pending Quorum Operation List
System Management
Audit Event List
KMA List
User List
Role List
Site List
SNMP Manager List
Key Transfer Public Key List
System Dump
System Time
Security
Security Parameters
Core Security
Backup Core Security
Key Split Configuration
Autonomous Unlock Option
Local Configuration
Lock/Unlock KMA
Software Upgrade
Network Configuration

Help Menu Options

- **OKM Manager Help**: Displays the online help index and table of contents for OKM Manager.
- **About OKM Manager**: Displays the version and copyright information about OKM Manager. Click the Close button to close this dialog box.



Toolbar Buttons

The table below describes the Toolbar buttons on the OKM.

Button	Description
	Displays the Connect to KMA dialog box that allows you to connect to a KMA by selecting a profile.
	Displays the Disconnect from KMA dialog box that allows you to disconnect from the KMA.
	Displays the online help index and table of contents for OKM.

Shortcut Keys

Shortcut keys allows you to choose commands in a single step. The following shortcut keys are used:

Cuts the current selection	Ctrl+X
Copies the current selection	Ctrl+C
Copies the contents from the Clipboard to the current selection point	Ctrl+V
Brings up a dialog box to save a report to a local site	Ctrl+S

Menu Accelerator Keys

Menu accelerator keys are supported for all menu items. Hold down the “Alt” key to display the accelerator keys.

Using Online Help

You can use online help for complete information about the OKM. Online help is easy to use. You are able to view topics in various ways. You can:

- Browse a table of contents
- Search for keywords
- Use an index
- Navigate backward
- Print topics.

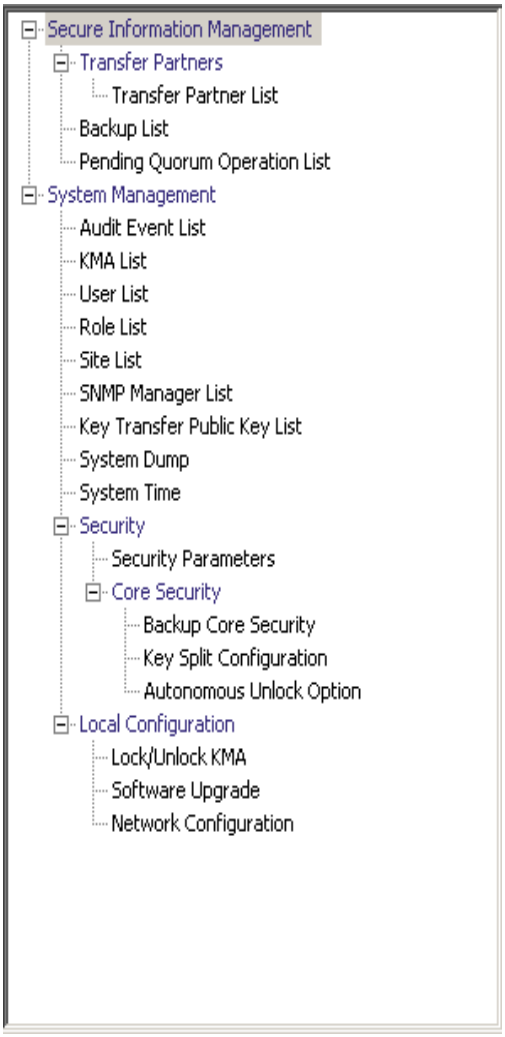
OKM Manager GUI Panes

The OKM Manager GUI includes three panes:

- OKM Management Operations Tree
- OKM Management Operation Details
- Session Audit Log.

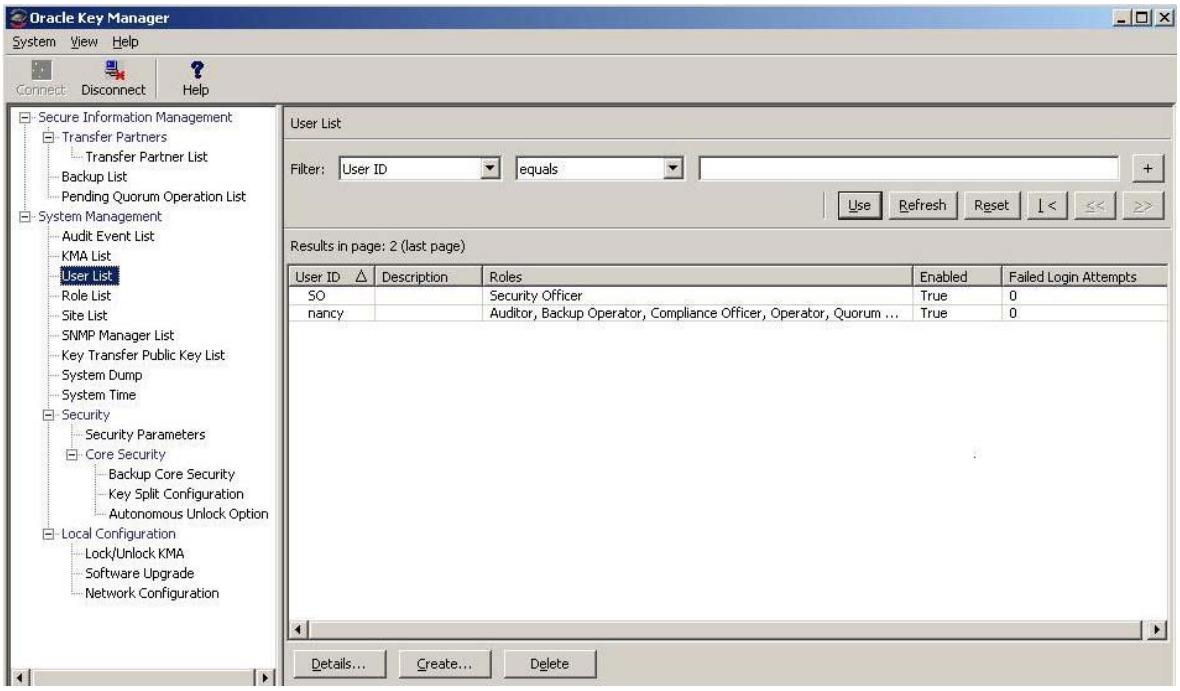
OKM Management Operations Tree Pane

The OKM Management Operations Tree pane, located on the left-side of the screen, displays all operational functions of the OKM. Depending on your assigned role(s), the options on this tree pane differ. The example below shows the operations that a Security Officer can perform.



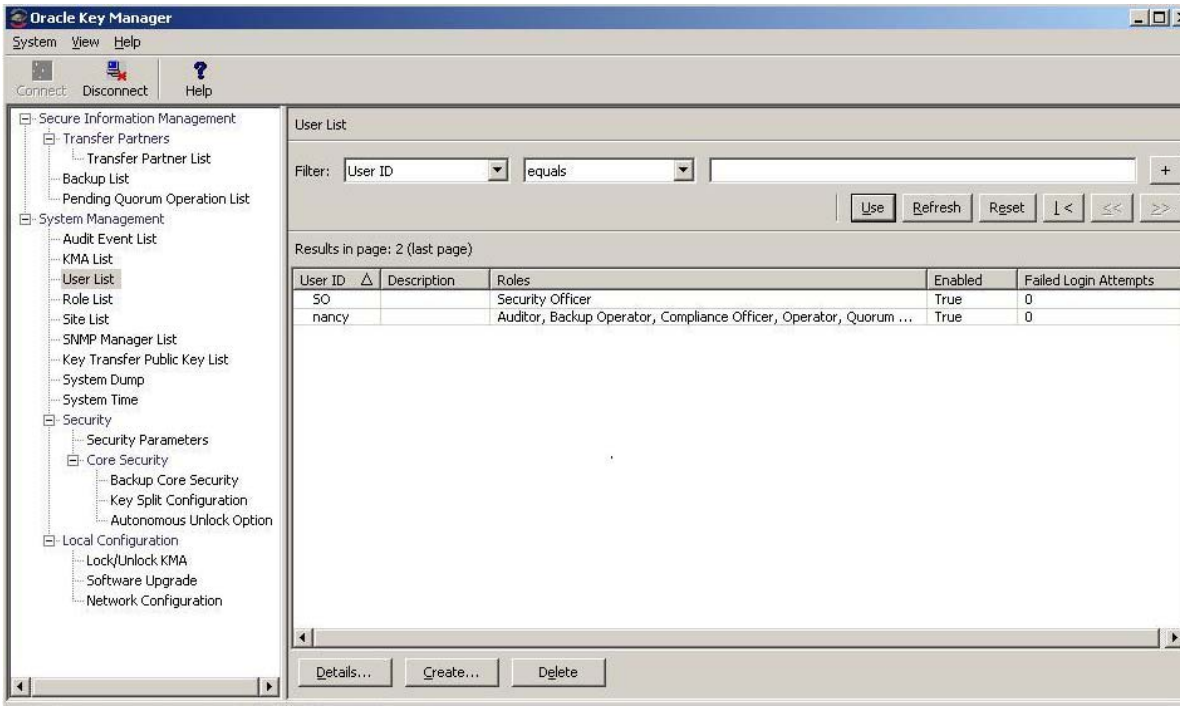
OKM Management Operation Details Pane

When an operation is selected, the OKM Manager Operation Details pane, to the right of the Operations Tree Pane, displays the required components for the selected operations. You can apply filters on the items that are displayed in list panels. The example below shows the User List, when the User List menu option was selected from the System Management menu in the Operations Tree pane.



Session Audit Log Pane

The Session Audit Log pane, below the Operations Tree Pane and the Operations Details Pane, provides a scrollable list of the most recent session events.

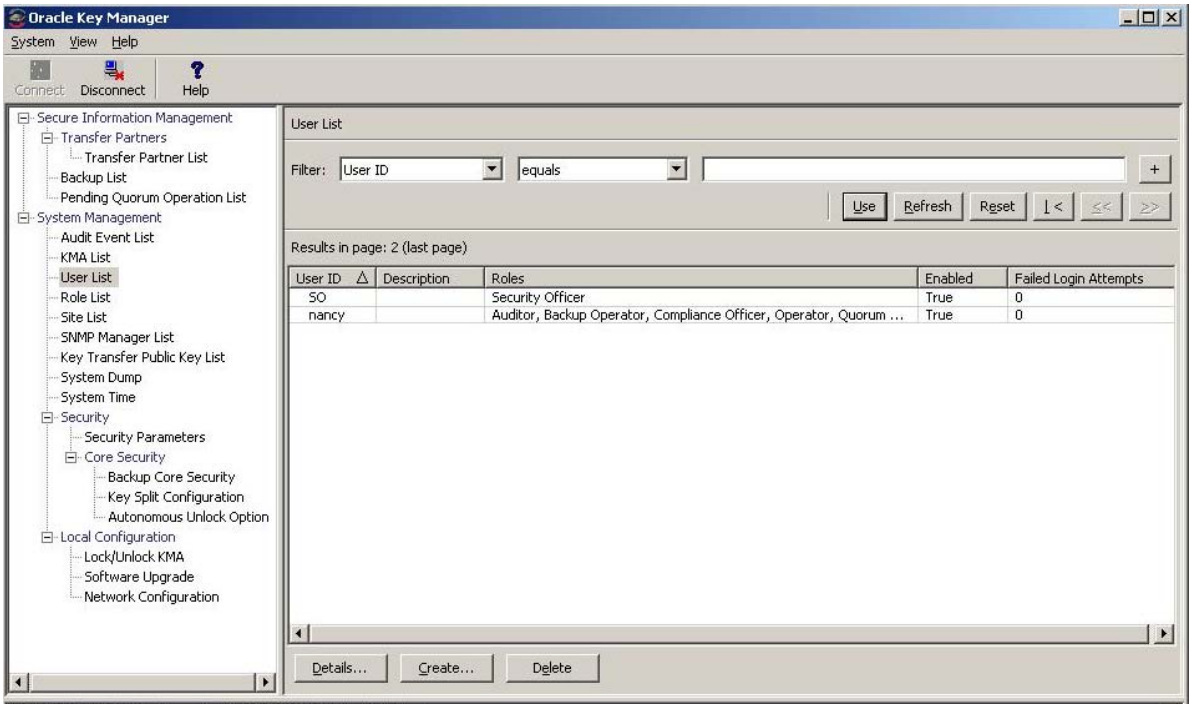


Status Bar

The Status Bar, at the bottom of the screen, is comprised of the following fields:

- **User Name:** Displays the user name of the currently logged-in user. In the screen below, the Security Officer (SO) is logged in.
- **Connection Status:** Displays the state of the current connection, that is, **Connected**
- **KMA IP Address:** Displays the Management Network IP address and Name of the target KMA.

If there is no connection to the KMA, the Status fields are blank.



Panels

The are common panel components in the OKM Manager screens. These are described below:

Title

Displays the title of the screen.

Filter

Allow you to filter the database by specific keys. It contains the following components:

Table label: Specifies the table to which the filtering applies

Filter Attribute combo box: Indicates the fields to filter

Filter Operator 1 combo box: Provides the filter operators that are applied to Filter Value 1. The filter operations are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not Empty

Filter Value 1 control: Used as a single value or the starting value of the filter key range

Filter Value 2 control: Used as a single value or the ending value of the filter key range

Use button: Applies the filter to the displayed list.

Refresh:

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of items that can be displayed on the current page. Appends "(last page)" if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

Note – If the number of records output is greater than the Query Page Size, multiple pages are displayed. Click the buttons below the filters to move between pages.

Sorting:

Click a column heading to sort the list by that field. If the output requires multiple pages, the complete set of results is sorted, then the corresponding page is returned.

Message

Displays messages that are related to database queries. It works in conjunction with the Database View list. It contains the following components:

- Static text label: Displays error messages, such as:

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

Uninstalling the OKM Manager Software

Two options are available to begin to uninstall the OKM software:

- Navigate to the directory where the uninstall program resides and launch the executable file from there
- For Windows users only, launch the Add or Remove Programs process

In both cases, the Preparing Setup window will be displayed after you finish these procedures. See "Completing the Uninstall Process" on page 85.

Invoking the Executable File

To uninstall the OKM Manager software:

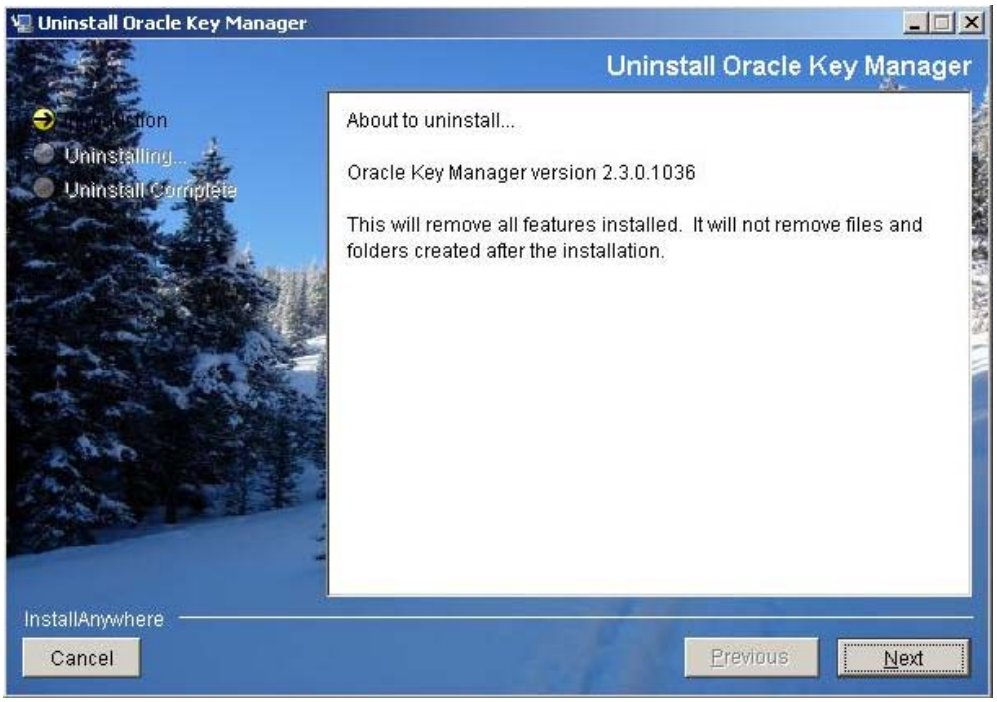
1. Navigate to the "Uninstall_Oracle_ Key_Manager" directory, which resides under the directory where the OKM Manager was installed.
2. Invoke the "Uninstall_Oracle_Key_Manager.exe" (Windows) or "Uninstall_Oracle_Key_Manager" (Solaris) executable to launch the uninstall process.
3. The Preparing Setup window is displayed, while the install/uninstall program prepares for the uninstall process.

Invoking Add/Remove Programs (Windows Only)

1. Click **Start**, select **Settings**, **Control Panel,** double-click **Add or Remove Programs**. The Add or Remove Programs window is displayed. Scroll down the list (if the software is not visible), select Sun KMS Manager, then click the Change/Remove button.
2. The Preparing Setup window is displayed, while the install/uninstall program prepares for the uninstall process.

Completing the Uninstall Process

The OKM uninstall dialog box is displayed, prompting you to confirm that you want to remove the selected application and all its features.



1. Click the Next button to continue or click the Cancel button to stop the process and return to the Add or Remove Program window (Windows) or shell prompt (Solaris).

Note – Your connection profiles will not be removed.

---

2. When the uninstall process is completed, the Uninstall Complete window is displayed. Click the Finish button to close this window. Close this window to return to the Add or Remove Program window (Windows) or shell prompt (Solaris).

CHAPTER 4

Using the System Menu

This chapter gives detailed instructions for connecting to the KMA using the OKM Manager. It also gives instructions for using the other options on the System menu.

Connecting to the Cluster

Important – Before connecting to a KMA, at least one Cluster profile must exist and a user must be created and enabled on the KMA.

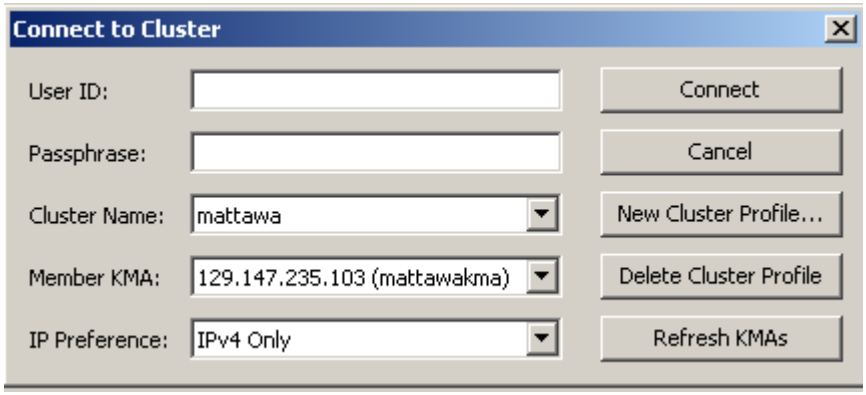
This section gives procedures for connecting to the KMA using the OKM Manager. If this is the first time that you are connecting to the KMA, you must first define a Cluster profile. On subsequent occasions, you will be able to connect to the KMA using the Cluster profile that you created. The OKM Manager uses the Cluster profile information to initiate communications with a Cluster (the KMA IP address).

Creating a Cluster Profile

To create a Cluster profile:

1. From the System menu, select Connect or from the Tool bar, click

. The Connect to Cluster dialog box is displayed. If you have pre-existing profile, the Cluster profile name and its IP address will be displayed in the Cluster Name and IP Address fields respectively.



2. Click the New Cluster Profile button. The Create Cluster Profile dialog box is displayed.

3. Complete the following parameters:

Cluster Name

Type a value that uniquely identifies the Cluster profile name.

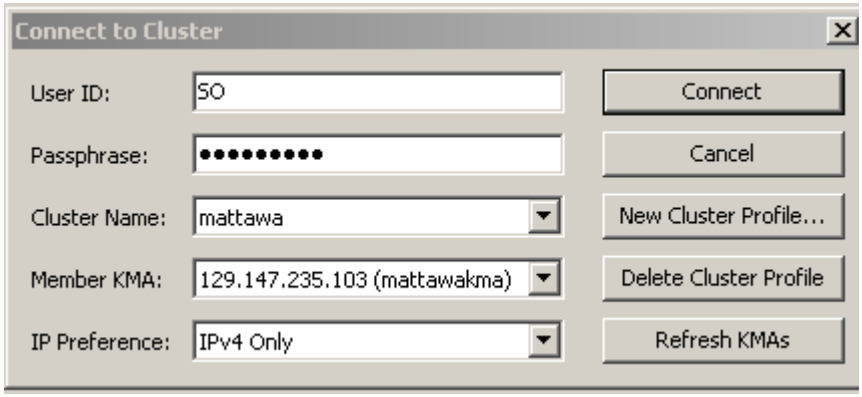
Initial IP Address or Host Name

Type the Service Network IP address or Host Name of the initial KMA in this Cluster to connect to. The choice of which network to connect to depends on what network the computer system where the OKM Manager is running is connected to.

Note – You only have to create a single Cluster profile because covers the entire Cluster and can be used by any user (of the Agent). The only reason that you would want to create another Cluster profile is if you want to establish a second Cluster or you have changed the IP addresses of all KMAs in the current Cluster.

---

4. Click the OK button. The Connect to Cluster dialog box is displayed with the Cluster profile information you created.



5. Complete the following parameters and click the Connect button:

User ID

Type the name of the user who will connect to specified KMA, or if this is the first time that you are connecting to the KMA after performing the initial QuickStart process, type the name of the Security Officer created during the QuickStart.

Passphrase

Type the passphrase for the selected user.

Cluster Name

Select the Cluster to connect to.

Member KMAs

Select the KMA to connect to within that Cluster.

IP Preference

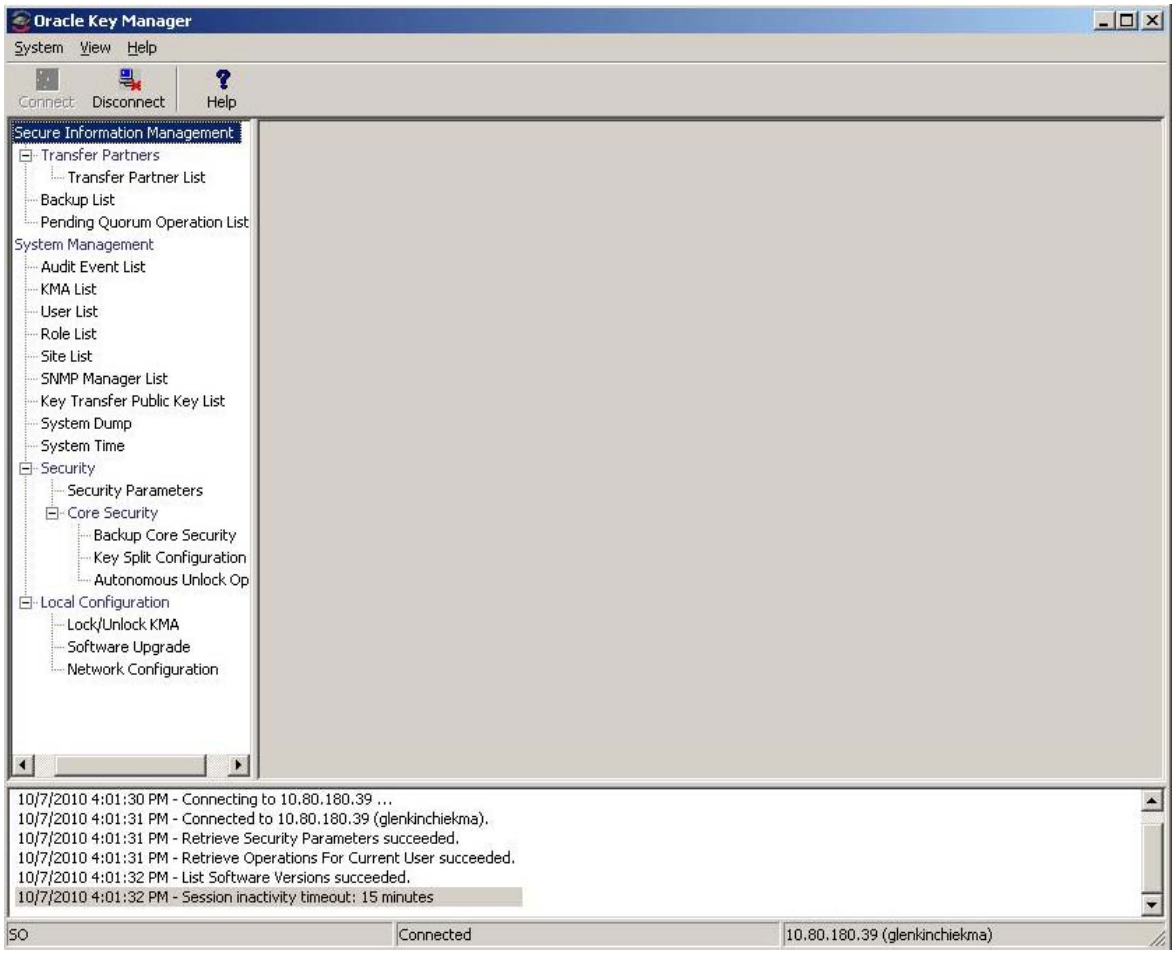
Select the Internet Protocol version you want, IPv4 only, IPv6 only, or IPv6 preferred.

Note – If a KMA has joined the Cluster after you have connected to that Cluster, that KMA does not appear in the Member KMAs list. To update the list, enter the user name and passphrase, choose a Cluster profile, and click the Refresh KMAs button.

Important – The KMA authenticates the user ID and passphrase. The returned list of KMA IP addresses is used to populate the Cluster profile and is stored on the host. The next time you connect to the KMA, you can enter the user name and passphrase, choose a Cluster profile, and select a KMA.

---

6. If the connection is successful, the Status bar of the OKM Manager GUI displays the user name and alias, the KMA's connection status (**Connected**), the KMA's IP address.



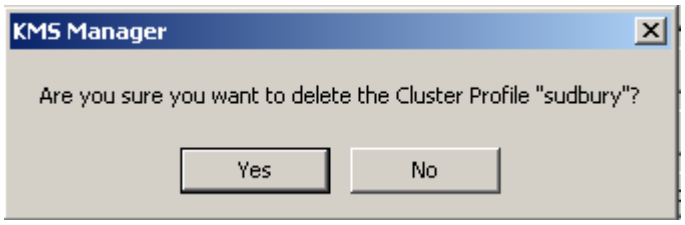
7. You can now use the OKM Manager to perform various operations. See Chapter 5 through Chapter 9 for the operations that various user roles can perform.

Note – Depending on the role assignment, the tasks in the KMA Management Operations Tree pane differ.

Deleting a Cluster Profile

To delete a Cluster profile:

1. From the Connect to Cluster dialog box, click the down-arrow beside the Cluster Name field, highlight the Cluster profile that you want to delete and click the Delete Cluster Profile button. The Delete Cluster Profile dialog box is displayed, prompting you to confirm that you want to delete the selected Cluster profile.



2. Click the Yes button to delete the Profile. The Cluster Profile is deleted and you are returned to the Connect to Cluster dialog box.

Disconnecting from the KMA

To disconnect from the KMA:

1. From the System menu, select **Disconnect** or from the Tool bar, click

. You are immediately disconnected from the KMA and the OKM Cluster. The session Audit Log pane indicates the date and time when you disconnected from the KMA.

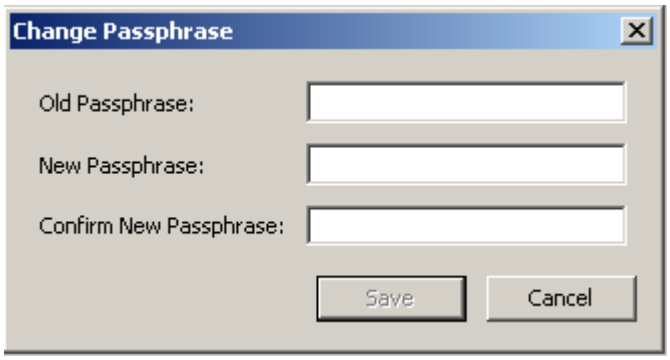
Changing the Passphrase

Note – This menu option is only enabled if you are connected to a KMA using a profile.

This function allows users to change their own passphrases. This function does not invalidate a user's current certificate.

To change a connected user's passphrase:

1. From the System menu, select **Change Passphrase...**. The Change Passphrase dialog box is displayed.



2. Complete the following parameters and click the OK button:

Old Passphrase

Type the user's old passphrase.

New Passphrase

Type the user's new passphrase.

Confirm New Passphrase

Retype the same passphrase.

3. The following message is displayed in the session Audit Log pane, indicating the date and time when you changed the user's passphrase.

Saving Certificates

This function allows you to export certificates that can be used by the OKM Command Line utility (refer to "OKM Command Line Utility" on page 360).

The Root CA Certificate is a public certificate saved in PEM format and can be used for Command Line Interface (CLI) operations as a PEM file.

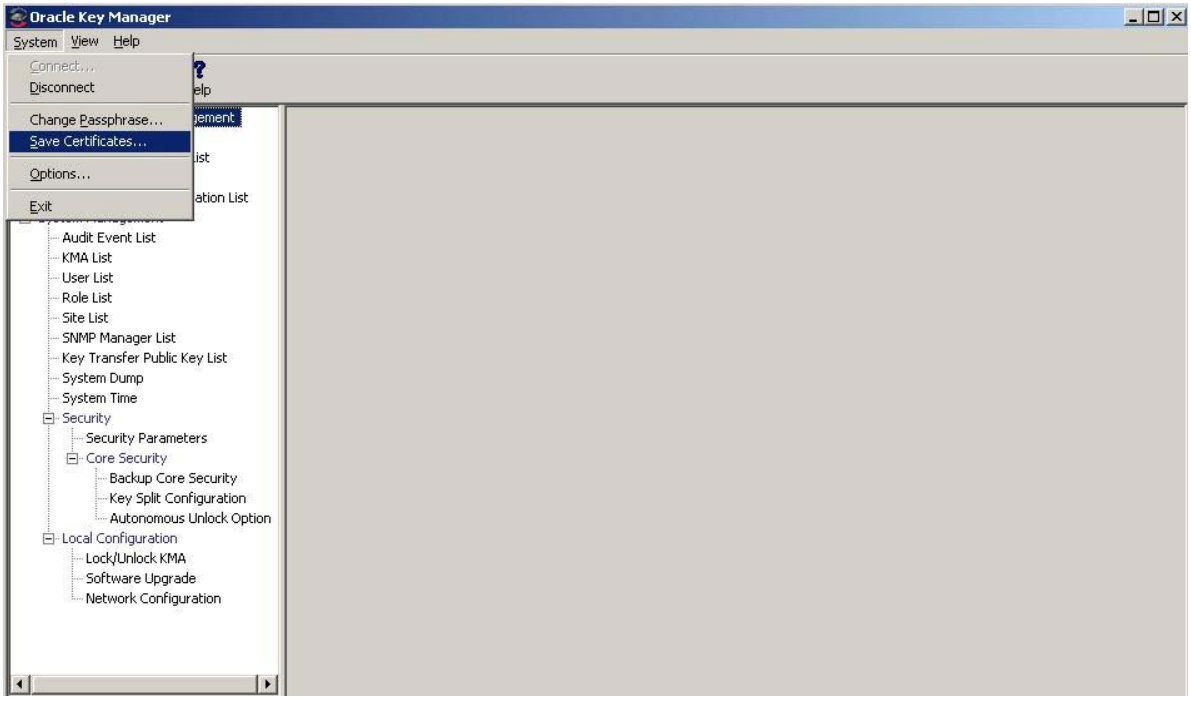
The Client Certificate can be saved in either PEM format or PKCS12 format. The PEM format contains the certificate and the unencrypted private key. A Client Certificate saved in this format can be used for CLI operations as a PEM file.

The PKCS12 format is encrypted. A Client Certificate saved in this format must be converted to PEM format before being used for CLI operations (see "Converting PKCS12 Format to PEM Format" on page 95). A password to use for encryption is required to save a Client Certificate in PKCS12 format. This password must contain at least 8 characters.

Note – You should store these certificate files in a secure location with sufficient permissions to restrict access by other users. **If you save the Client Certificate in PKCS12 format, then you must retain the password.**

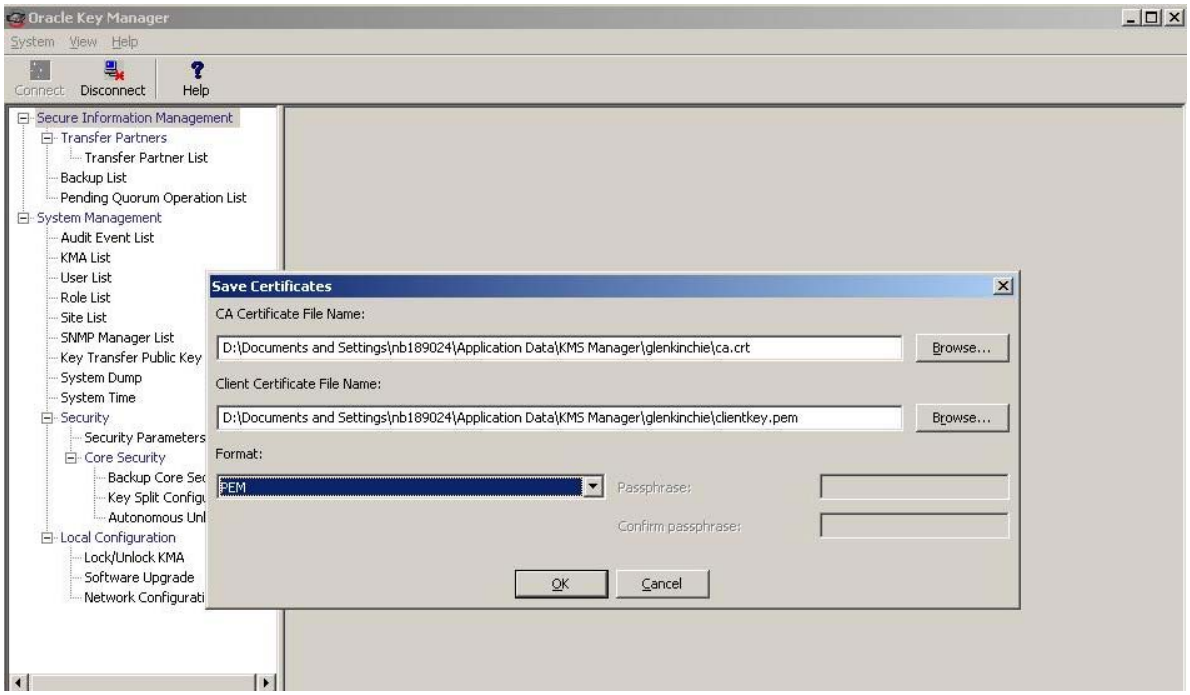
To save the certificates:

1. From the System menu, select Save Certificates.



Note – The Save Certificates menu option is enabled only if the user is connected to a KMA.

The Save Certificates dialog is displayed, with automatically-generated filenames for the Root CA Certificate and the Client Certificates.



You can edit these filenames directly or click Browse to select a different destination path or edit the filenames.

2. In the Format field, select the format that the Client Certificate should be in when it is exported.
3. If you selected the PKCS12 format, type a passphrase in the Passphrase field and retype this passphrase in the Confirm Passphrase field.
4. Click OK to export these certificates. When these certificates have been exported, a message is displayed, indicating the locations of these files.
5. Click Cancel to close this dialog and return to the previous screen.

Converting PKCS12 Format to PEM Format

If you saved the Client Certificate in PKCS12 format, then you must convert it to PEM format before you can use it with the OKM Command Line utility. Use the `openssl` utility to convert it.

The `openssl` utility appears in the OpenSSL directory under the directory where the OKM Manager GUI and the OKM Command Line utility are installed.

The syntax is:

```
openssl pkcs12 -in PKCS12file -out PEMfile -nodes \
-passin mypassword
```

For example:

```
openssl pkcs12 -in KeyTransferOperator.p12 -out
KeyTransferOperator.pem -nodes -passin pass:1234Five
```

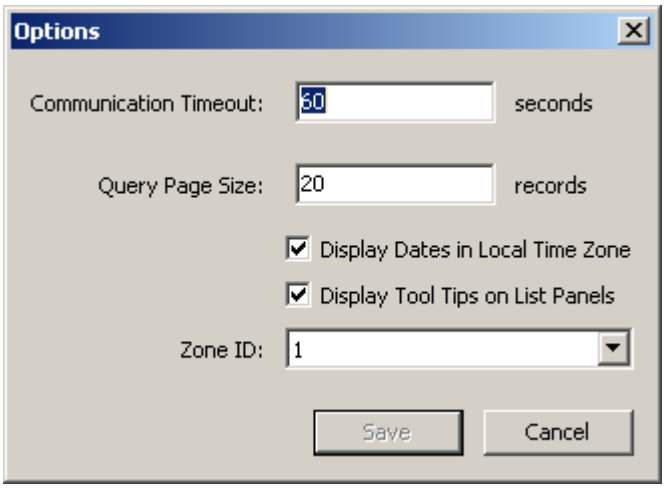
The -nodes argument is necessary to export the private key. Since the private key is not password protected, you should appropriately manage this file.

Specifying the Configuration Settings

To specify the configuration settings:

1. From the System menu, select Options.... The Options dialog box is displayed, showing the current configuration settings.

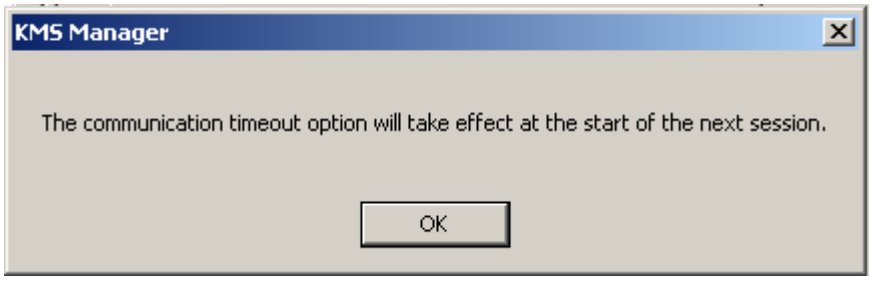
Note – The options selected are stored in the Windows Registry or in "`~/.KMS Manager`" for other platforms (where ~ is the user's home directory). The Windows Registry key for these values is "`My Computer\HKEY_CURRENT_USER\Software\Sun Microsystems\KMS Manager`."



2. Modify the following parameters, as required and click the Save button:

Communication Timeout

Type a timeout period (in seconds) for communications with the connected KMA. If the KMA does not respond within the timeout value, the OKM Manager will give up on the communication. The minimum value is 1; the maximum value is 60. The default is 15.



Query Page Size

Type the maximum number of items to display on a screen, dialog, or tab on a dialog that displays a list of items. Paging can be used to view a list longer than this limit. The minimum value is 1; the maximum value is 1000. The default is 20.

Display Dates in Local Time Zone

Select this check box to display all dates and times in the local machine's time zone (i.e., where the OKM Manager is running), rather than UTC. The default is selected. The following confirmation message is displayed.

Display Tool Tips on List Panels

Select this check box if you want to see a tool tip when you position the cursor over an item. This is the default.

Zone ID

If your KMAs are configured to have IPv6 addresses and if you want to connect to one of them using an IPv6 link-local address (that is, one that begins with "fe80"), then select a Zone ID to use when connecting to that link-local address.

See "IPv6 Addresses with Zone IDs" on page 98 for more information.

IPv6 Addresses with Zone IDs

For Windows system users, the OKM Manager GUI and the Backup and OKM Command Line utilities (see "Command Line Utilities" on page 359) allow you to enter link-local IPv6 addresses, however, you must perform some initial setup first.

Note – You must enter a Zone ID whenever you specify a link-local address (that is, an IPv6 address that begins with "fe80"). You can specify a Zone ID by appending it to the end of an IPv6 address, following a percent sign (%).

---

1. Display a command prompt window and determine which Zone IDs are available on your Windows system.

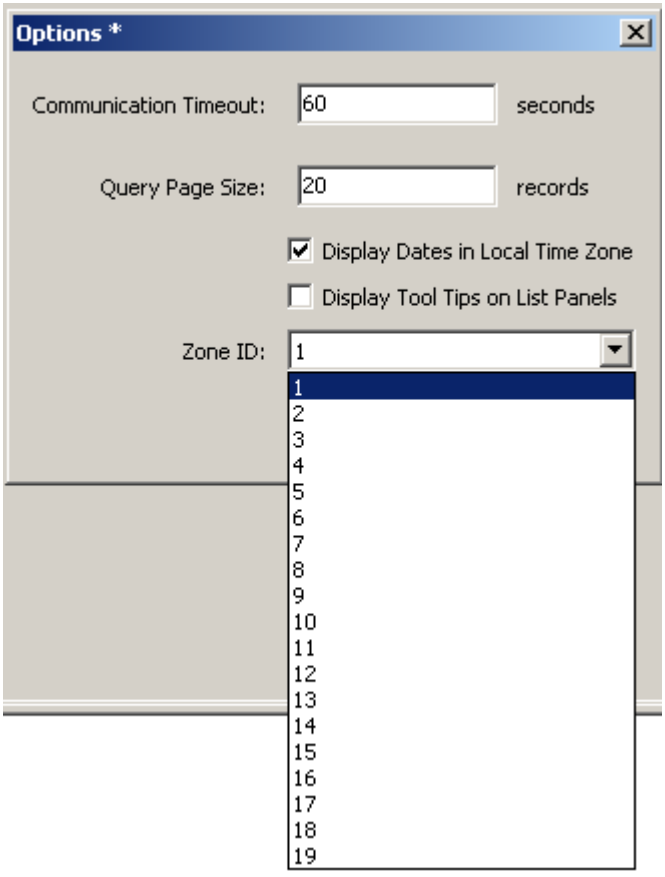
```
netsh interface ipv6 show interface
```

   The Zone IDs appear in the **Idx** column in the output of this command. Look for entries that show a **State** of "Connected."

2. Use the **ping** command to confirm network connectivity using one of these Zone IDs. For example:

```
ping fe80::216:36ff:fed5:fba2%4
```

3. Before you bring up the Connect dialog in the OKM Manager GUI, display the Options dialog and select the appropriate Zone ID.



4. Click the Save button.

Exiting from the OKM Manager

To exit from the OKM Manager:

1. From the System menu, select **Exit** or from the Title bar, click . The OKM Manager closes and you are returned to the Windows desktop.
2. The OKM Manager immediately disconnects if connected and closes.

CHAPTER 5

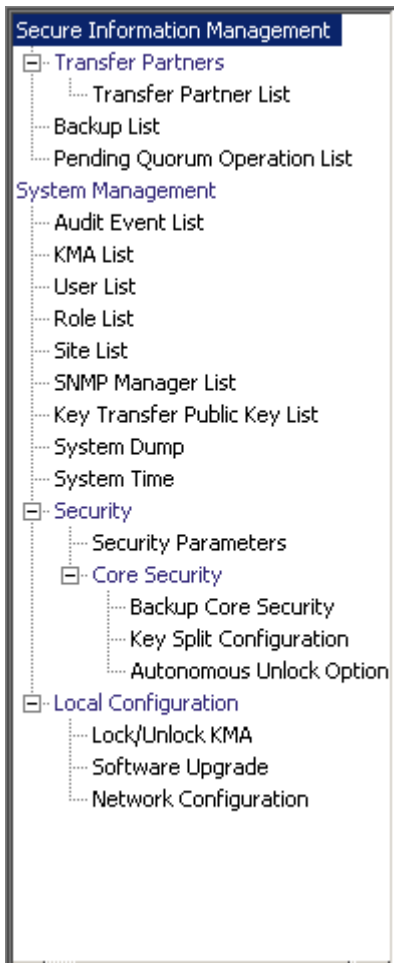
Security Officer Operations

A Security Officer manages security settings, users, sites, and Transfer Partners. This chapter describes the following:

- Operations that a user who has been given a Security Officer role can perform. If you have been assigned multiple roles, refer to the appropriate chapter for instructions on performing the specific role.
- Procedures for enabling and disabling a technical support account.

Security Officer Role

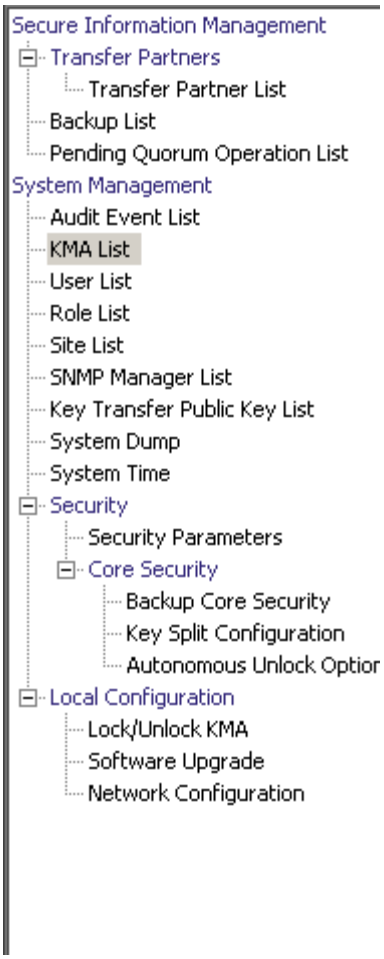
As a Security Officer, you can manage the entities (KMAs, users, sites, Transfer Partners) as well as various security aspects of the system.



KMA List Menu

The KMA List menu option allows you to:

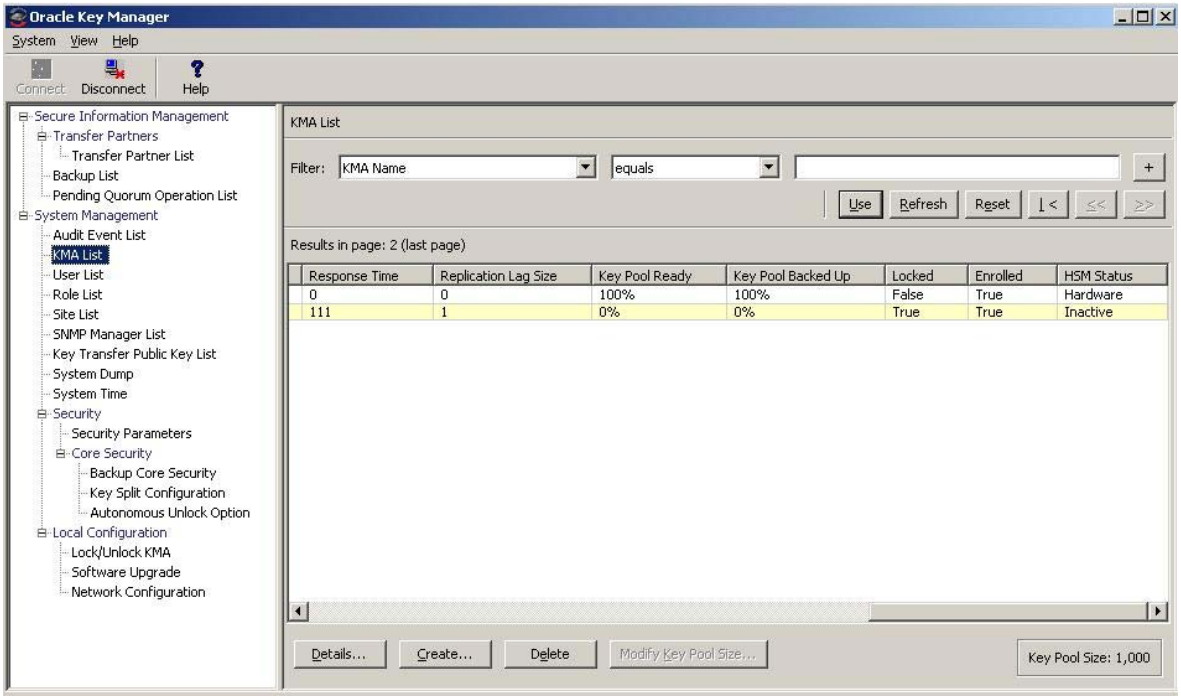
- View KMAs
- Create a KMA
- Modify a KMA's information
- Delete a KMA
- Modify a Key Pool size (refer to "Modifying a Key Pool Size" on page 307). This is a Backup Operator function.



Viewing KMAs

To view KMAs:

From the System Management menu, select KMA List. The KMA List screen is displayed.



You can also scroll through the database and filter the KMA list by any of the following keys:

- KMA Name
- Description
- Site ID
- Management Network Address
- Service Network Address
- Management Network Address (IPv6)
- Service Network Address (IPv6)
- Version
- Failed Login Attempts
- Enrolled

The **Use** button applies the filter to the displayed list for the KMA.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- KMA Name
- Description
- Site ID
- Management Network Address
- Service Network Address
- Management Network Address (IPv6)
- Service Network Address (IPv6)
- Version
- Failed Login Attempts
- Enrolled

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value 1 box:

Type a value in this field.

Use:

Click this button to apply the filter to the displayed list.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

KMA Name

Displays the user-supplied identifier that distinguishes each KMA in a Cluster.

KMA ID

Displays a system-generated unique identifier that identifies the KMA.

Description

Describes the KMA.

Site ID

Describes the site to which the KMA belongs.

Management Network Address

Displays the IP address of the KMA on the management network.

Service Network Address

Displays the IP address of the KMA on the service network.

Management Network Address (IPv6)

Displays the IPv6 address (if any) of the KMA on the management network.

Service Network Address (IPv6)

Displays the IPv6 address (if any) of the KMA on the service network.

Version

Displays the version number of the KMA software.

Failed Login Attempts

Displays the number of times that an attempted logon has failed.

Responding

Indicates whether the KMA is running. Possible values are True or False.

Response Time

Displays the time (in milliseconds) that the KMA takes to respond to a request.

Replication Lag Size

Displays the number of updates waiting to be replicated.

Key Pool Ready

Displays the percentage of unallocated keys that are ready.

Key Pool Backed Up

Displays the percentage of the Key Pool that has been backed up.

Locked

Indicates whether or not the KMA is locked.

Note – The **Key Pool Backed Up** and **Locked** fields show an "N/A" value if that KMA does not support these features.

Enrolled

Indicates whether the KMA has been added or logged into the Cluster successfully. Possible values are True or False.

HSM Status

Indicates the status of the Hardware Security Module (HSM). Possible values are Unknown, Inactive, Software, Hardware, SW Error, or HW Error.

Unknown

The KMA is running a software release older than OKM 2.3.

Inactive

The KMA currently does not need to use the HSM, typically because the KMA is locked.

Software

The HSM is not functional, and the KMA is using the software provider to generate Keys.

Hardware

The HSM is functional, and the KMA is using it to generate Keys.

SW Error/HW Error

The KMA encountered an error when it tried to query the status of the software provider (SW Error) or the HSM (HW Error).

Notes –

Normally, the HSM is functional (Hardware). However, if the HSM becomes non-functional (Software) and the FIPS Mode Only security parameter is set to Off (see "Retrieving the Security Parameters" on page 189), then the KMA switches to using the software provider to generate Keys.

If the HSM becomes non-functional and the FIPS Mode Only security parameter is set to On, then the KMA cannot generate Keys.

If the value is Software, SW Error, or HW Error, check the Sun Crypto Accelerator (SCA) 6000 card on this KMA (see "Checking the SCA 6000 Card").

Checking the SCA 6000 Card

It is possible that an existing KMA in a Cluster may contain a failed SCA 6000 card. To identify a failed card, examine the rear of the KMA server and check the LEDs on the card.

A functional SCA 6000 card on a KMS 2.1, 2.2, or OKM 2.3 KMA that has been initialized through the QuickStart program displays a flashing green Status LED (identified with an S) and solid green FIPS (F) and Initialized (I) LEDs.

If the Status LED is not flashing green and the FIPS and Initialized LEDs are not solid green, then the KMA has a faulty SCA 6000 card, and the KMA must be replaced if FIPS mode is required.

See the *SCA 6000 User Guide* for a description of the LEDs on an SCA 6000 card.

If you want to create a KMA, click the Create button. For more information, refer to "Creating a KMA" on page 109 below.

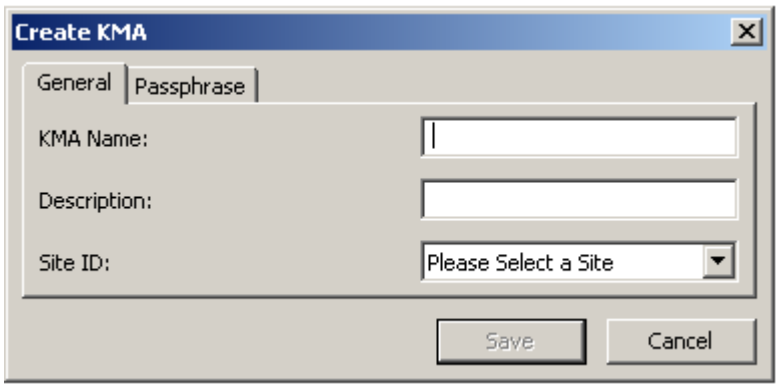
If you want to view / modify a KMA's details, highlight the KMA and click the Details button. For more information, refer to "Viewing/Modifying a KMA's Details" on page 112.

If you want to delete a KMA, click the Delete button. For more information, refer to "Deleting a KMA" on page 117.

Creating a KMA

To create a KMA:

1. From the KMA List screen, click the Create button. The Create KMA dialog box is displayed, with the General tab active.



2. Complete the following parameters:

General Tab

KMA Name

Type a value that uniquely identifies the KMA in a Cluster. This value can be between 1 and 64 (inclusive) characters.

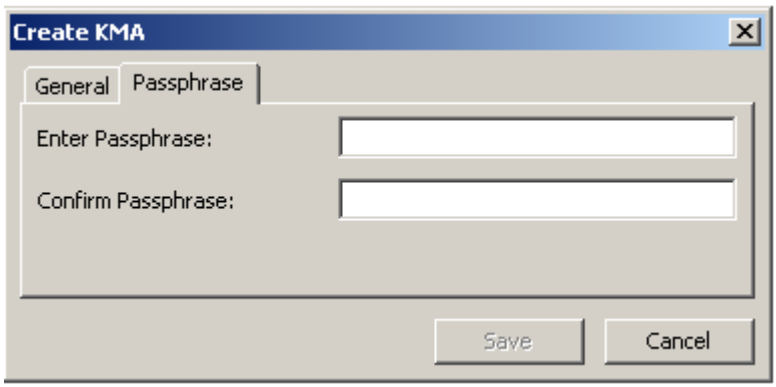
Description

Type a value that uniquely describes the KMA. This value can be between 1 and 64 (inclusive) characters.

Site ID

Click the down-arrow and select the site to which the KMA belongs. This field is optional.

3. Open the Passphrase tab.



4. Complete the following parameters and click the Save button.

Enter Passphrase

Type the passphrase for this user. The minimum value is 8 characters; the maximum value is 64 characters. The default value is 8.

Passphrase requirements:

- A passphrase must not contain the user's KMA Name.
- A passphrase must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.

  The following special characters are allowed:

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

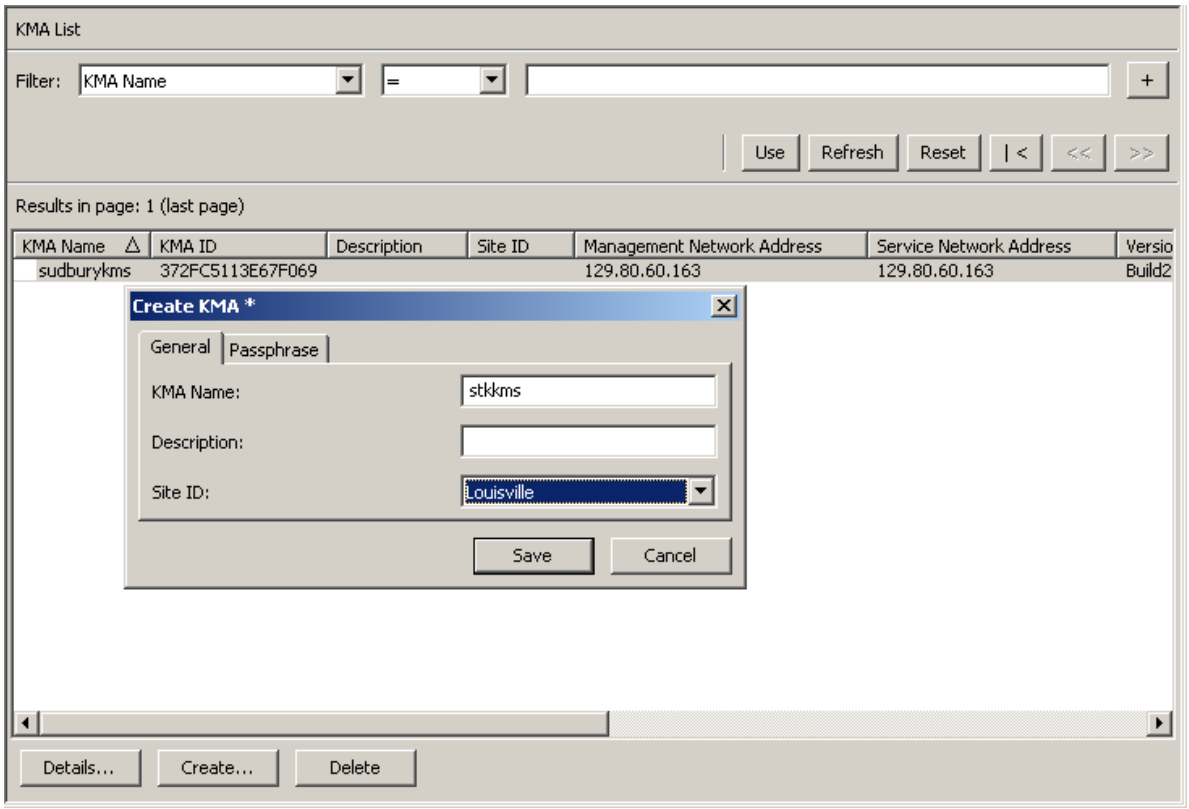
- Control characters, including tabs and linefeeds, are not allowed.

Note – To modify the minimum length requirement for passphrases, see "Modifying the Security Parameters" on page 192.

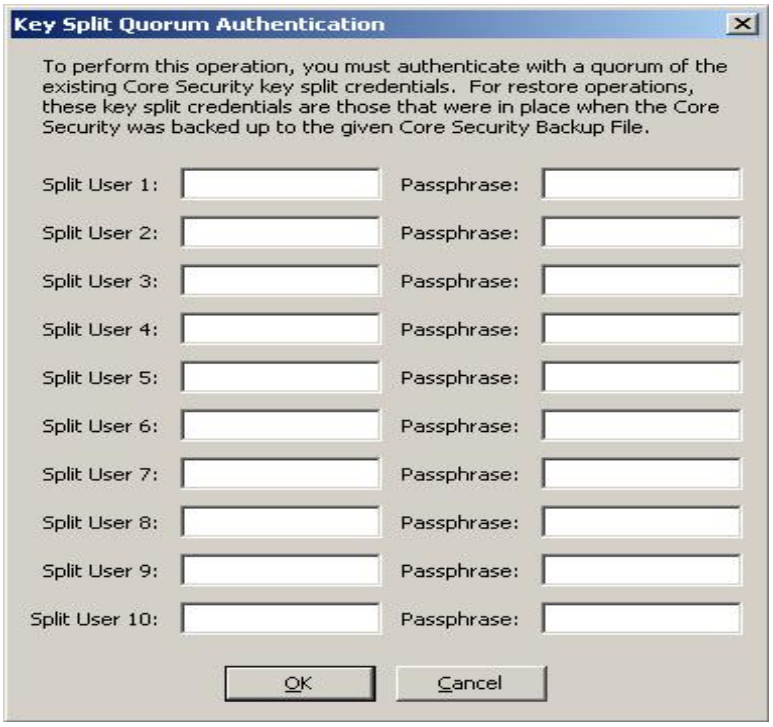
Confirm Passphrase

Type the same value that you entered in the Enter Passphrase field.

5. The KMA record is added to the database and the entry is displayed in the KMA List screen.



6. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

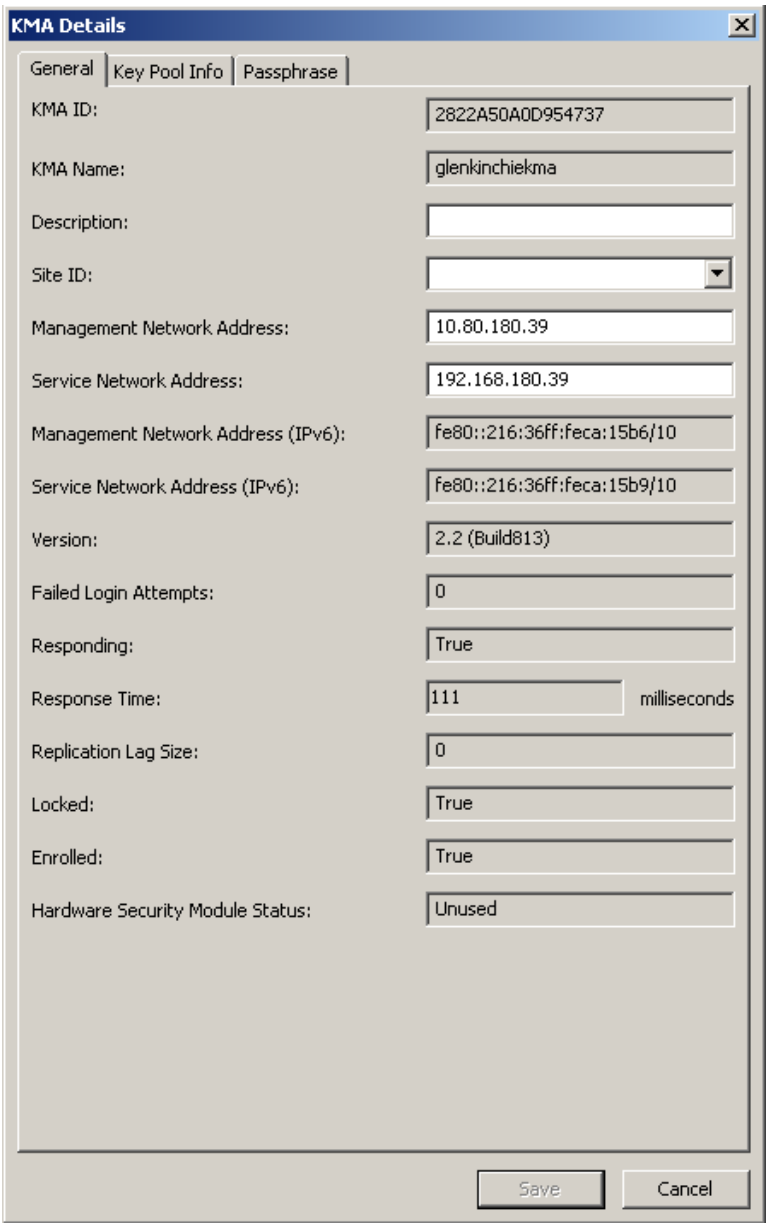
7. You must now run the QuickStart program on the KMA(s) you created so that they can join the Cluster. For procedures on joining a Cluster, refer to "Joining an Existing Cluster" on page 46.

Viewing/Modifying a KMA's Details

Note – If you are not a Security Officer, when you view a KMA's detailed information, all fields, including the Save button are disabled.

To modify a KMA's details:

1. From the KMAs List screen, double-click a KMA entry for which you want more detailed information or highlight a KMA entry and click the Details button. The KMA Details dialog box is displayed.



2. On the General tab, change the following fields:
- Description
- Site ID.

3. On the Key Pool Info tab, the following display-only fields appear:

Ready Keys

Displays the number of Keys that have been generated on this KMA and that have been backed up (for a single-node Cluster) or replicated to other KMAs (for a multi-node Cluster), but have not yet been given out to Agents for encryption.

Backup-Up Ready Keys

Displays the number of Ready Keys in the Key Pool that have been backed up. N/A means that the KMA cannot determine this value, because either the KMA runs down-level software or it is currently using a lower replication version.

Generated Keys

Displays the number of Keys that have been generated on this KMA but have not been backed up (for a single-node Cluster) or replicated to other KMAs (for a multi-node Cluster).

Key Pool Ready

Displays the percentage of Keys in the Key Pool that are ready to be used.

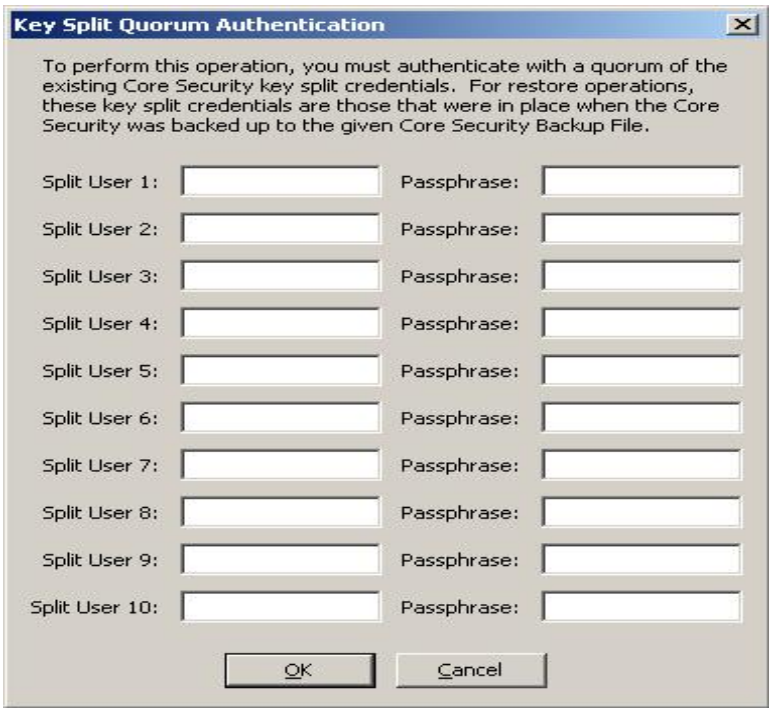
Key Pool Backed Up

Displays the percentage of Ready Keys in the Key Pool that have been backed up. N/A means that the KMA cannot determine this value, because either the KMA runs down-level software or it is currently using a lower replication version.

4. Open the Passphrase tab and modify the following parameters:
- Passphrase
- Confirm Passphrase (retype the same passphrase).

5. When you are finished, click the Save button. The KMA record in the database is modified.

6. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

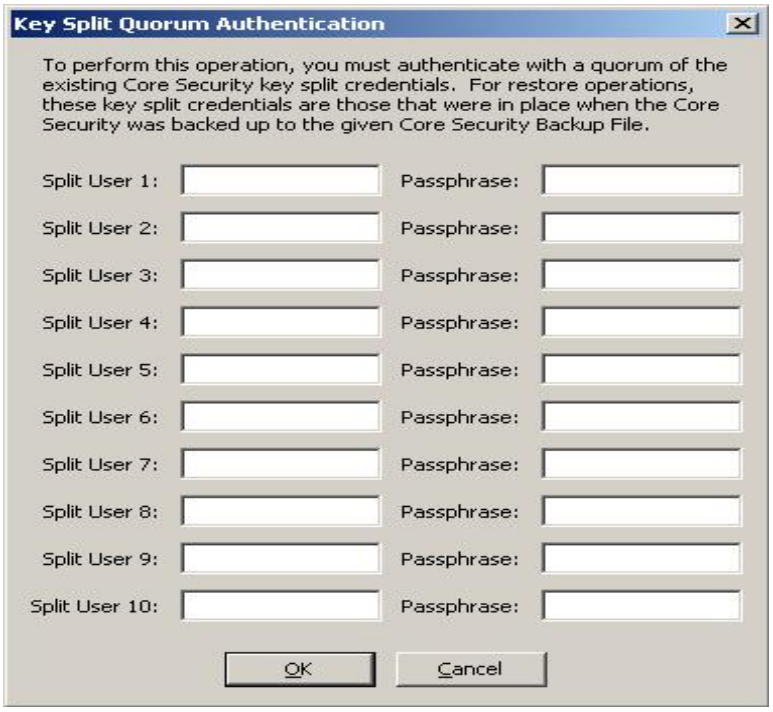
Setting a KMA Passphrase

Note – You can change a KMA's passphrase, provided you are not connected to it.

When you are creating a new Cluster, a random passphrase is automatically assigned to the KMA that is used to create the new Cluster. If the KMA wants to retrieve an entity's certificate from another KMA in the Cluster because its certificate has expired, then you would have to use this function to set the passphrase to a known value.

To set a KMA's passphrase:

1. From the KMA List screen, double-click the KMA entry or highlight a KMA entry and click the Details button. The KMA Details dialog box is displayed, with the General tab active.
2. Open the Passphrase tab and modify the following parameters:
   - Passphrase
   - Confirm Passphrase (retype the same passphrase).
3. Click the Save button to save the changes. The database entry for the KMA is changed.
4. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

5. Using the Console, on the KMA where the passphrase has been changed, select the function to log the KMA into the Cluster. The KMA is not able to communicate with the Cluster until it is logged back in.

Deleting a KMA

Important – Before you delete a KMA, you should take it off-line using the Console "Shutdown KMA" function. If you fail to do this, the KMA will continue to function outside of the Cluster, and send "stale information" to Agents and users.

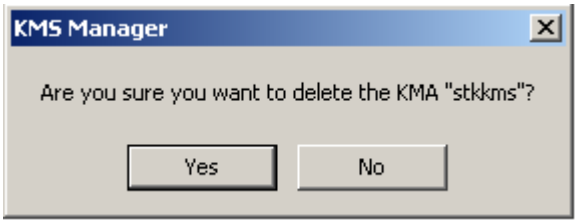
Normally, this command will only be used to delete a failed KMA from the Cluster. However, it may also be used to remove a KMA that is being decommissioned. However, in that case, using the Console "Reset KMA" function with the zeroize option is a better choice. This function deletes the KMA from the Cluster and wipes all information from the disk of the KMA that is being decommissioned.

If you want a deleted KMA to rejoin a Cluster, you must reset the KMA to the factory default and select option 2 from the QuickStart program.

This option gives the Security Officer the ability to delete a KMA that is no longer in service.

To delete a KMA:

1. From the KMAs List screen, highlight the KMA you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm that you want to delete the selected KMA.

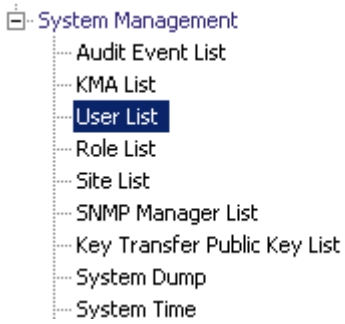


2. Click the Yes button to delete the KMA. The currently selected KMA is deleted and you are returned to the KMAs List screen. The system also removes any entries that are associated with the KMA and not used by any other entity.

User List Menu

The User List menu option allows you to:

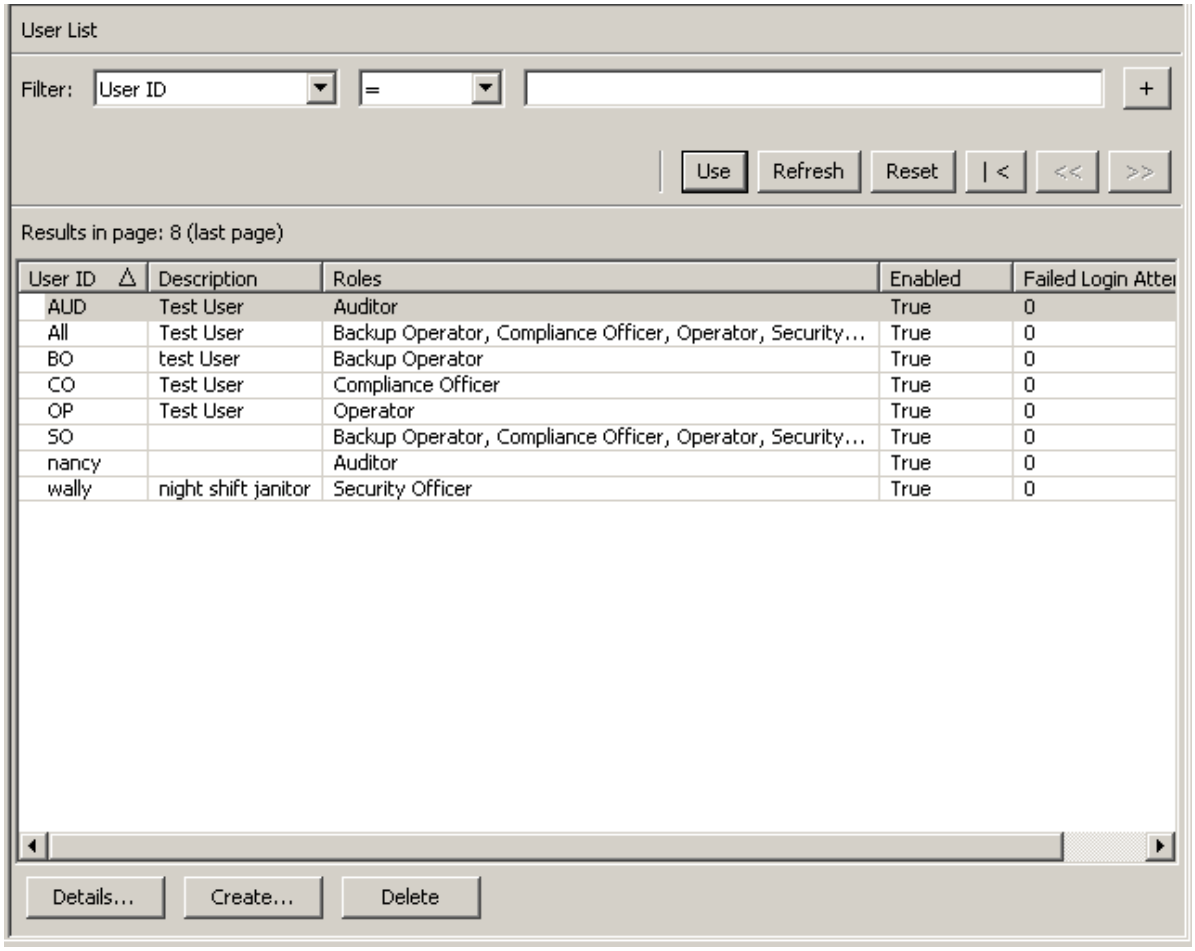
- View users
- Create a user
- Modify existing user information
- Delete an existing user



Viewing Users

To view users:

From the System Management menu, select **User List**. The User List screen is displayed.



You can also scroll through the database and filter the User list by any of the following keys:

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

The **Use** button applies the filter to the displayed list for the user.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- User ID
- Description
- Enabled
- Failed Login Attempts

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not Empty

Filter Value 1 box:

Type a value in this field.

Use:

Click this button to apply the filter to the displayed list.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

User ID

Displays a unique identifier, commonly referred to as "User Name" that distinguishes each user in a Cluster.

Description

Describes the user.

Roles

Displays the list of security roles for a user. The roles allow the user to perform various operations.

Enabled

Indicates the status of the user. Possible values are **True** or **False**.

Failed Login Attempts

Indicates the number of failed login attempts.

If you want to create a user, click the Create button. For more information, refer to "Creating a User" on page 122.

If you want to modify a user's details, highlight the user and click the Details button. For more information, refer to "Viewing/Modifying a User's Details" on page 125.

If you want to delete a user, click the Delete button. For more information, refer to "Deleting Users" on page 130.

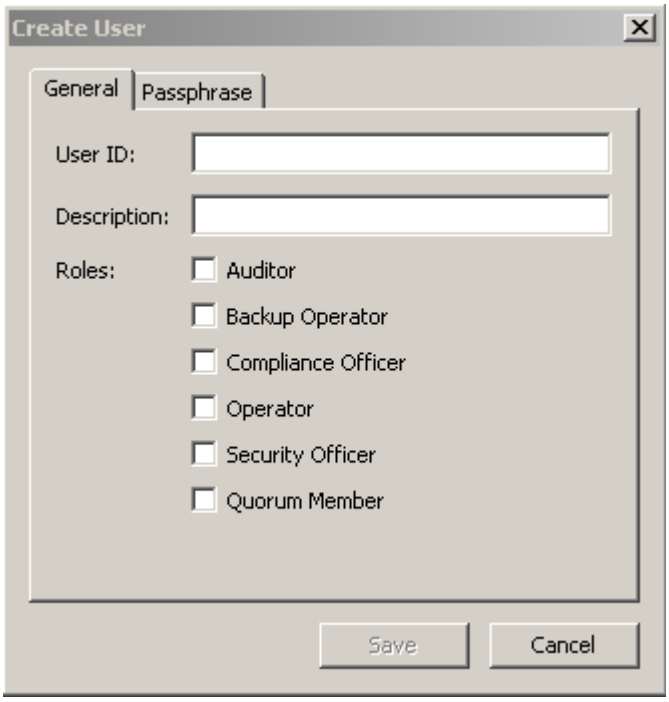
A Security Officer can set a user's passphrase if the user's passphrase and/or certificate has been compromised. For procedures on setting a user's passphrase, refer to "Setting a User's Passphrase" on page 128.

Users can also change their own passphrase. For procedures, refer to "Changing the Passphrase" on page 92.

Creating a User

To create a user:

1. From the User List screen, click the Create button. The Create User dialog box is displayed, with the General tab open.



2. Complete the following parameters:

General Tab

User ID

Type a value that uniquely identifies the user. This value can be between 1 and 64 (inclusive) characters.

Description

Type a value that describes the user. This value can be between 1 and 64 (inclusive) characters.

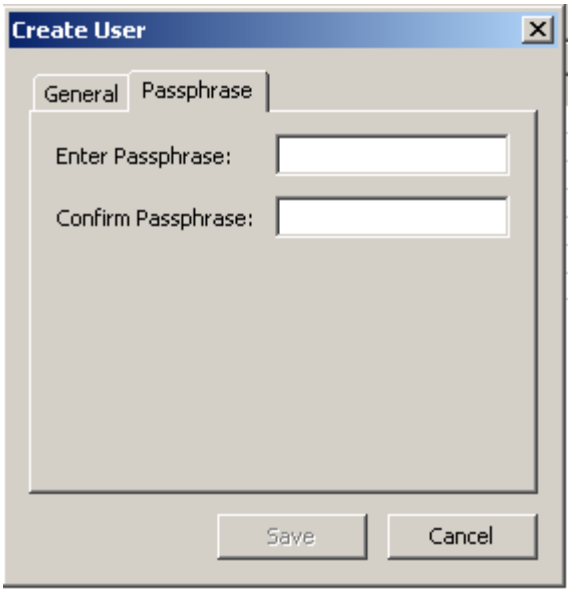
Roles

Select the check boxes beside the roles you want the user to perform.

Note – The Quorum Member check box is disabled (grayed out) if the KMA currently runs KMS software version 2.1 or earlier or if the replication version of the OKM Cluster is currently set to 10 or lower.

Passphrase Tab

3. Open the Passphrase tab.



4. Complete the following parameters:

Passphrase

Type the passphrase for this user. The minimum value is 8 characters; the maximum value is 64 characters. The default value is 8.

Passphrase requirements:

- A passphrase must not contain the user's User ID.
- A passphrase must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.

  The following special characters are allowed:

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

- Control characters, including tabs and linefeeds, are not allowed.

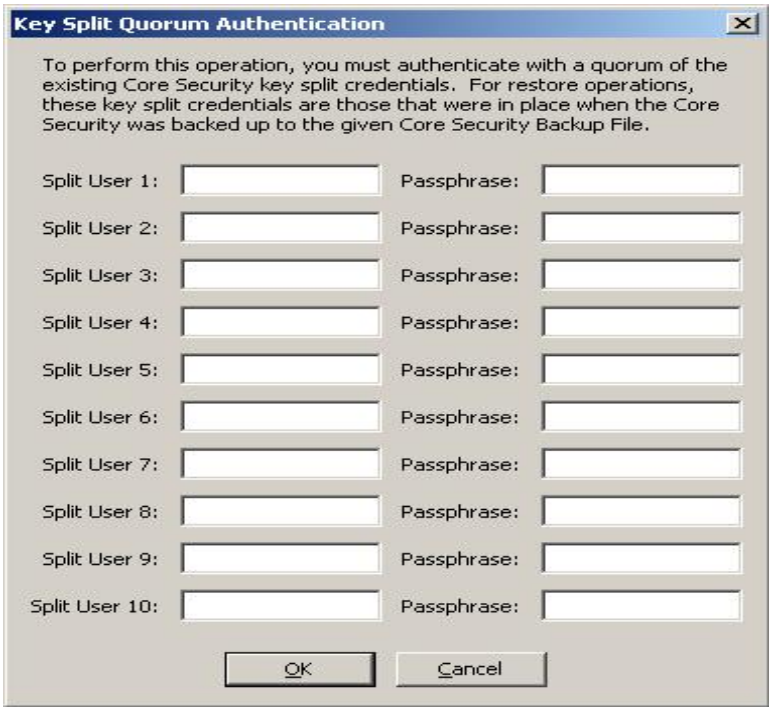
Note – To modify the minimum length requirement for passphrases, see "Modifying the Security Parameters" on page 192.

Confirm Passphrase

Type the same value that you entered in the Enter Passphrase field.

5. Click the Save button. The user record is added to the database. The new user is displayed in the User List.

6. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

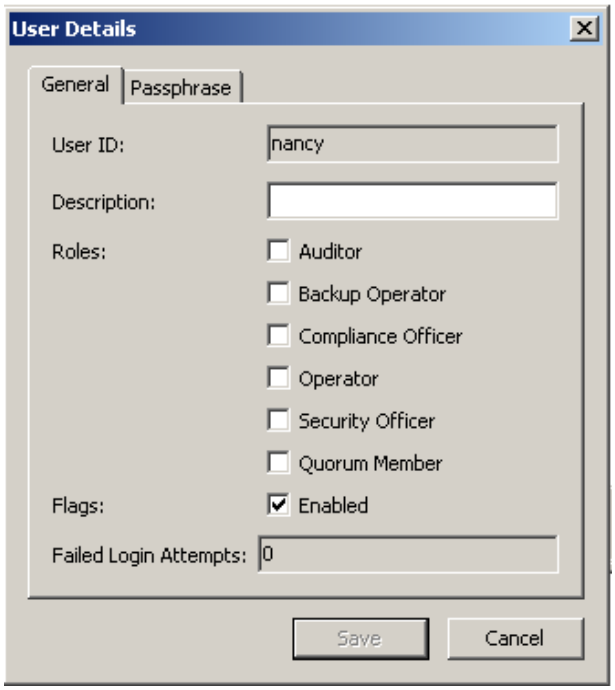
Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

Viewing/Modifying a User's Details

Note – The currently logged-in Security Officers cannot modify their records.

To modify user information:

1. From the Users List screen, double-click a user for which you want more information or highlight a user record and click the Details button. The User Details dialog box is displayed, where all fields, including the Save button are disabled.



2. On the General tab, modify the following parameters:

- Description
- Roles
- Flags - Enabled.

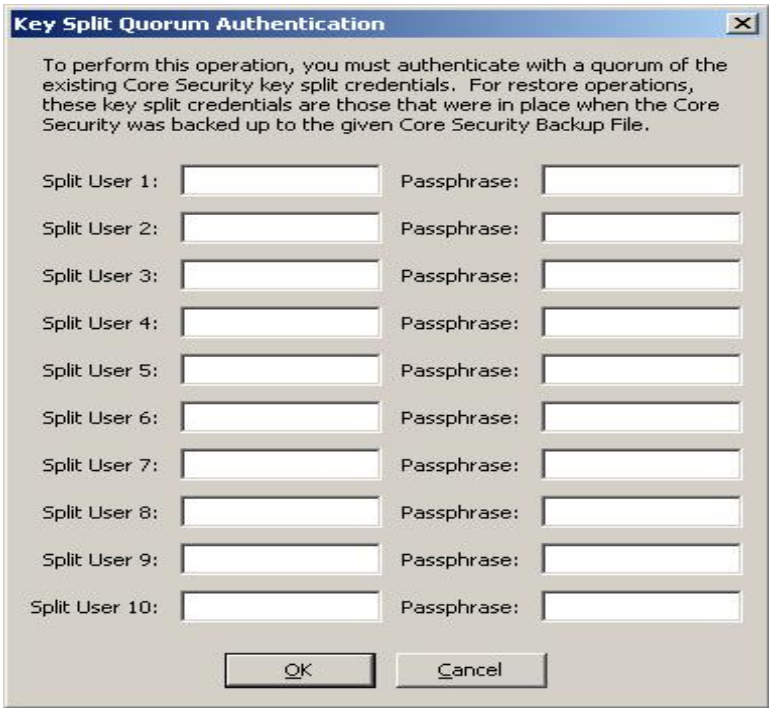
The Failed Login Attempts field displays the number of times that a login attempt has failed.

3. On the Passphrase tab, if you want to set the user's passphrase, see "Setting a User's Passphrase" on page 128.

4. When you are finished, click the Save button.

5. If user roles have been added, the Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.

Note – If user roles have not been added, user information is updated in the OKM Cluster after you click the Save button, and the Key Split Quorum Authentication dialog box is not displayed.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

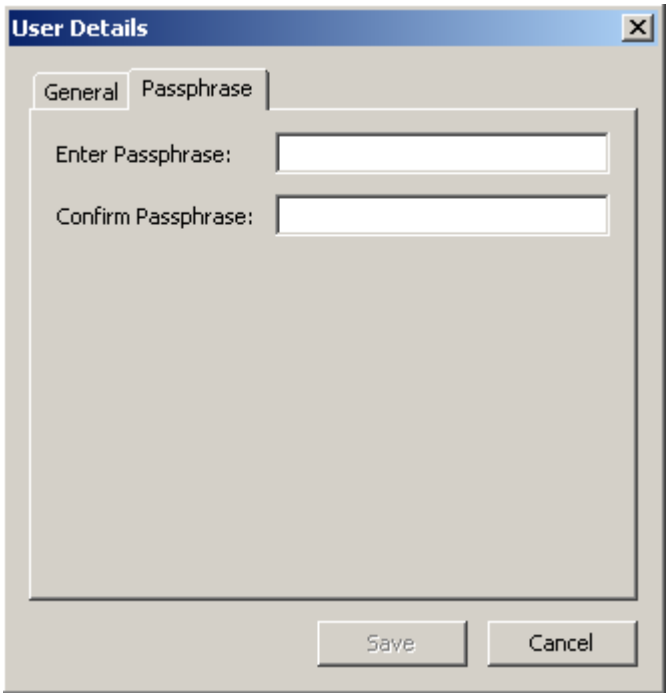
Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

Setting a User's Passphrase

As the Security Officer, you can set a user's passphrase if you believe that the user's passphrase and/or certificate has been compromised. A new certificate is generated when the user uses the new passphrase to logon to the KMA.

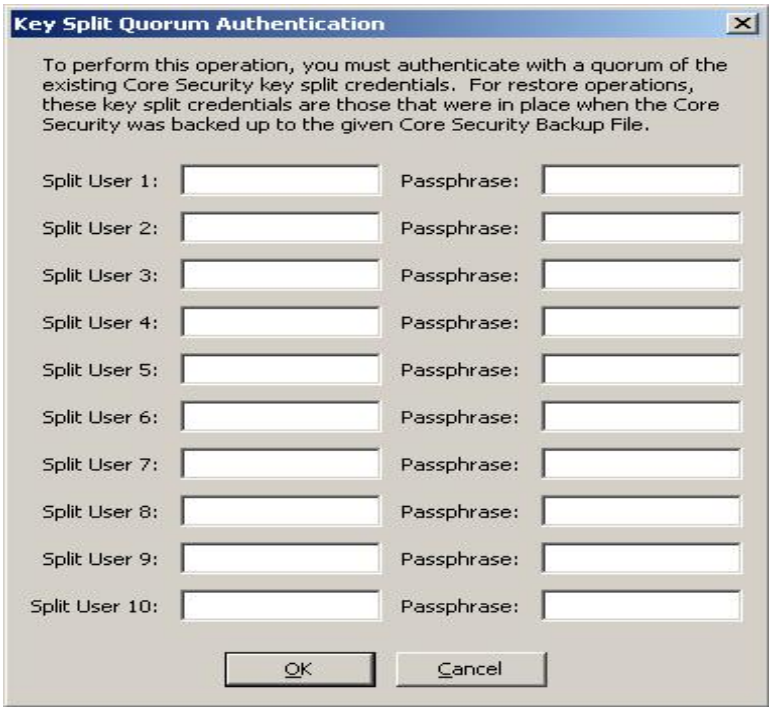
To set a user's passphrase:

1. From the User List screen, double-click the user whose passphrase you want to select or highlight the user and click the Details button.
2. The User Details dialog box is displayed. Open the Passphrase tab.



3. In the Enter Passphrase field, type the passphrase that was assigned by the Security Officer when the user account was created.
4. In the Confirm Passphrase field, type the same value you entered in Step 3. The new passphrase for the user record is saved.

5. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

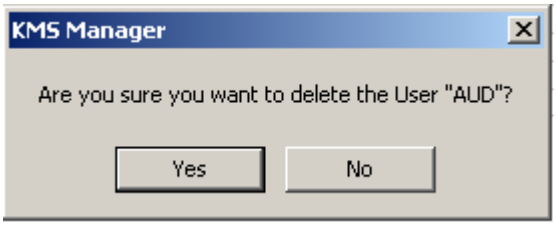
Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

Deleting Users

Users cannot delete themselves.

To delete a user:

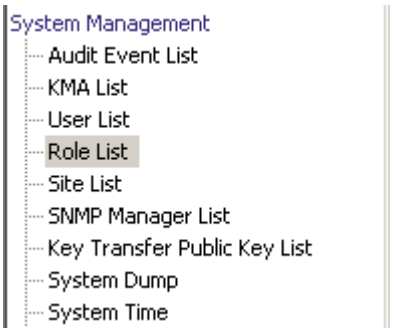
1. From the Users List screen, select the user you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm that you want to delete the selected user.



2. Click the Yes button to delete the user. The currently selected user is deleted and you are returned to the User List screen, where the deleted user is no longer in the User List.

Role List Menu

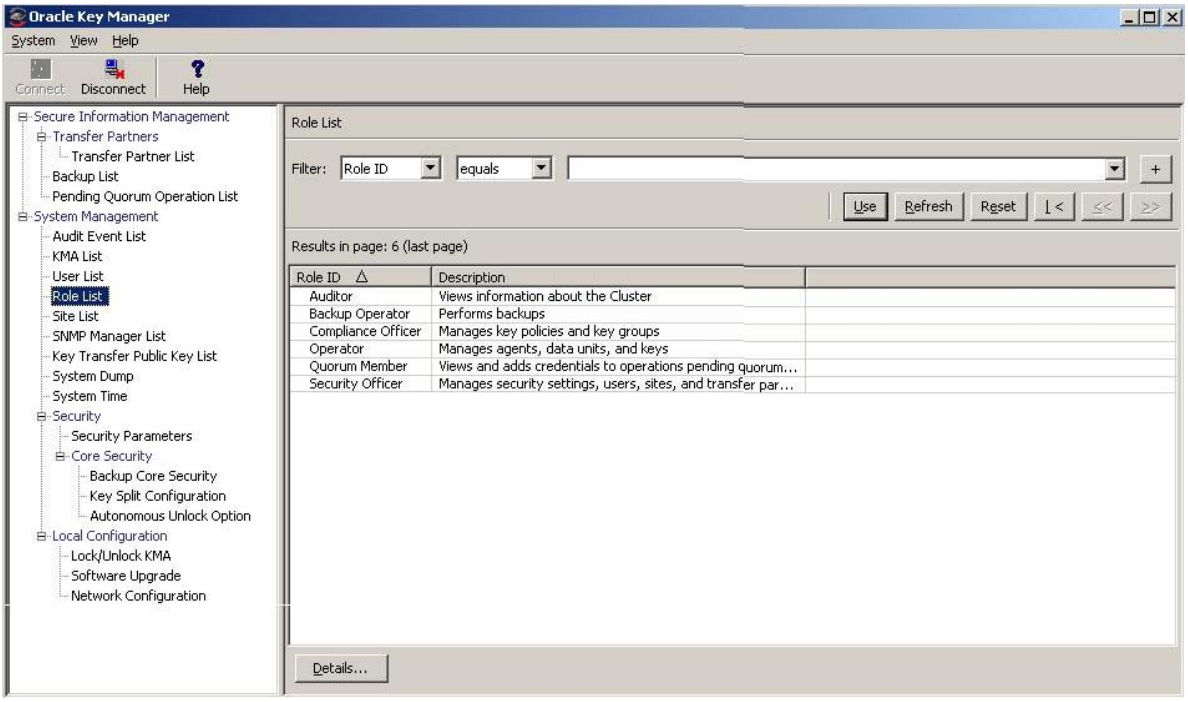
The Role List menu option allows gives you the ability to view user roles. Roles are fixed logical groupings of various system operations that a user can perform. A user can have more than one role.



Viewing Roles

To view roles:

From the System Management menu, select **Role List**. The Role List screen is displayed.



You can also scroll through the database and filter the Roles list by either of the following keys:

- Role ID
- Description.

The **Use** button applies the filter to the displayed list.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Role ID
- Description

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Empty
- Not Empty

Filter Value 1 box:

Type a value in this field.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Role ID

Displays the unique identifier that distinguishes each security role.

Description

Describes the role.

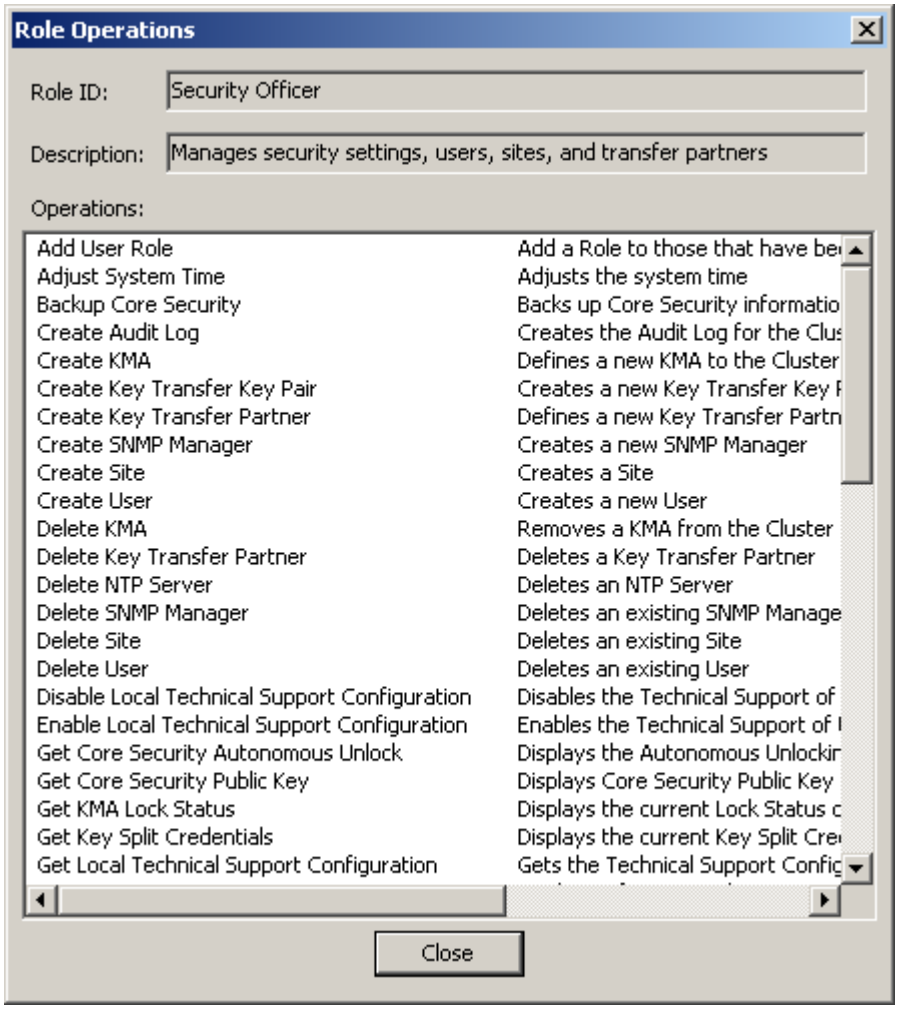
If you want more detailed information on a role, highlight a role entry and click the Details button. For more information, refer to "Viewing Operations for a Role" on page 134.

Viewing Operations for a Role

The Role Operations dialog box allows the you to view a role and its permitted operations.

To view the operations for a specific role:

1. From the Role List screen, highlight a role and click the Details button. The Role Operations dialog box is displayed, indicating the operations for the selected role.



2. Click the Close button to close this dialog box. You are returned to the Role List screen.

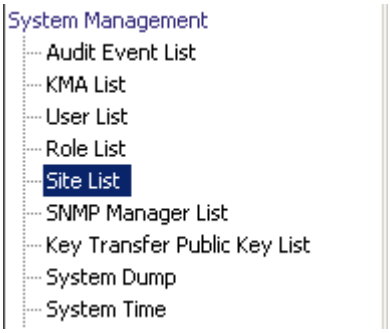
Site List Menu

A Site is a physical location with at least one KMA, to which several Agents (Hosts and OKM Cluster) connect. Sites allows Agents to respond to KMA failures or load balancing more effectively by connecting to another KMA in the local Site rather than a remote one

The Site List menu option gives you the ability to:

- View sites
- Create a site
- Modify an site's information
- Delete a site.

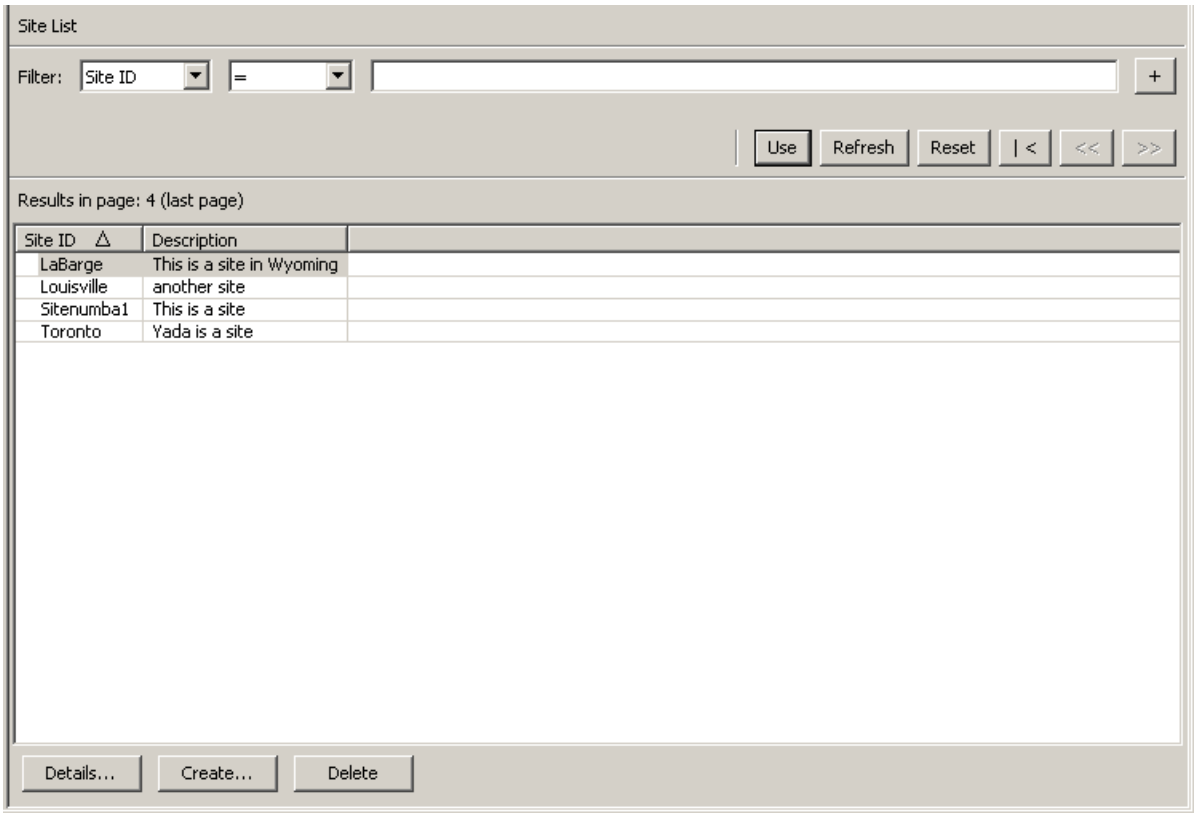
Note – An Operator can view sites only. A Security Officer can manage the sites.



Viewing Sites

To view sites:

From the System Management menu, select Site List. The Site List screen is displayed.



You can also scroll through the database and filter the Sites list by any of the following keys:

- Site ID
- Description.

The **Use** button applies the filter to the displayed list for the Site.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Site ID
- Description

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~

Filter Value 1 box:

Type a value in this field.

Use:

Click this button to apply the filter to the displayed list.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Site ID

Uniquely identifies the site.

Description

Describes the site.

Click the Create button to create a Site. For more information, refer to "Creating a Site" on page 139.

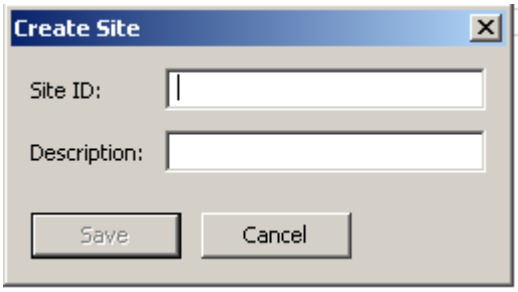
If you want to view / modify a Site's detailed information, highlight the Site and click the Details button. For more information, refer to "Viewing/Modifying a Site's Details" on page 141.

Click the Delete button to delete a selected Site. For more information, refer to "Deleting a Site" on page 142.

Creating a Site

To create a site:

1. From the Site List screen, click the Create button. The Create Site dialog box is displayed.



2. Complete the following parameters:

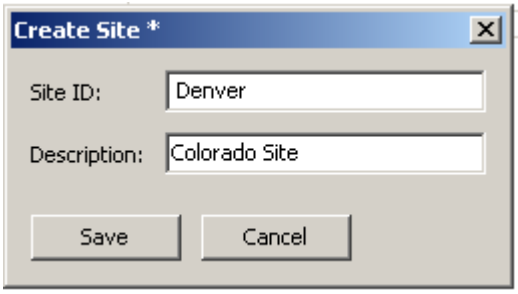
Site ID

Type a value that uniquely identifies the site. This value can be between 1 and 64 (inclusive) characters.

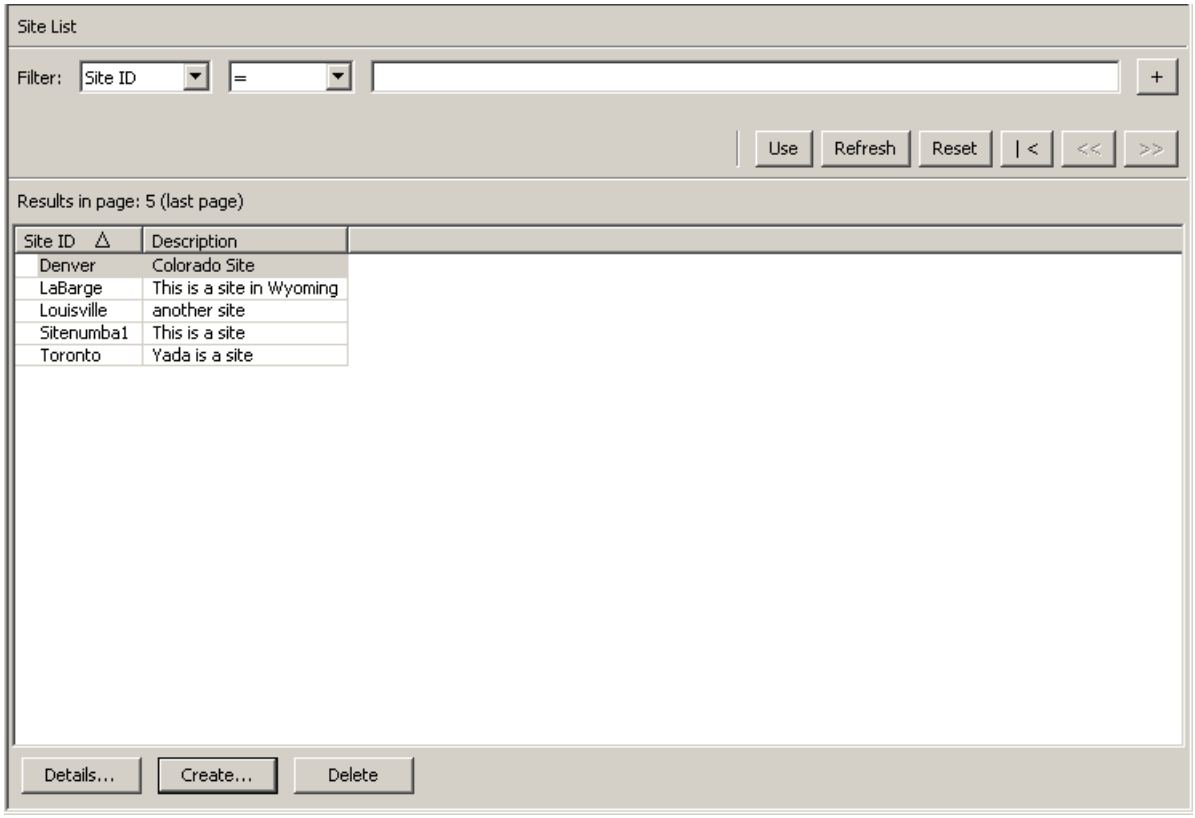
Description

Type a value that uniquely describes the site. This value can be between 1 and 64 (inclusive) characters.

An example of a completed dialog box is shown below.



3. Click the Save button. The new Site is saved and stored in the database and is displayed in the Site List.

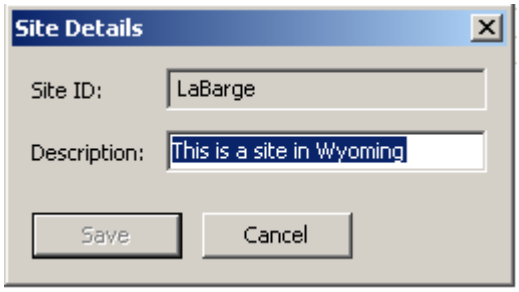

Site List
Filter:
Site ID
=
+
Use
Refresh
Reset
| <
<<
>>
Results in page: 5 (last page)
Site ID
Description
Denver
Colorado Site
LaBarge
This is a site in Wyoming
Louisville
another site
Sitenumba1
This is a site
Toronto
Yada is a site
Details...
Create...
Delete

Viewing/Modifying a Site's Details

Note – If you are not a Security Officer, when you view a site's detailed information, all fields, including the Save button are disabled.

To modify a Site's details:

1. From the Site List screen, click the Details button. The Site Details dialog box is displayed.



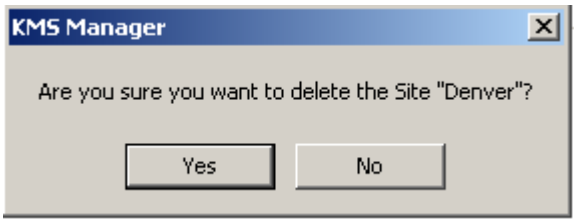
2. Change the Description field and click the Save button. The Site details are modified and stored in the database.

Deleting a Site

Note – If the site is in use, that is, agents or KMAs are specified to be at the site, they must first be deleted or changed to a different site before you can delete it.

To delete a site:

1. From the Site List screen, highlight the Site you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm your actions.



2. Click the Yes button to delete the Site. The currently selected Site is deleted and you are returned to the Site List screen.

SNMP Manager List Menu

The following menus discuss viewing, creating, and modifying SNMP Managers.

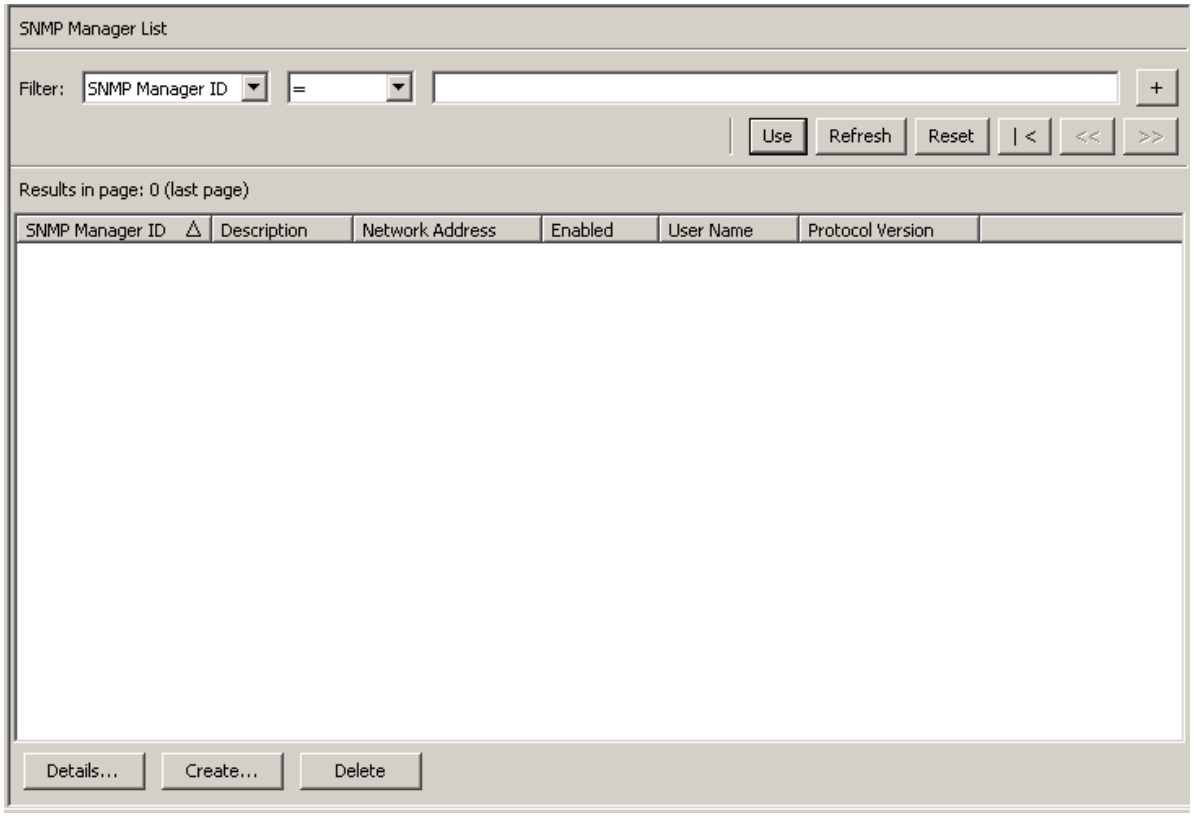
Additionally, SNMP information is generated for users who have configured an SNMP Agent in their network and defined SNMP Managers in the OKM Manager GUI. When at least one SNMP Manager is defined in the OKM Manager GUI, the KMAs will send SNMP Informs to the IP address of that SNMP Manager(s).

Refer to "SNMP Management Information Base (MIB) Data" on page 379 for more details about the information that KMAs send in their SNMP Inform packets.

Viewing a KMA's SNMP Managers

To view the SNMP Managers:

From the System Management menu, select SNMP Manager List. The SNMP Manager List screen is displayed.



You can also scroll through the database and filter the SNMP Manager List by any of the following keys:

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

The **Use** button applies the filter to the displayed list for the SNMP Manager.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

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

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value 1 box:

Type a value in this field.

Use:

Click this button to apply the filter to the displayed list.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

SNMP Manager ID

Displays the user-defined unique identifier for the SNMP Manager.

Description

Displays a description for the SNMP Manager. This field is optional.

Network Address

Displays the network address that will be used when sending an SNMP trap.

Enabled

Indicates whether this SNMP Manager is enabled or not.

User Name

Displays the user name that was used to establish a secure, trusted SNMPv3 connection to this SNMP Manager.

Protocol Version

Indicates the SNMP protocol version, either SNMPv3 (Version 3) or SNMPv2 (Version 2).

SNMP protocol Version 3 (SNMPv3) supports authentication, using user names and passphrases. SNMP protocol Version 2 (SNMPv2) does not support authentication and does not use user names and passphrases. You can configure an SNMP Manager to use either SNMPv3 or SNMPv2. KMAs do not send SNMP informs to SNMP Managers configured to use SNMPv2 if the replication version of the OKM Cluster is currently set to 10 or lower.

Click the Create button to create a new SNMP Manager. For more information, refer to "Creating a New SNMP Manager"below.

If you want to view/modify a SNMP Manager detailed information, highlight the entry and click the Details button. For more information, refer to "Viewing/Modifying an SNMP Manager's Details" on page 149.

Click the Delete button to delete the selected SNMP Manager. For more information, refer to "Deleting an SNMP Manager" on page 150.

Creating a New SNMP Manager

Notes –

If your SNMP agent is configured to use SNMP protocol Version 3, ensure that you have created an SNMP protocol Version 3 user **before** you create an SNMP manager in your OKM Cluster. This SNMP user should use SHA (not MD5) as the authentication protocol and DES as the privacy protocol. Refer to your SNMP Agent documentation for more information about creating SNMP Version 3 users.

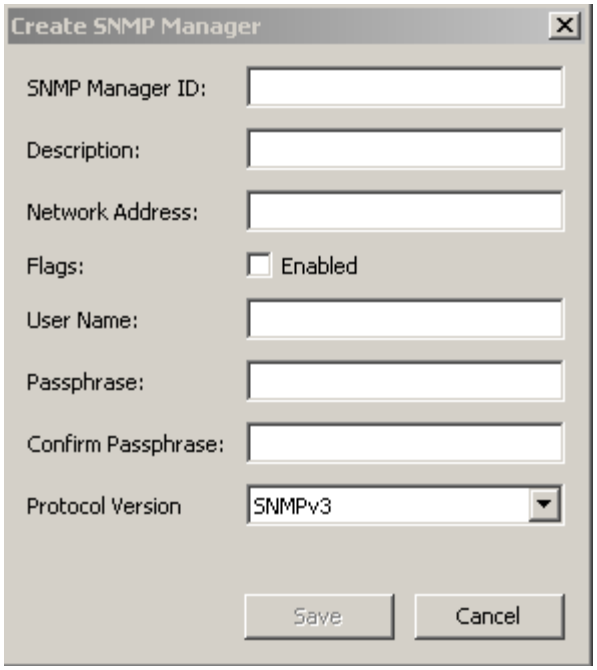
Also, if the SNMP user has a passphrase, then the KMA uses this passphrase for both the Authentication Passphrase and the Encryption Passphrase for that SNMP user. Thus, these passphrases must have the same value for this SNMP user in the SNMP Agent. If the SNMP user does not have a passphrase, then the KMA uses a security level of "noAuthNoPriv" when it sends SNMP informs to the SNMP Agent.

If your SNMP agent is configured to use SNMP protocol Version 2, then you do not need to configure an authentication protocol or create an SNMP user. Currently, OKM supports only the "public" community for Version 2.

Consult your SNMP Agent documentation for more information about creating SNMP Users. For example, refer to the *Solaris System Management Agent Administration Guide* (http://docs.sun.com/app/docs/doc/817-3000) for more information about configuring the System Management Agent on a Solaris system. Also, refer to http://www.net-snmp.org/FAQ.html for more general information about Net-SNMP.

1. From the SNMP Managers List screen, click the Create button.

   The Create SNMP Manager dialog box is displayed.



2. Complete the following parameters:

SNMP Manager ID

Type a value that uniquely identifies the SNMP Manager. This value can be between 1 and 64 (inclusive) characters.

Description

Type a value that describes the SNMP Manager. This value can be between 1 and 64 (inclusive) characters.

Network Address

Type the SNMP Manager's network address.

Flags - Enabled

Select this check box to indicate whether SNMP is enabled or not.

User Name

Type the user name that will be used to authenticate the SNMP Manager.

Passphrase

Type the passphrase that will be used to authenticate the SNMP Manager.

Confirm Passphrase

Type the same passphrase that was entered in the Passphrase field.

Protocol Version

Select the SNMP protocol version that this SNMP Manager should use. A value of SNMPV3 means that it is using SNMP protocol Version 3. A value of SNMPV2 means that it is using SNMP protocol Version 2.

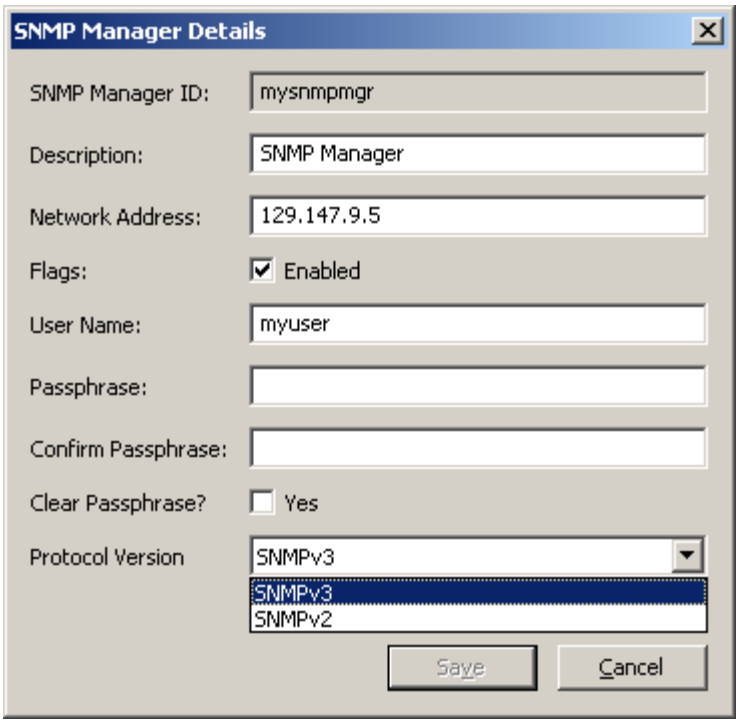
SNMP protocol Version 3 (SNMPv3) supports authentication, using user names and passphrases. SNMP protocol Version 2 (SNMPv2) does not support authentication and does not use user names and passphrases. You can configure an SNMP Manager to use either SNMPv3 or SNMPv2. KMAs do not send SNMP informs to SNMP Managers configured to use SNMPv2 if the replication version of the OKM Cluster is currently set to 10 or lower.

3. When you are finished, click the Save button to save the information. The new SNMP Manager entry and its associated profile is stored in the database.

Viewing/Modifying an SNMP Manager's Details

To view/modify an SNMP Manager's details:

1. From the SNMP Managers List screen, double-click an SNMP Manager entry for which you want more information and click the Details button. The SNMP Manager Details dialog box is displayed.



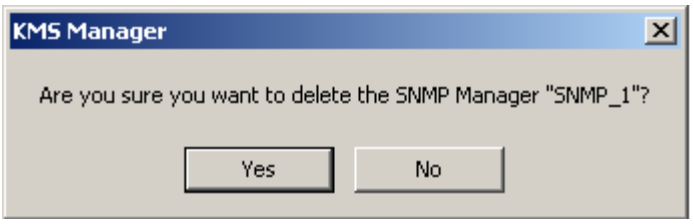
2. Change the parameters, as required.
3. When you are finished, click the Save button to save the changes.

Note – Every time you modify a SNMP Manager's details, you have to re-specify the passphrase.

Deleting an SNMP Manager

To delete an SNMP Manager:

1. From the SNMP Managers List screen, highlight the SNMP Manager you want to delete and click the Delete button. The SNMP Manager Confirm Delete dialog box is displayed.



2. Click the Yes button to delete the SNMP Manager. The currently selected SNMP Manager is deleted and you are returned to the SNMP Managers List screen.

Key Transfer

Overview

Key Transfer, also called Key Sharing, allows keys and associated data units to be securely exchanged between Partners and is required to exchange encrypted media. This process requires each party in the transfer establish a public/private key pair and then provide the public key to the other party.

Each party enters the other party's public key into their own OKM Cluster. Once this initial configuration is complete, the sending party uses Export Keys to generate a transfer file, which is sent from the sending party to the receiving party. The receiving party then uses Import Keys to import the keys and their associated data units into their OKM Cluster.

The transfer file is signed using the sending party's private key and encrypted using the receiving party's public key. This allows only the receiving party to decrypt the transfer file using their own private key. The receiving party can verify the file was in fact produced by the expected sender by using the sender's public key.

Key Transfer Partners Feature

The Key Transfer Partners feature allows keys to be moved from one OKM Cluster to another. Typically, this feature can be used to exchange tapes between companies or within a company if multiple Clusters are configured to deal with large numbers of sites.

The Key Transfer process involves these steps:

- Each OKM Cluster configures the other Cluster as a Transfer Partner. This is usually done once.
- The user exports keys from one OKM Cluster and imports them into the other. This step can be done many times.

Key Transfer Process

Within the OKM, you must perform a number of tasks in a specific order. Since these tasks involve more than one user role, the actual procedures reside in different chapters in this document.

Configuring Key Transfer Partners

To move keys, you must configure a key transfer partner for both OKM Clusters participating in key movement.

In the following procedure, "C1" refers to the first OKM Cluster, "C2" to the second.

C1 Administrator (Security Officer role):

1. Acquire the Public Key information for C1 (your Cluster). To do this, go to the Key Transfer Public Key List Menu. See "Viewing the Key Transfer Public Key List" on page 171 and "Viewing the Key Transfer Public Key Details" on page 174.
2. Cut and paste the Public Key ID and Public Key into an e-mail or other agreed-upon form of communication. Send this information to the C2 administrator.

Note – The exact communication method should be sufficiently secure that when C2 receives the information, it can be confident it actually came from C1. There is a mechanism, the fingerprint, to prevent modification of this information in transit.

C2 Administrator (Security Officer role):

3. C2 Administrator: Enter the Public Key information from C1 into the OKM Cluster by accessing the Transfer Partner List menu. See "Transfer Partner List Menu" on page 157.
4. Click the Create... button. Fill in a name for the Transfer Partner, a description, and contact information. Determine what you want to do with this Partner. See "Creating a Transfer Partner" on page 161.
5. Select the Public Keys tab. Fill in the Public Key ID and Public Key from the information supplied by C1.

   As the Public Key is entered, the system will compute the fingerprint. The C1 and C2 administrators should be communicating with each other using a different mechanism than was used for the transfer of the key itself.

   Both administrators should look at their OKM and verify the fingerprint matches. A mismatch indicates the key has been damaged or modified during the transfer.
6. If the fingerprint is correct, click Save. The system will prompt for a quorum. This is because the key export operations that are enabled by this step could be used to extract valid keys from a OKM Cluster. C1 is now configured as a Transfer Partner in the C2 OKM Cluster.

C2 Administrator (Security Officer role):

7. Repeat Step 1 and Step 2, this time for the C2 OKM Cluster.

C1 Administrator (Security Officer role):

8. Repeat Step 3 through Step 6 to add C2's Public Key to C1.

C1 Administator (Compliance Officer Role):

9. C1 must configure Key Groups that can be sent to C2. See "Viewing Key Group Assignments" on page 246.

C2 Administrator (Compliance Officer Role):

10. C2 must configure Key Groups that can receive keys from C1. See "Viewing Key Group Assignments" on page 246.
11. Select the desired Transfer Partner.
12. Select one or more disallowed Key Groups, and click the Move to button to add them to the Key Group list. See "Adding a Key Group to a Transfer Partner" on page 247.

Exporting/Importing Keys

Before you export keys, keys must meet **all** of the following criteria. Keys that do not are not exported when an Operator issues an Export Keys request.

- Keys must belong to a Key Group associated with a Key Policy that has its `Allow Export From` flag set to "True." See "Viewing/Modifying Data Unit Details" on page 287 and "Viewing Key Groups" on page 225.

  To set the flag, refer to "Viewing/Modifying a Key Policy" on page 220.
- The destination key transfer partner must have its `Enabled` and `Allow Export To` flags set to "True." See "Viewing/Modifying Transfer Partner Details" on page 165.

  To set the flag, refer to "Viewing/Modifying a Key Policy" on page 220.
- The destination key transfer partner must be associated with the Key Group of the selected key. See "Adding a Key Group to a Transfer Partner" on page 247.
- Keys must be in Protect and Process, Process Only, Deactivated, or Compromised state. See "Viewing/Modifying Data Unit Details" on page 287.

In addition, the `Export Format` setting of the destination transfer partner (see "Transfer Partner List Menu" on page 157) must match:

- The software version (see "Uploading and Applying Software Upgrades" on page 295) on the KMA where the keys are to be imported and
- the `FIPS Mode Only` security parameter values (see "Retrieving the Security Parameters" on page 189) on the OKM Clusters where the keys are to be exported and imported.

TABLE 5-1 summarizes the relationship between these settings.

TABLE 5-1 Export Format Settings

Software Version - Importing KMA	FIPS Mode Only - Exporting OKM Cluster	FIPS Mode Only - Importing OKM Cluster	Export Format
2.0.2 or lower	Off	N/A	v2.0 or Default
2.0.2 or lower	On	N/A	v2.0
2.1 or higher	Off	Off	v2.0 or Default
2.1 or higher	On	Off	v2.0
2.1 or higher	Off	On	v2.1 (FIPS)
2.1 or higher	On	On	v2.1 (FIPS) or Default

The following procedure is used to export keys from one OKM Cluster and import them into another. This can be done many times.

In this procedure, "C1" refers to the first OKM Cluster, "C2" to the second. These instructions are written to allow C2 to export keys that are then imported into C1.

C2 Administrator (Operator Role):

1. To exchange keys, go to the Data Unit List screen. See "Viewing Data Units" on page 283.
2. Select one or more Data Units (tapes) to be sent from C2 to C1. The External Tag is the barcode on the tapes.

   Keys associated with the selected Data Units must belong to Key Groups associated with Key Policies that have their `Allow Export From` flag set to "True." These keys must also be activated (their Activation Date is not empty) and not destroyed (their Destroyed Date is empty). See "Viewing/Modifying Data Unit Details" on page 287.
3. Click the Export Keys button to display the dialog box.
4. Select the destination Transfer Partner, select the Export Keys file name if necessary, and click Start. The Transfer File will be created.

   Only the Keys belonging to the Key Groups that are allowed to be exported to C1 are exported.

   The selected destination Transfer Partner must be assigned to the Key Group to which these keys belong. See "Transfer Partner Assignment to Key Groups Menu" on page 249.
5. Send the Transfer File to the C1 administrator by email or another agreed-upon form of communication or mechanism to move files.

C1 Administrator (Operator Role):

6. Select the Import Keys screen. See "Import Keys Menu" on page 280.
7. Supply the Destination Key Group the keys are to be imported to, the Sending Transfer Partner (C2, in this case) that exported these keys, and the Key Transfer file name. The selected Key Group must be a Key Group that is configured to receive keys from C2.

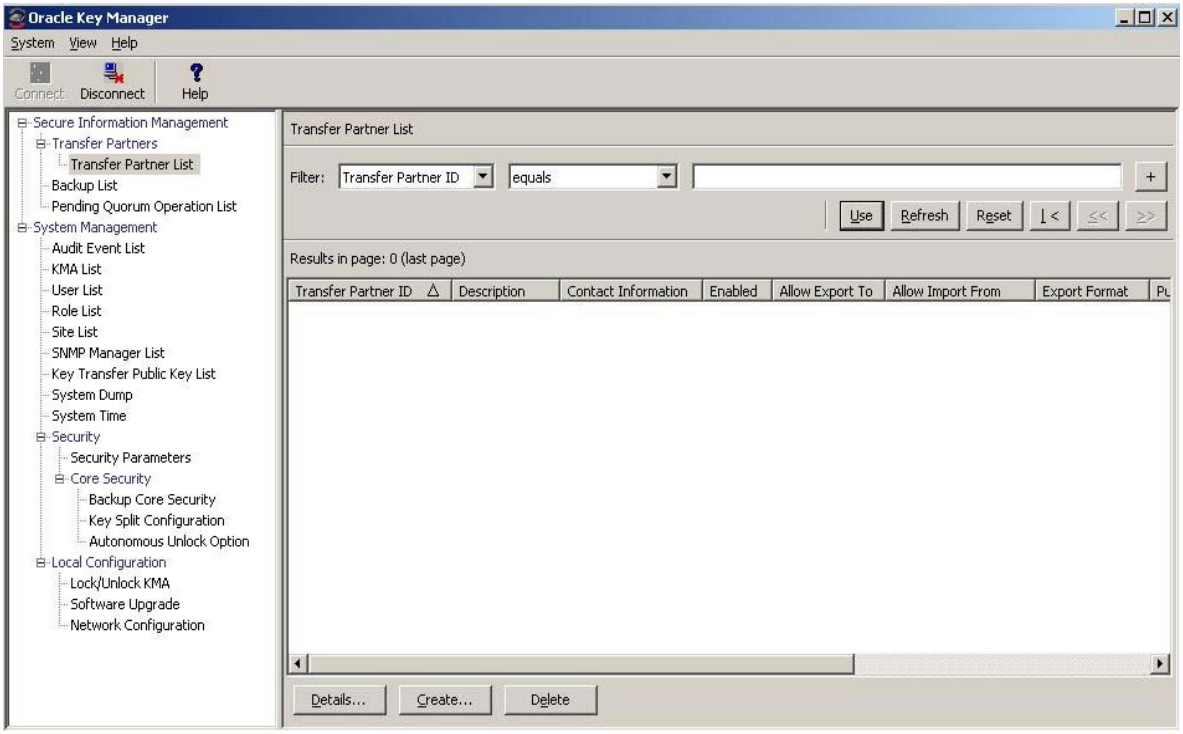
   That is, the Key Policy associated with the selected Key Group must have its `Allow Import To` flag set to "True." Also, the selected Transfer Partner must have its `Enabled` and `Allow Import From` flags set to "True," and its Export Format value set as described above. The selected Transfer Partner must be assigned to the selected Key Group. See "Transfer Partner Assignment to Key Groups Menu" on page 249.
8. Click Start.

Transfer Partners Menu

The Key Transfer Partners feature allows keys to be moved from one OKM Cluster to another.

Transfer Partner List Menu

From the Secure Information Management menu, select **Transfer Partner List**.



You can also scroll through the database and filter the Transfer Partner list by any of the following keys:

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

The **Use** button applies the filter to the displayed list for the Transfer Partner.

The fields and their descriptions are given below:

Filter:

Select filter options to filter the displayed list of Transfer Partners. Only Transfer Partners that satisfy all filters are displayed.

Filter Attribute combo box:

Click the down-arrow and select an attribute to filter by. Possible values are:

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

Filter Operator combo box:

Click the down-arrow and select the filter operation to apply to the selected attribute. This filter option is not displayed for all filter attributes. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value text box:

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Click this button to add additional filters.

Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

Use:

Click this button to apply the selected filters to the displayed list and go to the first page.

Refresh:

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of items that can be displayed on the current page. Appends "(last page)" to the number of items if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

Transfer Partner ID:

Displays the unique identifier that distinguishes each Transfer Partner. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

Description:

Describes the Transfer Partner. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

Contact Information:

Displays contact information about the Transfer Partner. Click this Column Name to sort by this attribute.

Enabled:

Indicates whether the Transfer Partner is allowed to share keys. Possible values are: True or False. If this field is False, the Transfer Partner cannot share keys. Click this Column Name to sort by this attribute.

Allow Export To:

Indicates whether the Transfer Partner is allowed to export keys. Possible values are: True or False. If this field is False, the Transfer Partner cannot export keys. Click this Column Name to sort by this attribute.

Allow Import From:

Indicates whether keys can be imported from this Transfer Partner. Possible values are: True or False. If this field is False, keys cannot be imported from this Transfer Partner. Click this Column Name to sort by this attribute.

Export Format:

Indicates whether keys can be wrapped (wrap keys encrypt the media key on the LAN and the token.)

In the Export Format column, a "v2.0" value means that this Transfer Partner does not wrap keys when it exports them.

A "v2.1 (FIPS)" value means that this Transfer Partner wraps keys when it exports them.

An "N/A" value signifies that the connected KMA runs 2.0.*x* OKM software, and thus does not allow the user to select this setting.

Note – To exchange keys with a Cluster running KMS 2.0, the Security Officer should create a Transfer Partner that has an Export Format value of "v2.0."

Refer to the `FIPS Mode Only` parameter in "Retrieving the Security Parameters" on page 189 for more information.

Public Key ID

Displays the unique identifier that distinguishes each Public Key. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

Public Key Fingerprint

Shows the fingerprint, or hash value, of the Public Key.

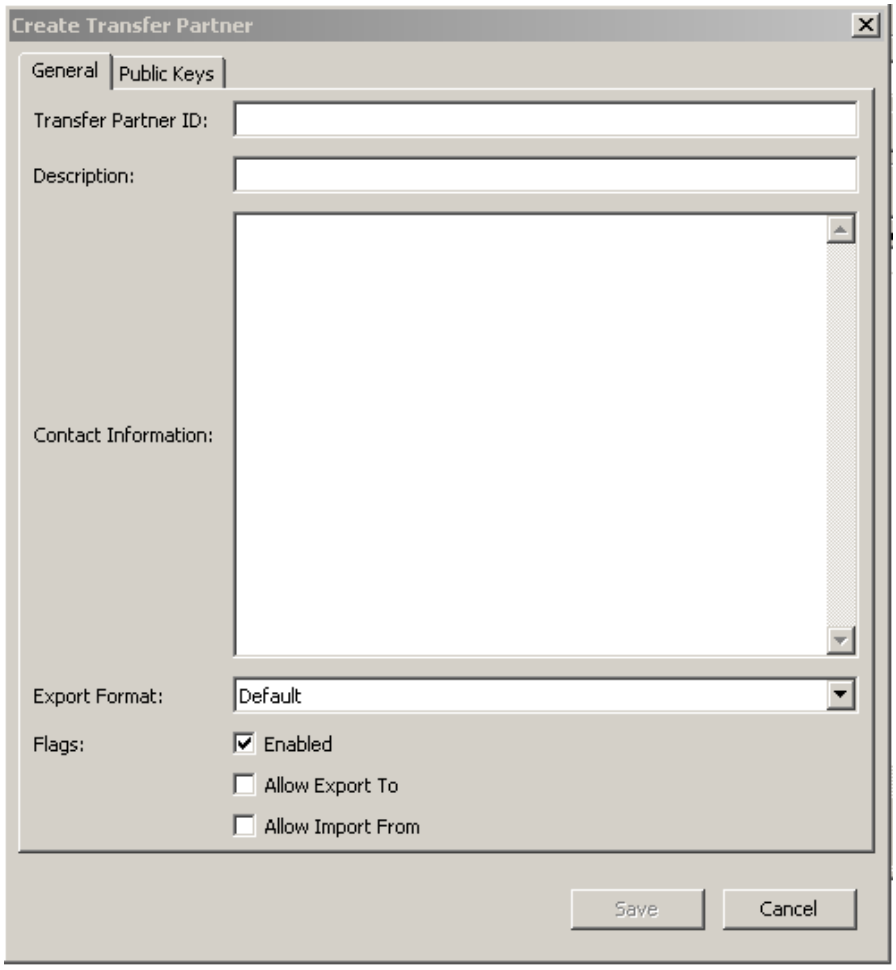
Entry Date

Displays the date the Public Key was entered into the OKM Cluster.

Creating a Transfer Partner

To create a Transfer Partner:

1. From the Transfer Partner List screen, click the Create button. The Create Transfer Partner dialog box is displayed, with the General tab active.



2. Complete the following parameters:

General Tab

Transfer Partner ID

Uniquely identifies the Transfer Partner.

Description

Type a value that uniquely describes the Transfer Partner. This value can be between 1 and 64 (inclusive) characters. This field can be left blank.

Contact Information

Type a value that identifies contact information about the Transfer Partner. This field can be left blank.

Export Format

Select either the default, v2.0, or v2.1 (FIPS) to determine the export format.

A "v2.0" value means this Transfer Partner does not wrap keys when it exports them.

A "v2.1 (FIPS)" value means this Transfer Partner wraps keys when it exports them.

A "Default" value means when you are exporting a key transfer file for this Transfer Partner, the format depends on the setting of the **FIPS Mode Only** security parameter (see "Retrieving the Security Parameters" on page 189).

If **FIPS Mode Only** is "Off," the format is v2.0. If **FIPS Mode Only** is "On," the format is v2.1 (FIPS).

Note – An advantage of setting a Transfer Partner's Export Format to "Default" is that it allows you to alter the format of the Transfer Partner's transfer files simply by changing the **FIPS Mode Only** security parameter, instead of editing the Transfer Partner's Export Format setting directly, which requires a quorum to authenticate the change.

Flags - Enabled

Check this box to allow this Transfer Partner to share keys. If the field is not selected, the Transfer Partner cannot share keys.

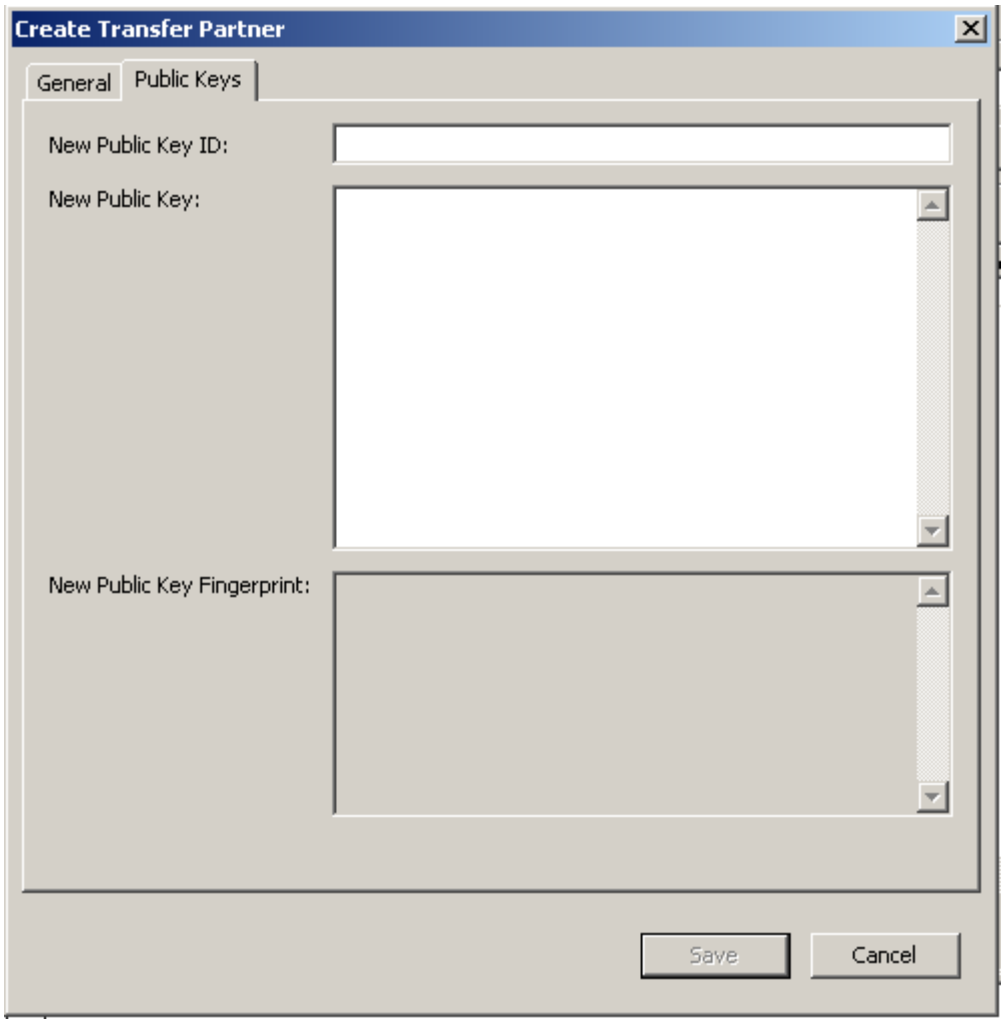
Allow Export To

Check this box to allow keys to be exported to the Transfer Partner. If this field is not selected, the Transfer Partner will not be available for the export keys operation.

Allow Import From

Check this box to indicate whether keys can be imported from this Transfer Partner. If this field is not selected, keys cannot be imported from this Transfer Partner.

3. Open the Public Keys tab.



Public Keys Tab

New Public Key ID

Enter the Public Key ID provided to you by the Transfer Partner.

New Public Key

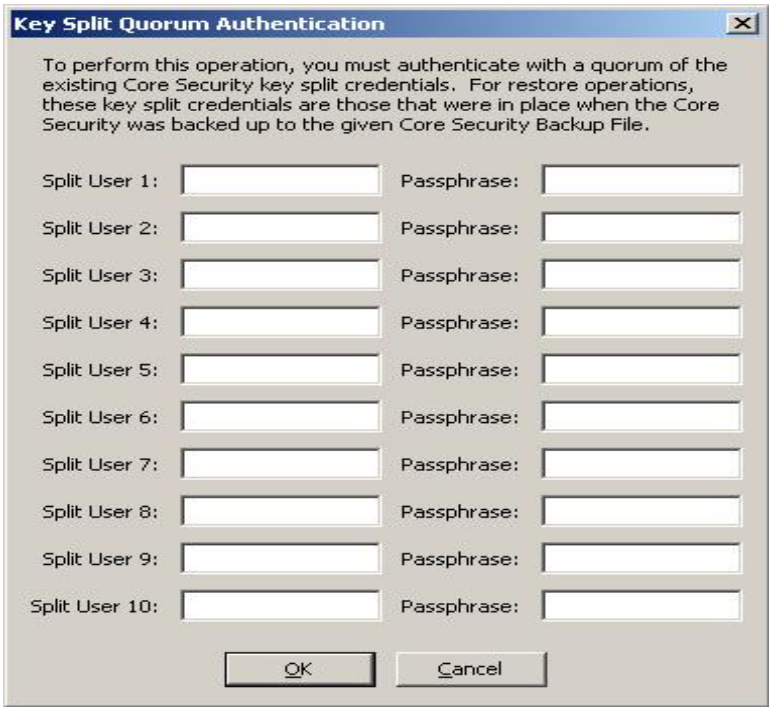
Enter the Public Key provided to you by the Transfer Partner.

New Public Key Fingerprint

This read-only field shows the fingerprint, or hash value, of the new Public Key. Verify this fingerprint with the Partner to ensure the Public Key has not been tampered with, accidentally or deliberately, during transmission.

4. When you are finished, click the Save button.

5. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

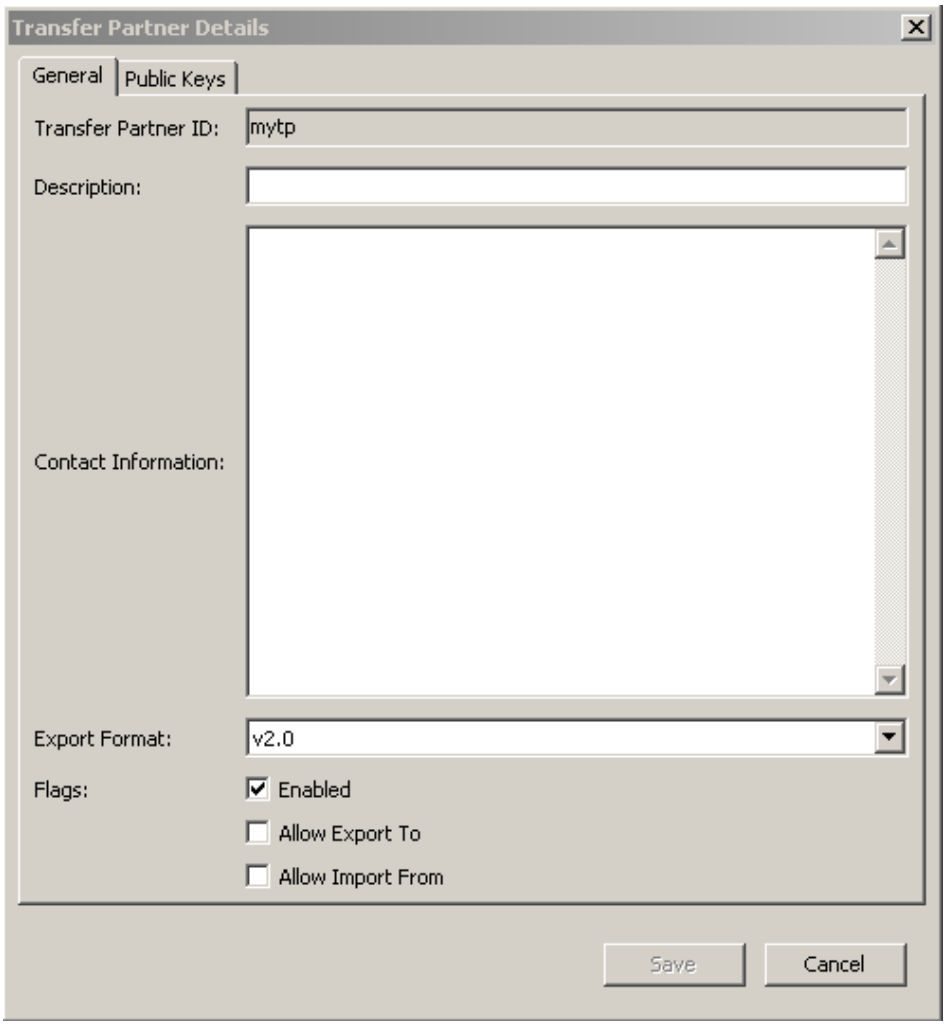
Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

Viewing/Modifying Transfer Partner Details

The Transfer Partner Details dialog box allows you to view detailed information about a specific Transfer Partner.

To view these details:

1. From the Transfer Partner List screen, highlight a Transfer Partner ID and click the Details button. The Transfer Partner Details dialog box is displayed.



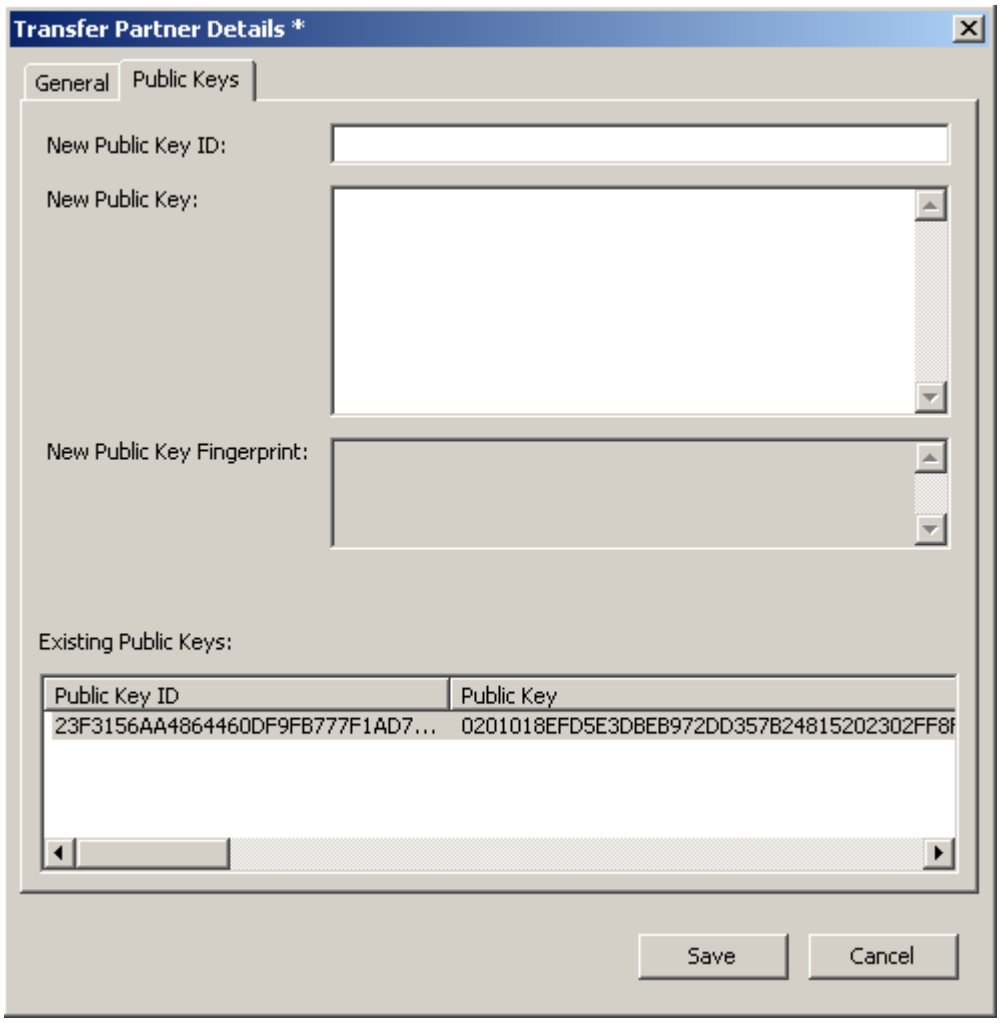
General Tab

2. On the General tab, you can change the following fields:

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

The Transfer Partner ID field is read-only.

3. When you are finished, click the Save button. The Transfer Partners record in the database is modified.
4. Open the Public Keys tab.



Public Keys Tab

5. On the Public Keys tabs, you can change the following fields:

New Public Key ID

Enter the new Public Key ID provided to you by the Transfer Partner.

New Public Key

Enter the new Public Key provided to you by the Transfer Partner.

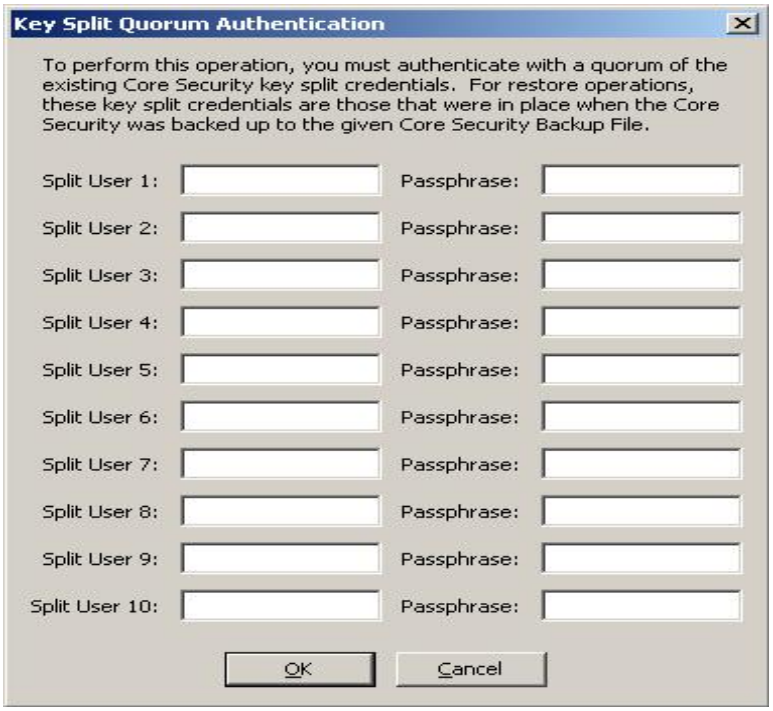
New Public Key Fingerprint

This read-only field shows the fingerprint, or hash value, of the new Public Key. Verify this key with the sending Transfer Partner.

Existing Public Keys

This list displays Public Keys associated with this Transfer Partner.

6. When you are finished, click the Save button.
7. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

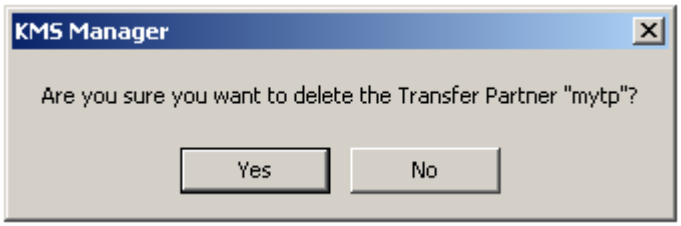
Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

Deleting a Transfer Partner

This option gives the Security Officer the ability to delete a Transfer Partner.

To delete a Transfer Partner:

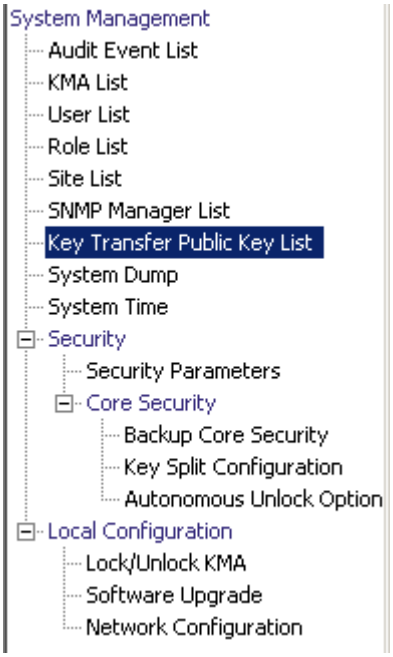
1. From the Transfer Partner List screen, highlight the Transfer Partner ID you want to delete and click the Delete button. The Transfer Partner Confirm Delete dialog box is displayed.



2. Click the Yes button to delete the Transfer Partner. The currently selected Transfer Partner is deleted, and you are returned to the Transfer Partner List screen.

Key Transfer Public Key List Menu

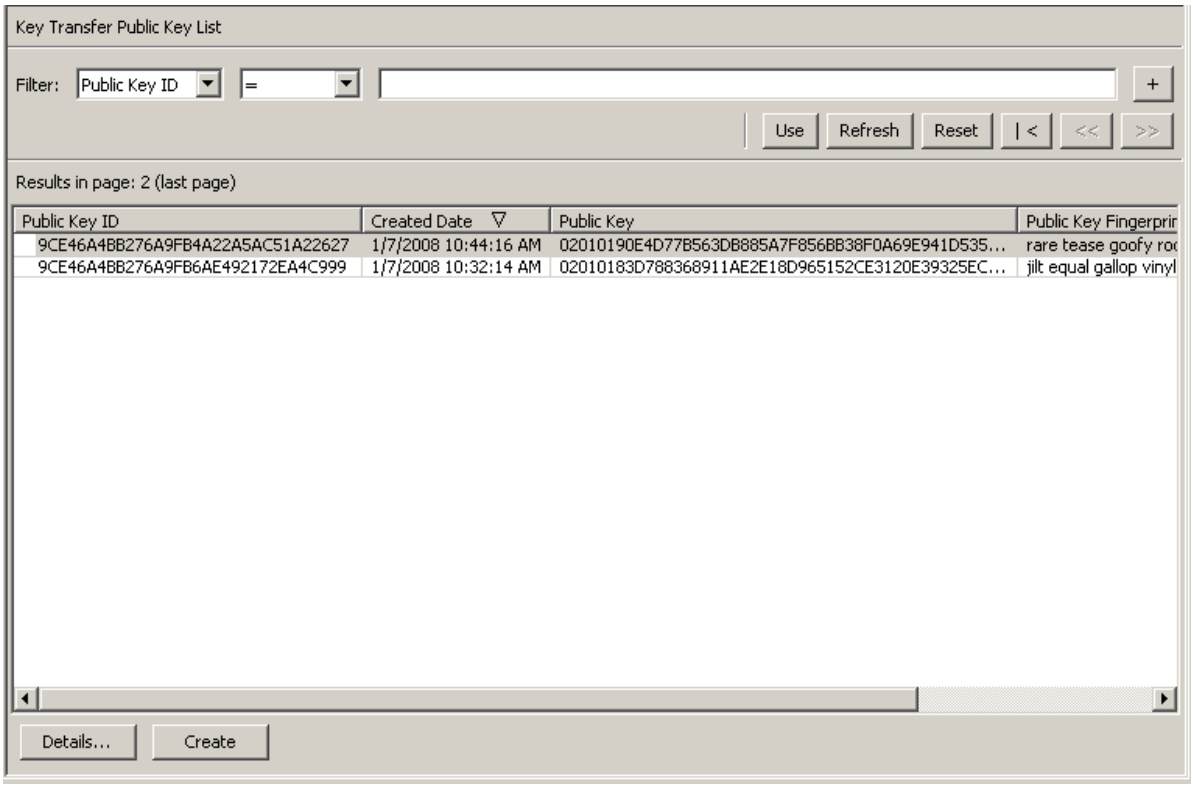
To share keys between Transfer Partners, Security Officers first must access Public Key information for their OKM Cluster. This menu provides public key information. The Public Key and Public Key ID displayed by this command must be sent to the Transfer Partner.



Viewing the Key Transfer Public Key List

To view the Key Transfer Public Key List:

1. From the System Management menu, select Key Transfer Public Key List.



You can also scroll through the database and filter the Key Transfer Public Key List by any of the following keys:

- Public Key ID
- Created Date
- Public Key.

The **Use** button applies the filter to the displayed list for the Key Transfer Public Key List.

The fields and their descriptions are given below:

Filter:

Select filter options to filter the displayed list of Public Keys. Only Public Keys that satisfy all filters will be displayed.

Filter Attribute combo box:

Click the down-arrow and select an attribute to filter by. Possible values are:

- Public Key ID
- Created Date
- Public Key

Filter Operator combo box:

Click the down-arrow and select the filter operation to apply to the selected attribute. This filter option is not displayed for all filter attributes. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value text box:

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Click this button to add additional filters.

Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

Use:

Click this button to apply the selected filters to the displayed list and go to the first page.

Refresh:

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of items that can be displayed on the current page. Appends "(last page)" to the number of items if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

Public Key ID:

Displays the unique identifier that distinguishes each Public Key. This value can be between 1 and 64 (inclusive) characters. Click this Column Name to sort by this attribute.

Created Date:

Displays the date and time when this Public Key was created. Click this Column Name to sort by this attribute.

The private key corresponding to the most recently created public key will be used to sign all exported Key Transfer files.

Public Key:

Displays the Public Key used to perform key transfers between Transfer partners. This value is shown in base 64. Click this Column Name to sort by this attribute.

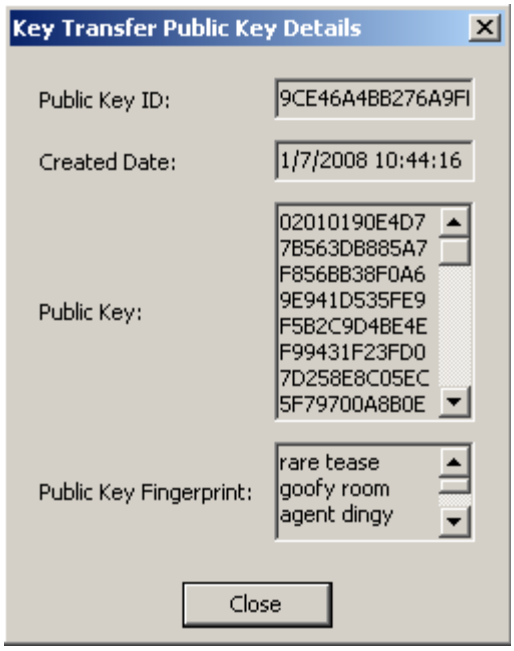
Public Key Fingerprint:

The hash of the Public Key. This value is used to verify the Public Key is correctly transmitted, and it is shown in base 64.

Viewing the Key Transfer Public Key Details

To view the Key Transfer Public Key details screen:

1. Select a Public Key and click the Details button.
   The Key Transfer Public Key Details dialog box is displayed.

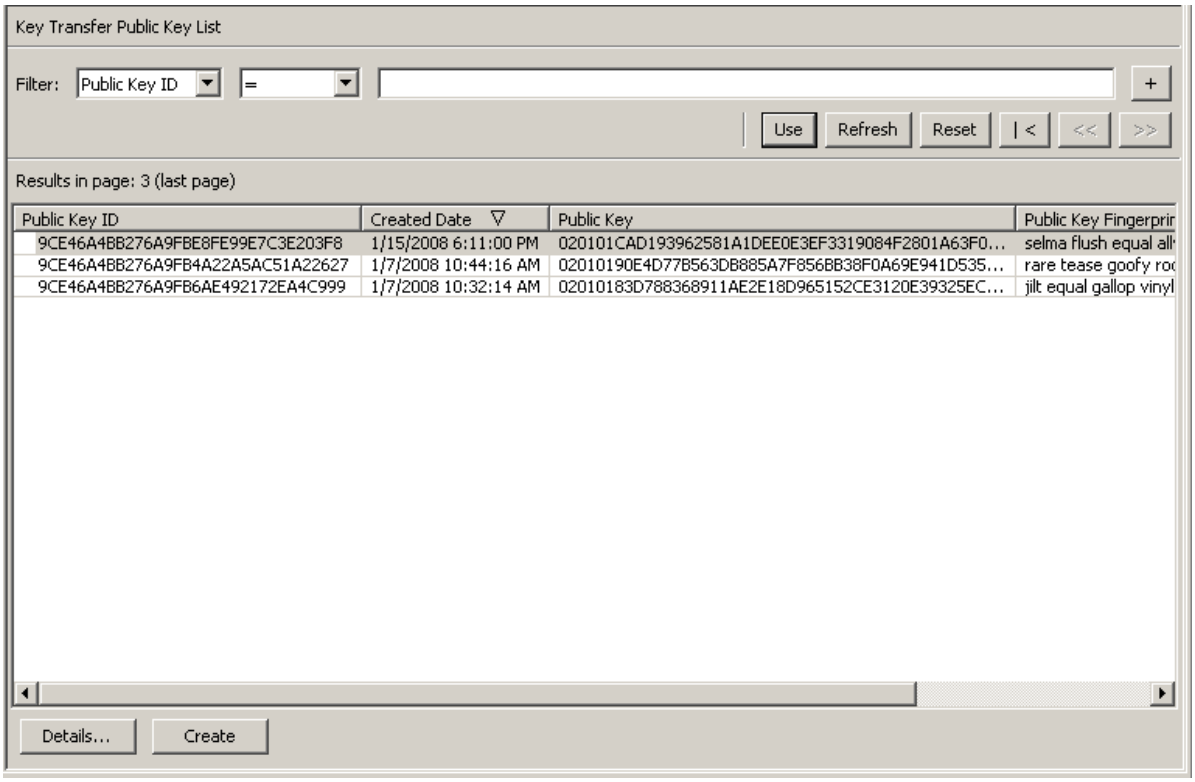


Creating a Key Transfer Public Key

To create a Key Transfer Public Key:

1. Click the Create button.
2. Provide the new key to all existing Transfer Partners.

   Since any Key Transfer files created after the new Key Transfer Public Key is created will be signed with the new Key Transfer Public Key, partners must be provided with the new Key Transfer Public Key before they can import the new Key Transfer files.



Backup List Menu

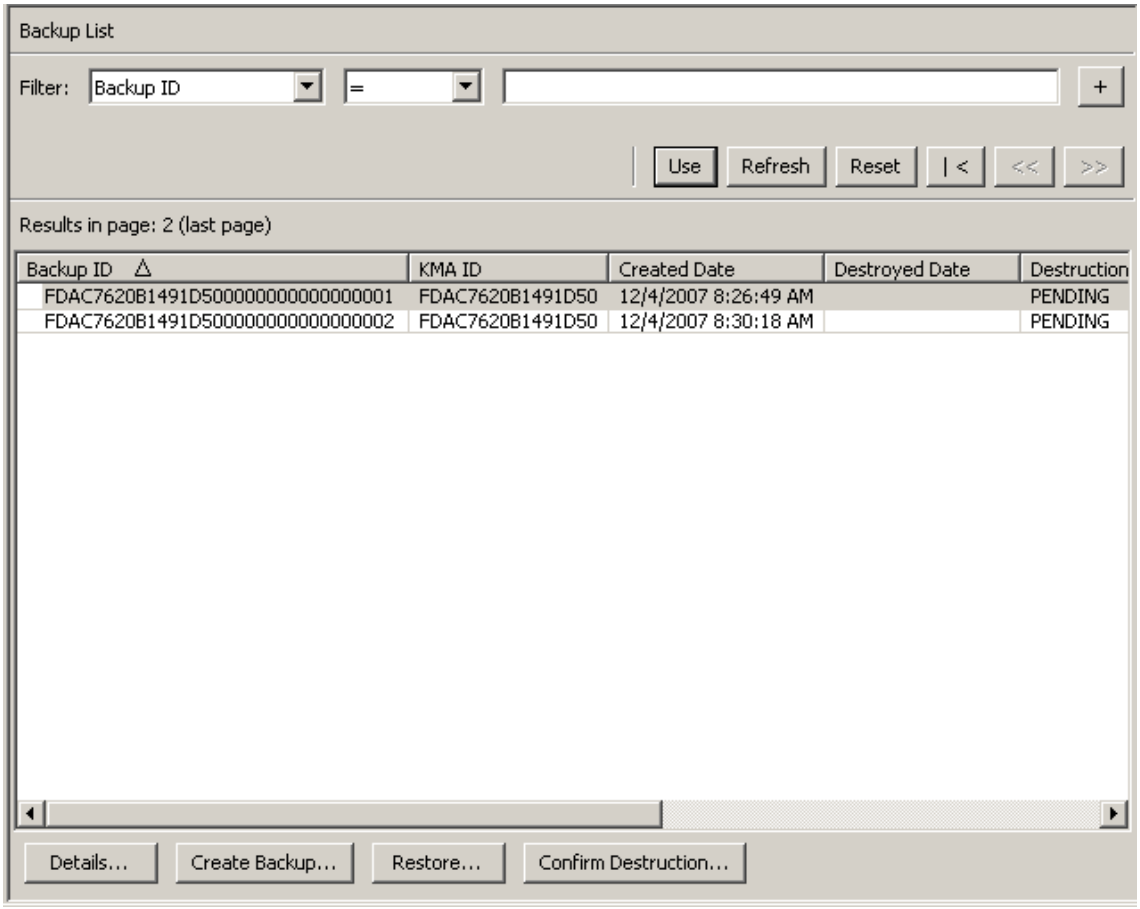
The Backups List menu option allows the Security Officer to:

- View the history of the Backups
- View details of a Backup file
- Restore Backups.

Viewing Backup Files History

To view Backup files history:

From the Secure Information Management menu, select Backup List. The Backup List screen is displayed.



You can also scroll through the database and filter the Backup Files by any of the following keys:

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

The + button applies the filter to the displayed list for the Backup file.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

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

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~

Filter Value 1 box:

If you selected a date filter, click Set Date to specify start date and time. The value appears as a starting value of the filter key range. If you selected any other filter, type a value in this field.

Filter Value 2 box:

If you selected a date filter, click Set Date to select an end date and time. The value appears as a ending value of the filter key range.

Use:

Click this button to apply the filter to the displayed list.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Backup ID

Displays a system-generated unique identifier that distinguishes each Backup file.

KMA ID

Displays the KMA for which the Backup file was generated.

Created Date

Displays the date when the backup was created.

Destroyed Date

Displays the date that the Backup file was marked as being manually destroyed.

Destruction Status

Indicates the status of the backup with respect to its destruction. Possible values are:

NONE

The Backup file has not been destroyed and does not contain Data Unit keys that have been destroyed.

PENDING

The Backup file has not yet been manually destroyed and contains copies of Data Unit keys that have been destroyed.

DESTROYED

The Backup file has been manually destroyed.

Destruction Comment

Displays user-supplied information on the Backup file's destruction.

Details:

Click this button to view more detailed information on a Backup.

Create Backup:

Click this button to create a Backup. This button is not enabled if you are a Security Officer.

Restore:

Click this button to restore a Backup.

Confirm Destruction:

Click this button to confirm the destruction of a Backup. This button is not enabled if you are a Security Officer.

If you want more detailed information on a backup, highlight the backup and click the Details button. For more information, refer to "Viewing Backup Details" on page 180.

Click the Restore button to restore the currently selected backup. For more information, refer to "Restoring a Backup" on page 182.

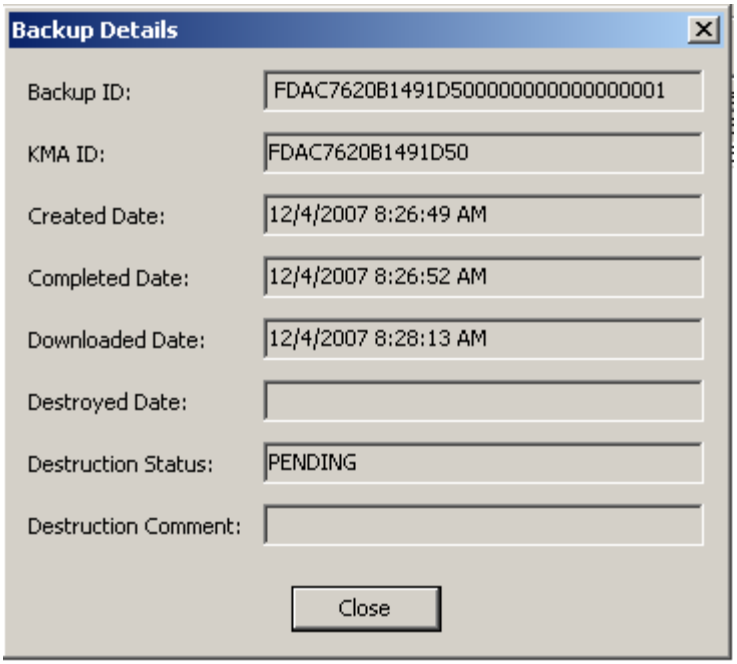
Viewing Backup Details

The Backup Details dialog box is used to view the details of a Backup file.

Note – Backup files are created and restored on the KMA.

To view the details of a Backup file:

1. From the Backups List screen, double-click the Backup entry for which you want more information or highlight the Backup entry and click the Details button. The Backup Details dialog box is displayed, with all fields read-only.



2. The fields and their descriptions are given below:

Backup ID

Displays a system-generated unique identifier that distinguishes each Backup file.

KMA ID

Displays the KMA on which this Backup file is generated.

Created Date

Displays the date and time when the Backup file was created.

Completed Date

Displays the date and time when the Backup file was completed.

Downloaded Date

Displays the date and time when the Backup file was downloaded.

Destroyed Date

Displays the date when the Backup file was destroyed.

Destruction Status

Indicates the status of the backup with respect to its destruction.

Destruction Comment

Displays user-supplied information on the Backup file's destruction.

3. Click the Close button to close this dialog box.

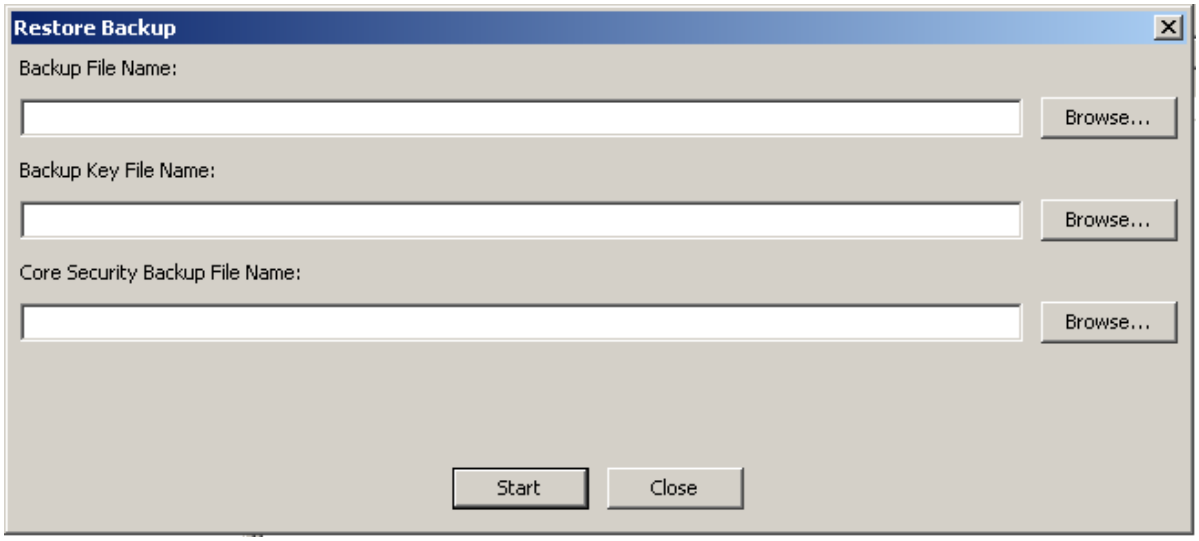
Restoring a Backup

This function gives you the ability to upload and restore a backup that consists of a Backup file and a Backup key file to the KMA. Before you restore a Backup file to a KMA, ensure that you have the quorum for authentication.

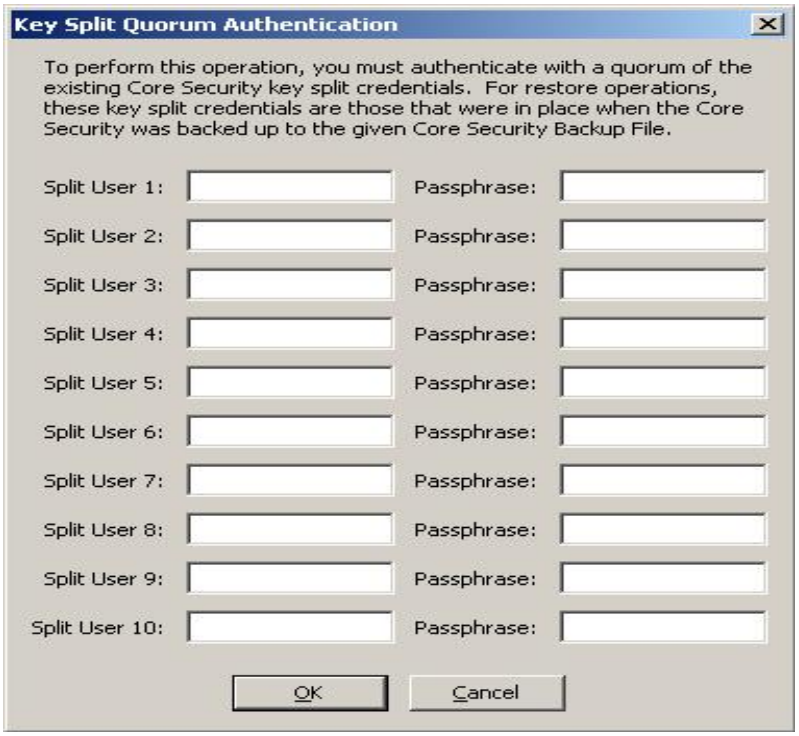
Important – Before you start this procedure, you must perform the procedure "Restoring a Cluster From a Backup" on page 52.

To restore a backup:

1. From the Backup List screen, highlight the Backup you want to restore and click the Restore button. The Restore Backup dialog box is displayed.
2. Select the desired Core Security backup, backup key file, and backup file. The backup key file and the backup must match, that is, they must have been created at the same time. The Core Security backup can be older or newer than the backup key file and backup file. Any Core Security backup file can be used with any backup key file and backup file.
3. Click the Start button.



4. When the upload process is completed, it is indicated on the Restore Backup dialog box and the Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



Note – The Security Officer must provide a sufficient quorum of Key Split Credentials. You initially set the Key Split Threshold value, which determines the quorum size, through the "Entering Key Split Credentials" operation shown on page 40. The quorum value can be changed using "Modifying the Key Split Configuration" discussed on page 198.

If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

5. The Restore Backup dialog box is displayed, indicating the status of the restore process.
6. The fields and their descriptions are given below:

Backup File Name

Name of the backup file.

Backup Wrapping Key File Name

Displays the name of the Backup Key File.

Core Security Backup File Name

Name of the backup file containing Core Security Key material.

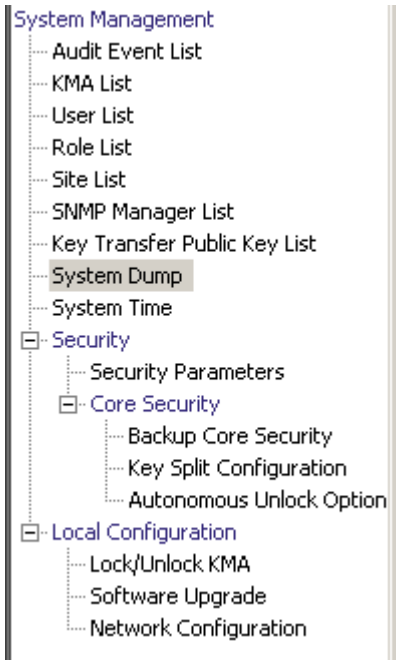
7. When the restore is completed, a message indicating this is displayed. Click the Close button to close this dialog box. The database and the Secure Key Store are restored to the KMA.

Note – After you successfully restore a backup, you need to update the IP address settings for the KMA. Network settings are not backed up, and thus are not restored. Refer to "Setting the KMA Management IP Address" on page 339 and "Setting the KMA Service IP Addresses" on page 341.

System Dump Menu

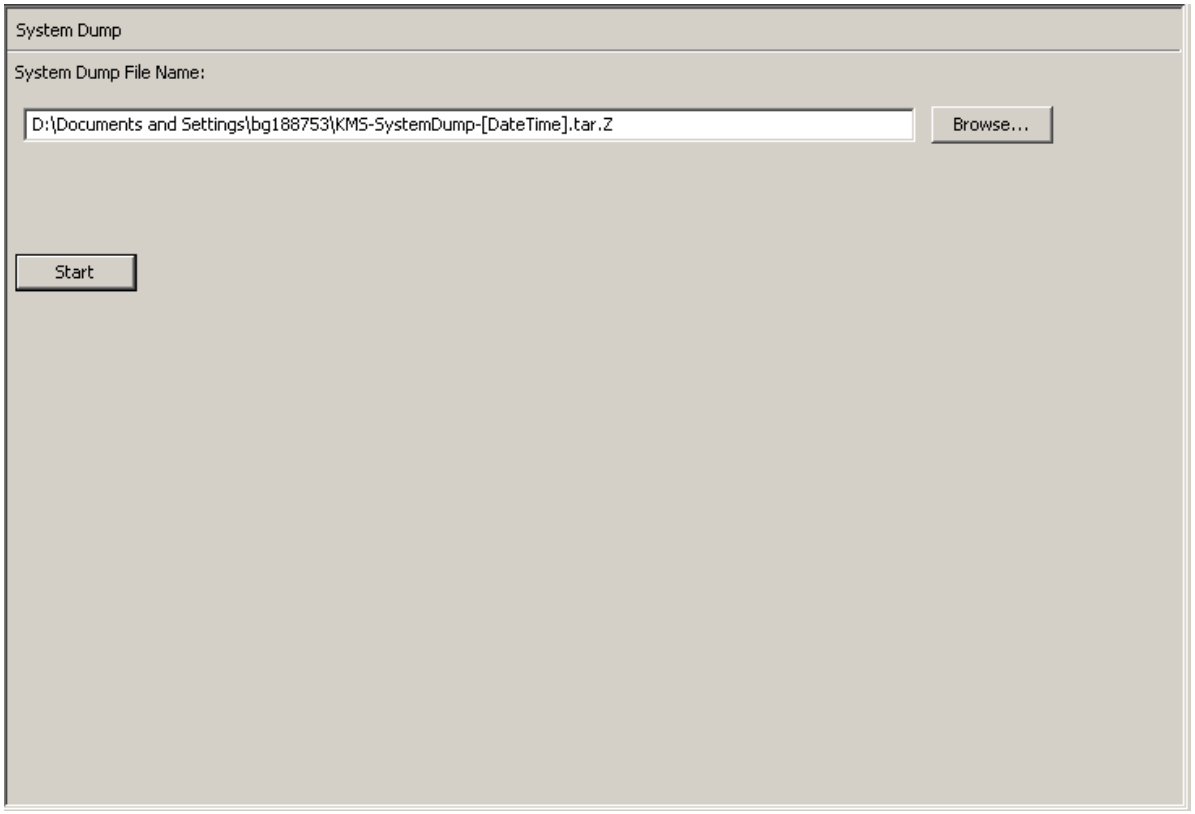
The System Dump menu creates a system dump for problem resolution and downloads it to a compressed file on the system where the OKM Manager is running. The downloaded file is in a format that can be opened with compression utilities.

Note – The dump does not include any key material or information from which keys can be inferred.



Creating a System Dump

1. To create a system dump, from the System Management menu, select System Dump. The screen is displayed and shows an automatically-generated *.tar.Z file. If desired, you can click Browse to select a destination path.
2. Click the Start button to begin the download. The system displays messages indicating the amount of system dump information that is being downloaded in real-time and tells you when the process is complete.
3. Go to the destination path and open the *.tar.Z file to view the system dump information.



The fields and their descriptions are given below:

File Name:

Displays an automatically-generated *.tar.gz file.

Browse:

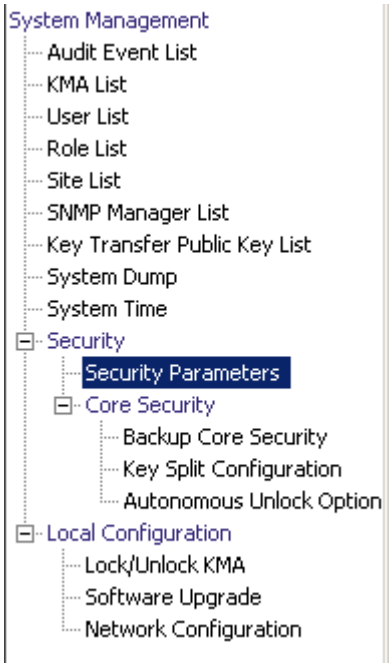
Click this button to specify a location for this file.

Start:

Click this button to initiate the download process.

Security Parameters Menu

The Security menu gives the Security Officer the ability to view and modify the KMA's security parameters.



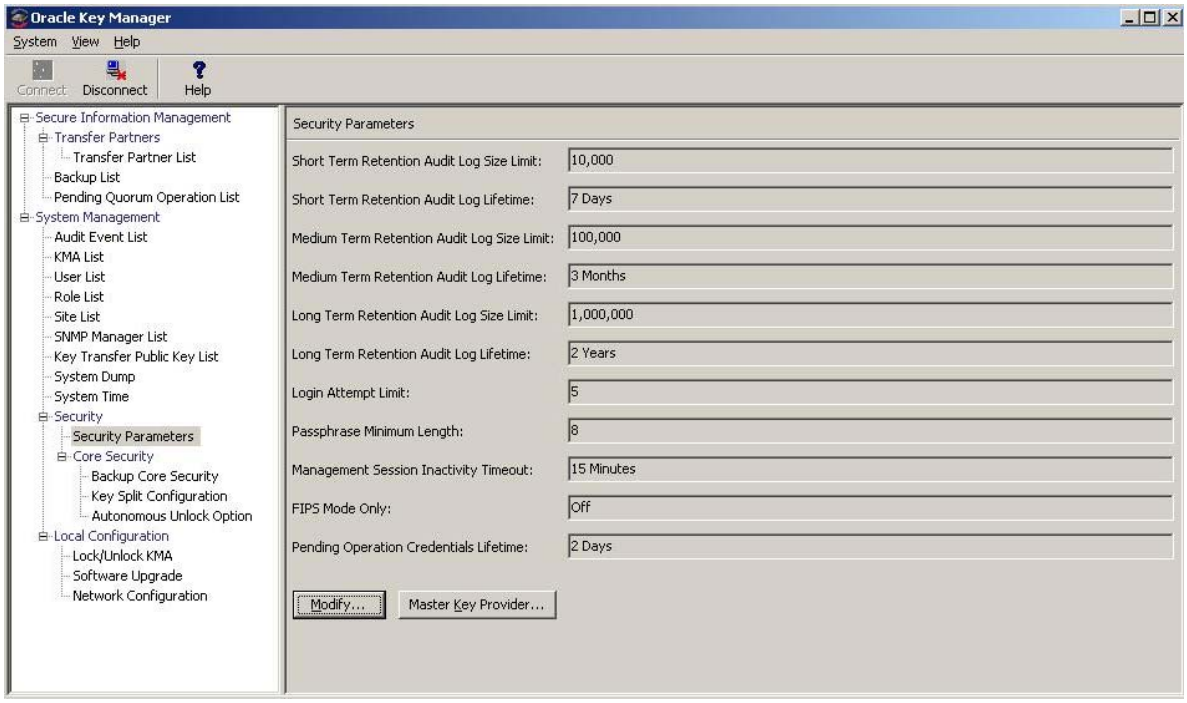
Retrieving the Security Parameters

Note – The Master Key Provider button is used only if you want the OKM Cluster to obtain master keys from an IBM mainframe. The button is enabled only when the replication version of the OKM Cluster is currently set to 11 or higher and the FIPS Mode Only value is "Off."

See the *OKM-ICSF Integration Guide* for details.

To retrieve the security parameters:

From the Security menu, select Security Parameters. The Security Parameters screen is displayed in read-only mode.



The fields and their descriptions are given below:

Note – For the following six Retention-related fields, there is just one audit log, and it resides in the largest file system in the KMA.

The main reason for adjusting these parameters is to control how many audit log entries are returned in queries you issue from the Audit Event List menu (see "Viewing Audit Logs" on page 256).

Entries in the audit log can show a short, medium, or long retention term. The KMA truncates (removes) old audit log entries based on the limit and lifetime of their retention term.

For example, Short Term Audit Log entries are typically truncated more frequently than Medium Term Audit Log entries; Medium Term Audit Log entries are truncated more frequently than Long Term Audit Log entries.

The Security Officer can define these retention term limits and lifetimes to control how frequently old audit log entries are removed.

Short Term Retention Audit Log Size Limit

Displays the number of Short Term Audit Log entries that are retained before they are truncated. The default is 10,000. The minimum value is 1000; maximum value is 1,000,000.

Short Term Retention Audit Log Lifetime

Displays the amount of time (in days) that Short Term Audit Log entries are retained before they are truncated. The default is 7 days. The minimum value is 7 days; maximum value is 25,185 days (approximately 69 years).

Medium Term Retention Audit Log Size Limit

Displays the number of Medium Term Audit Log entries that are retained before they are truncated. The default is 100,000. The minimum value is 1000; maximum value is 1,000,000.

Medium Term Retention Audit Log Lifetime

Displays the amount of time (in days) that Medium Term Audit Log entries are retained before they are truncated. The default is 90 days. The minimum value is 7 days; maximum value is 25,185 days.

Long Term Retention Audit Log Size Limit

Displays the number of Long Term Audit Log entries that are retained before they are truncated. The default is 1,000,000. The minimum value is 1000; maximum value is 1,000,000.

Long Term Retention Audit Log Lifetime

Displays the amount of time (in days) that Long Term Audit Log entries are retained before they are truncated. The default is 730 days. The minimum value is 7 days; maximum value is 25,185 days.

Login Attempt Limit

Indicates the number of failed login attempts before an entity is disabled. The default is 5. The minimum value is 1; maximum value is 1000.

Passphrase Minimum Length

Displays the minimum length of the passphrase. The default is 8 characters. The minimum value is 8 characters; the maximum value is 64 characters.

Management Session Inactivity Timeout

Displays the maximum length of time (in minutes) a OKM Manager or Console login session can be left idle before being automatically logged out. Changing this value has no effect on sessions that are already in progress. The default is 15 minutes. The minimum value is 0, meaning no time is used; the maximum value is 60 minutes.

FIPS Mode Only

Displays the import key and format transfer file settings.

An **Off** value means KMAs do not wrap Keys. The KMA can import 1.0 keys and allows export and import of v2.0 or v2.1 (FIPS) format transfer files.

An **On** value means KMAs in this Cluster wrap Keys with an Advanced Encryption Standard (AES) wrapping key before sending them to Agents (tape drives). The KMA cannot import 1.0 keys and allows export and import of v2.1 (FIPS) format transfer files only.

The **On** value can be set only if the current Replication Version is at least 10.

See the **Export Format** parameter in "Transfer Partner List Menu" on page 157 for more information.

Pending Operation Credentials Lifetime:

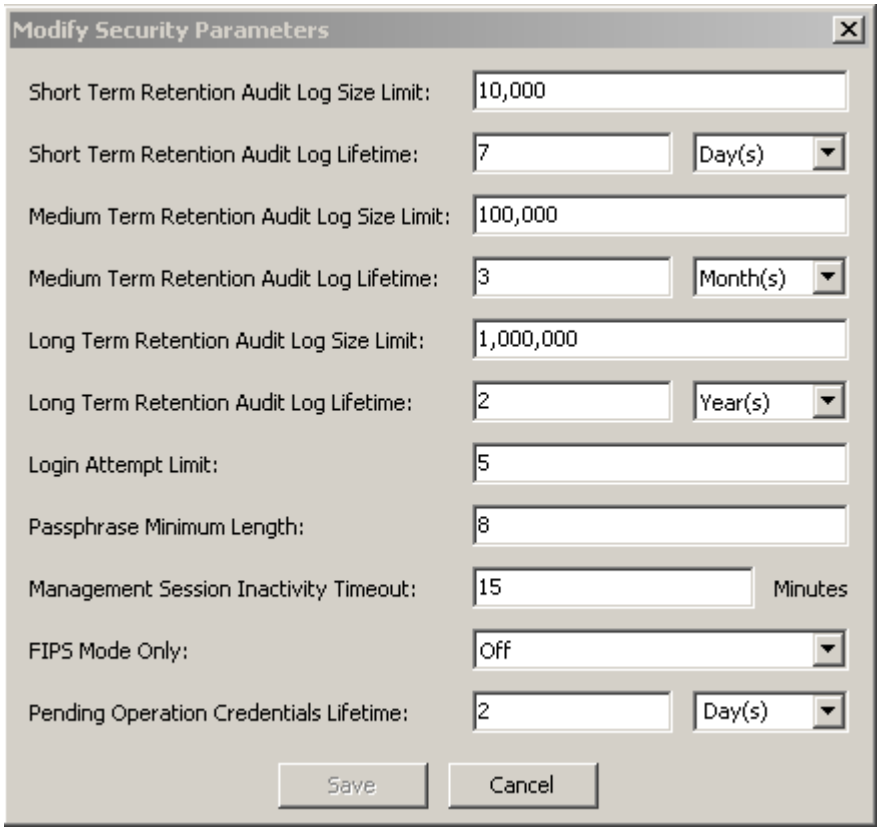
The amount of time (in days) that Key Split Credentials are retained as having approved a pending quorum operation. If an insufficient number of Key Split Credentials approve the pending quorum operation before this lifetime is reached, then these credentials expire. After they expire, Quorum Members must reapprove the pending quorum operation. The default is 2 days. This value is used only when the Replication Version is at least 11.

If you want to change the Security Parameters, click the Modify button. For more information, refer to "Modifying the Security Parameters" on page 192.

Modifying the Security Parameters

To modify security parameters:

1. From the Security Parameters List screen, click the Modify button. The Modify Security Parameters screen is displayed.



The fields are described on page 190.

2. Modify the security parameters, as required. When you are finished, click the Save button. The changes are saved in the KMA database.

Core Security

The primary element of the Core Security component is the Root Key Material. It is key material that is generated when a Cluster is initialized. The Root Key Material protects the Master Key. The Master Key is a symmetric key that protects the Data Unit Keys stored on the KMA.

Core Security is protected with a key split scheme that requires a quorum of users defined in the Key Split Credentials to provide their user names and passphrases to unwrap the Root Key Material.

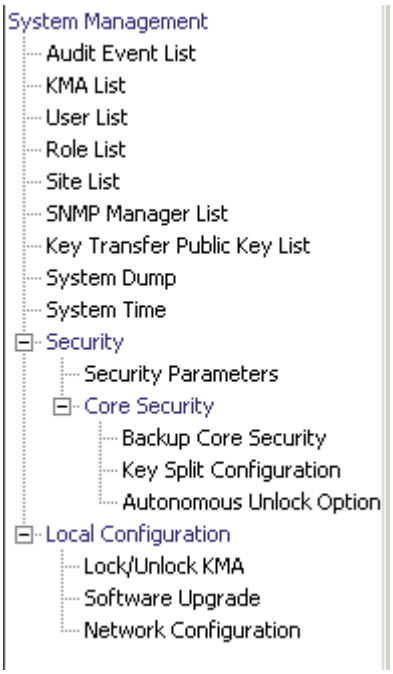
This security mechanism enables two operational states for the KMA: locked and unlocked.

A KMA in the locked state is not able to unwrap the Root Key Material, and thus is unable to access the Data Unit Keys. As a result, the KMA is unable to service Agent requests to register new Data Units or retrieve Data Unit Keys for existing Data Units.

A KMA in the unlocked state is able to use the Root Key Material to access the Data Unit Keys and service Agent requests for Data Unit Keys.

Core Security Management Menu

The Core Security menu contains the following menu options:



It allows the Security Officer to:

- Create a Core Security backup
- View/Modify Key Split Credentials
- Enable/Disable the Autonomous Unlock Option.

Backup Core Security

The Backup Core Security option allows the Security Officer to back up Core Security Key material and download it to a file on the local system.

Caution – Core security backup files should be carefully protected. Because any Core Security backup file can be used with any backup file/backup key file pair, even old Core Security backup files remain useful.

Creating a Core Security Backup

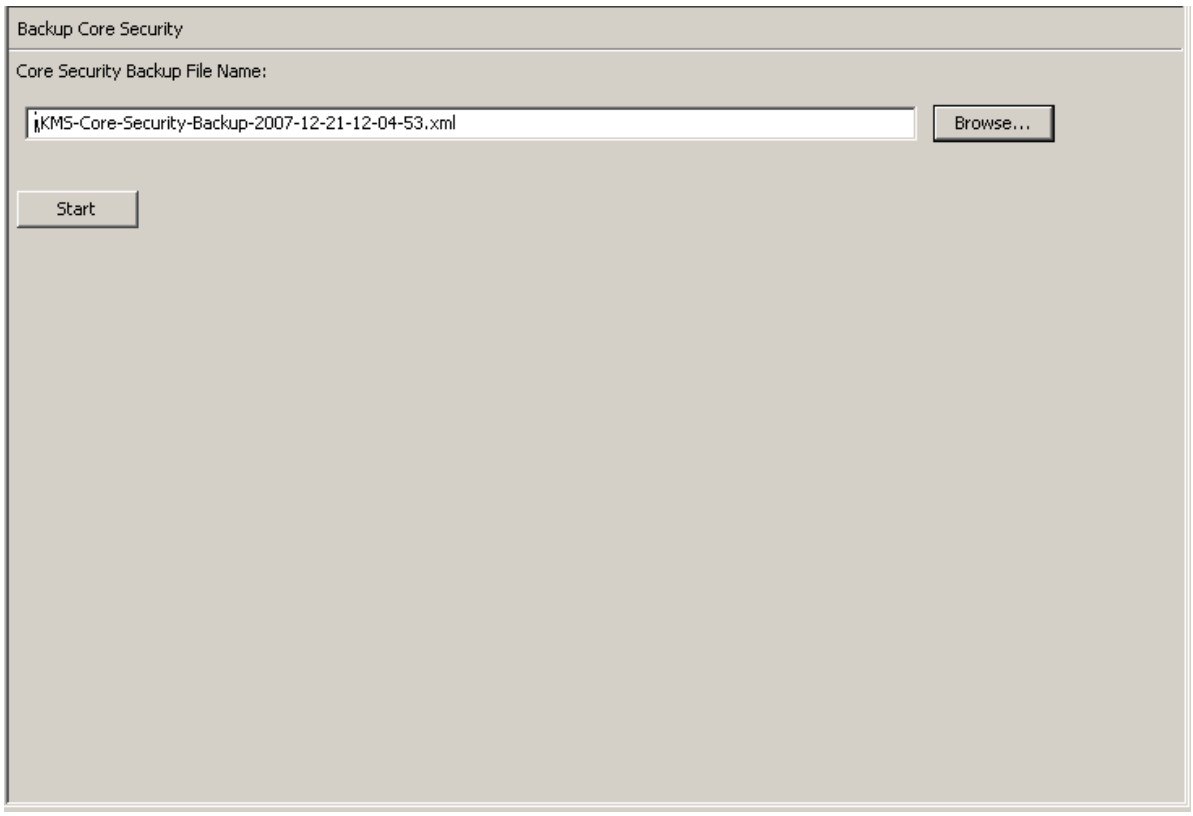
A new core security backup needs to be performed after the Key Split Credentials are modified.

Important – The Security Officer must back up Core Security Key material before the Backup Officer can create a backup. See "Creating a Backup" on page 305.

---

1. From the Core Security menu, select Backup Core Security. The Backup Core Security dialog box is displayed.

Note – The Core Security Backup File names are automatically generated. However, you can edit the names, and you can also click the Browse button to select a destination path.



2. Select the Start button to create the Core Security Backup file and download it to the user-specified destination.
3. When the backup is completed, a message is displayed. Click the Close button to close this dialog box
4. You are returned to the Backup Core Security screen.

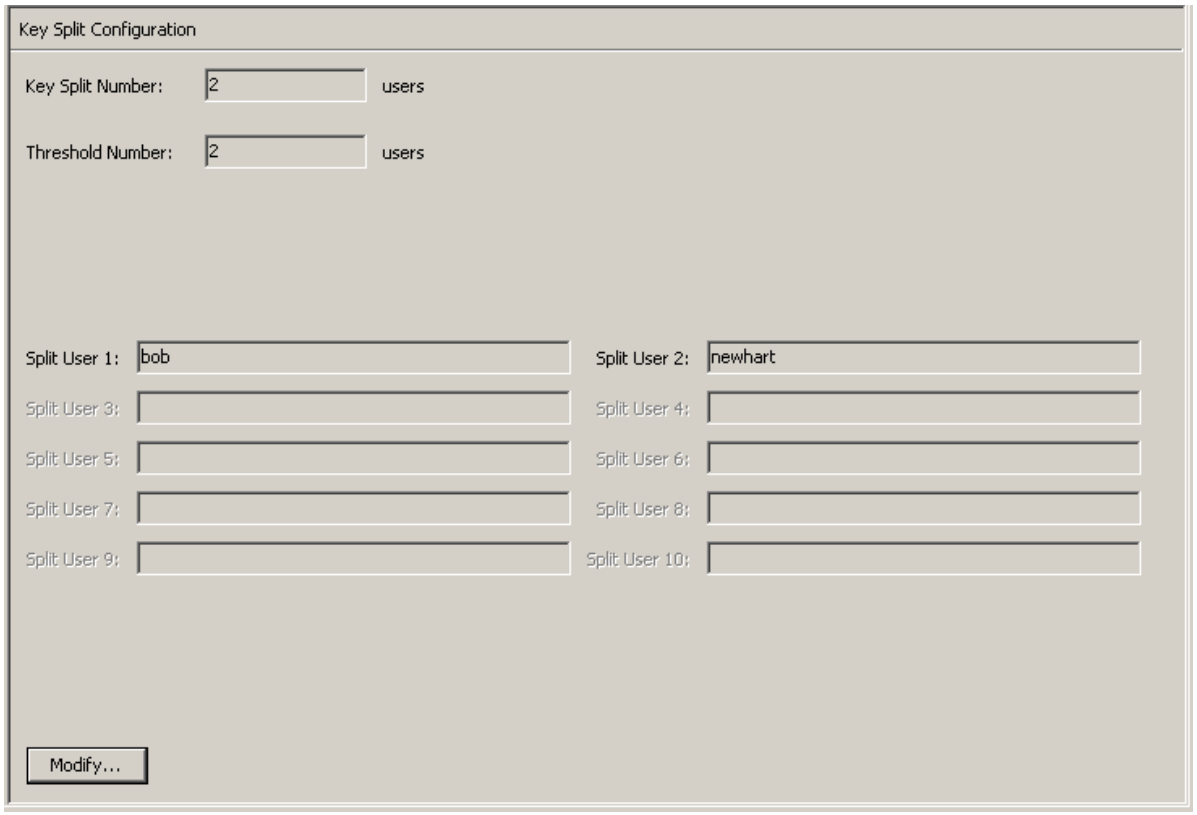
Key Split Configuration

The Key Split Configuration menu option gives the Security Officer the ability to view and modify the Key Split Credentials for the KMA.

Viewing the Key Split Configuration

To view the Key Split Configuration:

1. From the Core Security menu, select Key Split Configuration. The Key Split Configuration dialog box is displayed.



The fields and their descriptions are given below:

Key Split Number

Displays the number of key splits. The maximum is 10.

Threshold Number

Displays the number of users that are necessary to authenticate a quorum.

Split User (1-10)

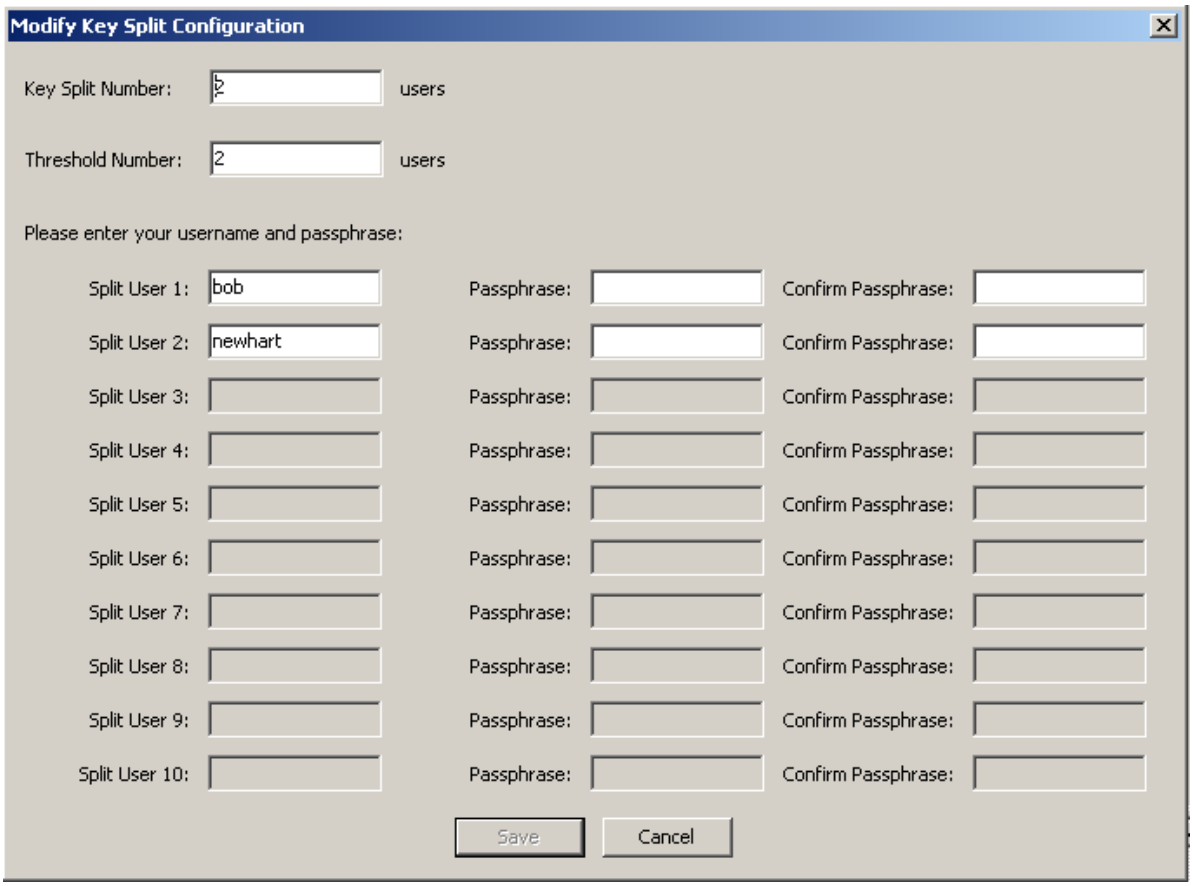
Displays the user names of the existing split.

If you want to modify the Key Split user names, passphrases, and threshold number, click the Modify button. For more information, refer to "Modifying the Key Split Configuration" on page 198.

Modifying the Key Split Configuration

To modify the Key Split configuration:

1. From the Key Split Configuration screen, click the Modify button. The Modify Key Split Configuration dialog box is displayed.



2. Complete the following parameters and click the OK button:

Key Split Number

Type a new value for the number of key splits. The maximum number is 10.

Threshold Number

Type a new value for the number of users that will be required to form a quorum.

Split User *x*

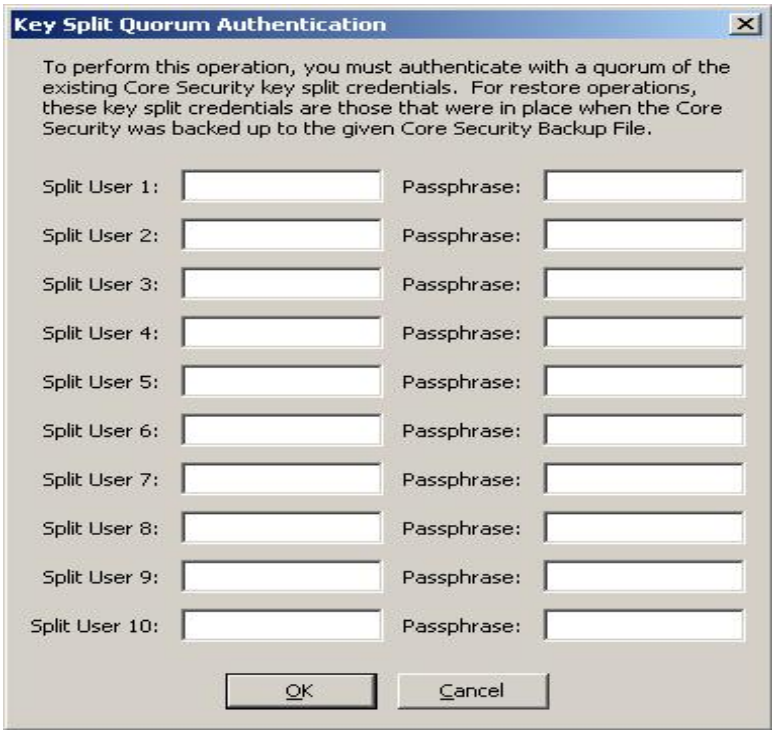
Type the new user name. For each Split User, complete its associated Passphrase and Confirm Passphrase fields.

Note – The number of Split User fields that are enabled is dependent on the value that you entered in the Key Split Number field.

---

3. Click the Save button after the last user name and passphrase is entered.

4. The Key Split Quorum Authentication dialog box is displayed after the new Key Split credentials are entered. Type the user name and passphrase for the existing quorum credentials and click the OK button. This is required to set "new" credentials set in Step 2 and Step 3.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

5. The system updates the old configuration information with the new configuration in the database. The new configuration is displayed in the Key Split Credentials screen.

Note – The Core Security Key material is re-wrapped using the updated Key Split credentials.

---

6. Create a new Core Security backup (see "Creating a Core Security Backup" on page 195).

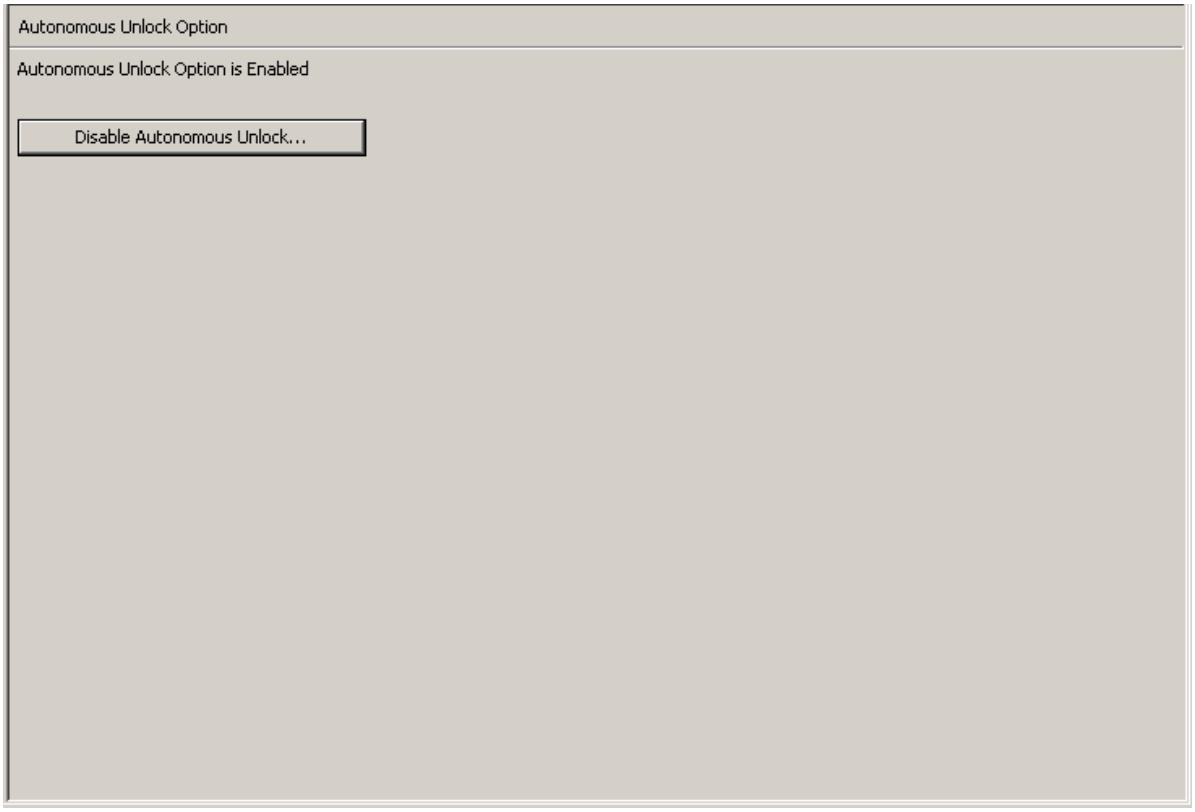
Note – Destroy all old Core Security backup files to ensure that the previous Key Split Credentials cannot be used to destroy a backup.

Autonomous Unlock Option

The Autonomous Unlock Option menu option gives the Security Officer the ability to enable or disable the autonomous option for the KMA.

To enable or disable the Autonomous Unlock option:

1. From the Core Security menu, select Autonomous Unlock Option. The Autonomous Unlock Option screen is displayed, indicating the current autonomous status.



2. Depending on the current autonomous boot status, click the Enable Autonomous Unlock to enable this option or click the Disable Autonomous Unlock to disable the option.

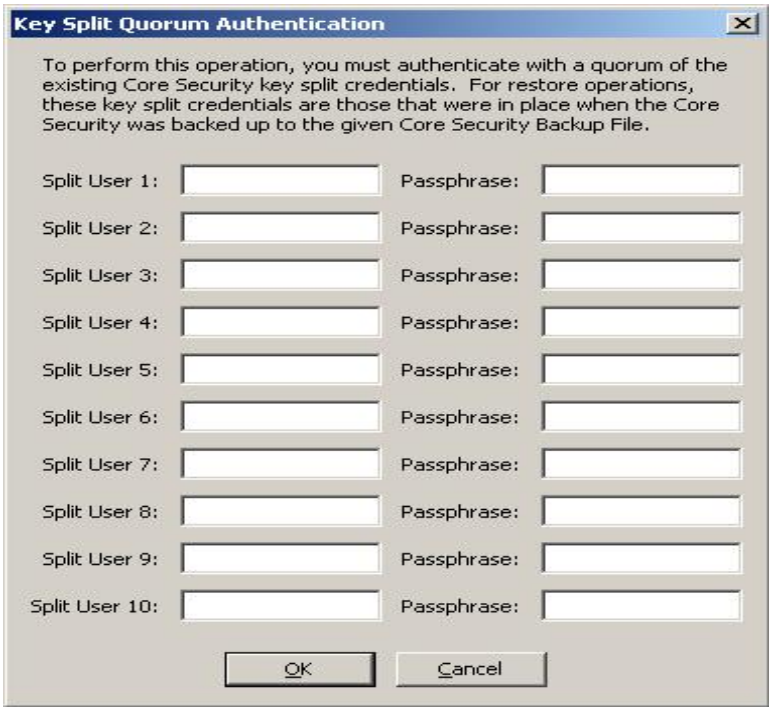
Notes –

• The Lock/Unlock button toggles between states and sets the KMA locked state opposite to the current state.

• You must provide a quorum to enable or disable the Autonomous Unlock Option.

---

3. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

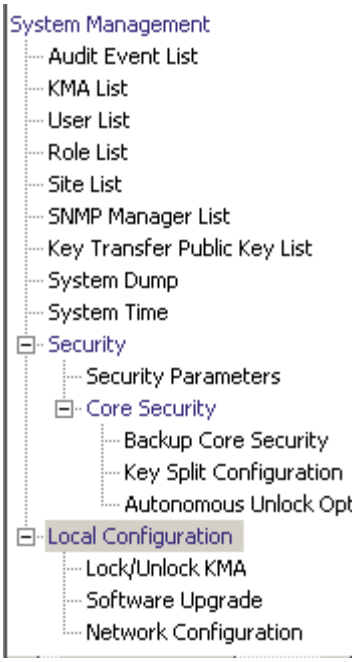
If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

Local Configuration Menu

The Local Configuration menu includes the following options:

- Lock/Unlock the KMA
- Upgrade the software (see "Software Upgrade Menu" on page 294)
- Network configuration information.



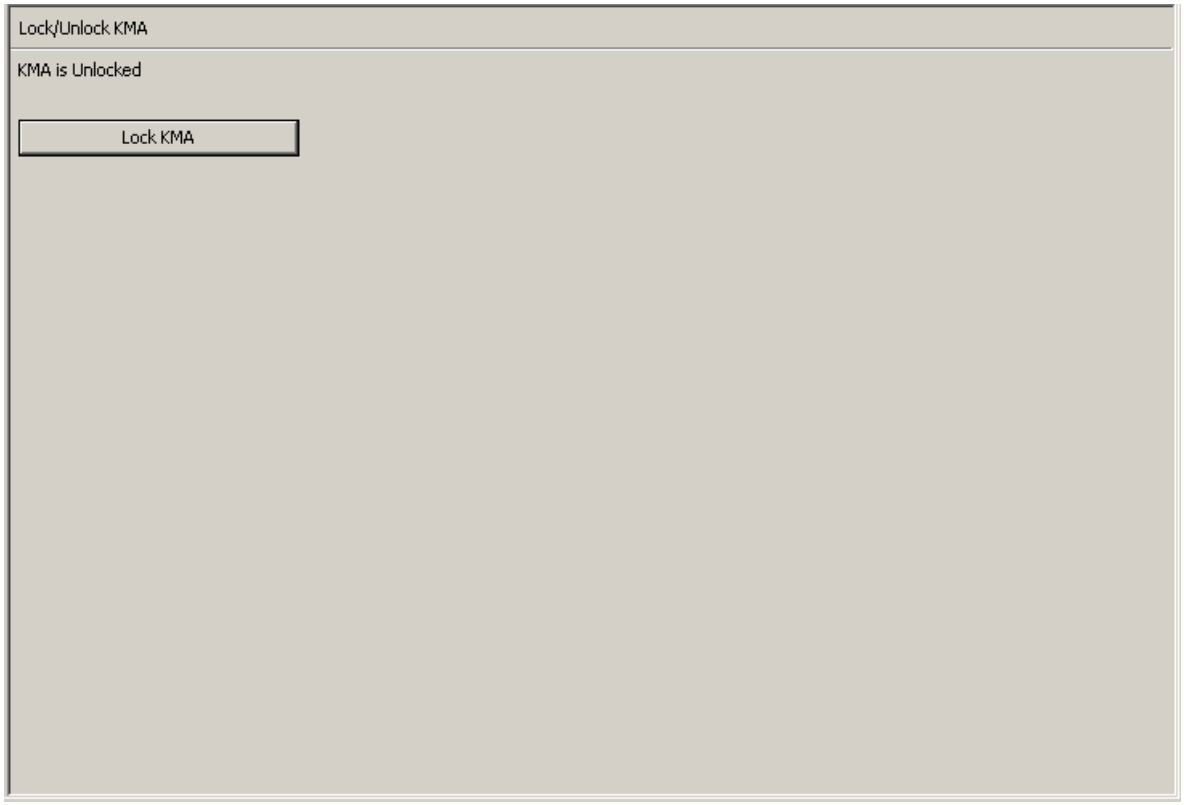
Lock/Unlock KMA

The Lock/Unlock KMA menu option gives the Security Officer the ability to lock and unlock the KMA's Core Security. Please see "Core Security" on page 193 for details on Core Security and the behavior of the KMA when Core Security is locked and unlocked.

Locking the KMA

To lock the KMA:

1. From the Local Configuration menu, select **Lock/Unlock KMA**. The Lock/Unlock KMA screen is displayed, indicating the state of the KMA. In this example, it is "Unlocked."



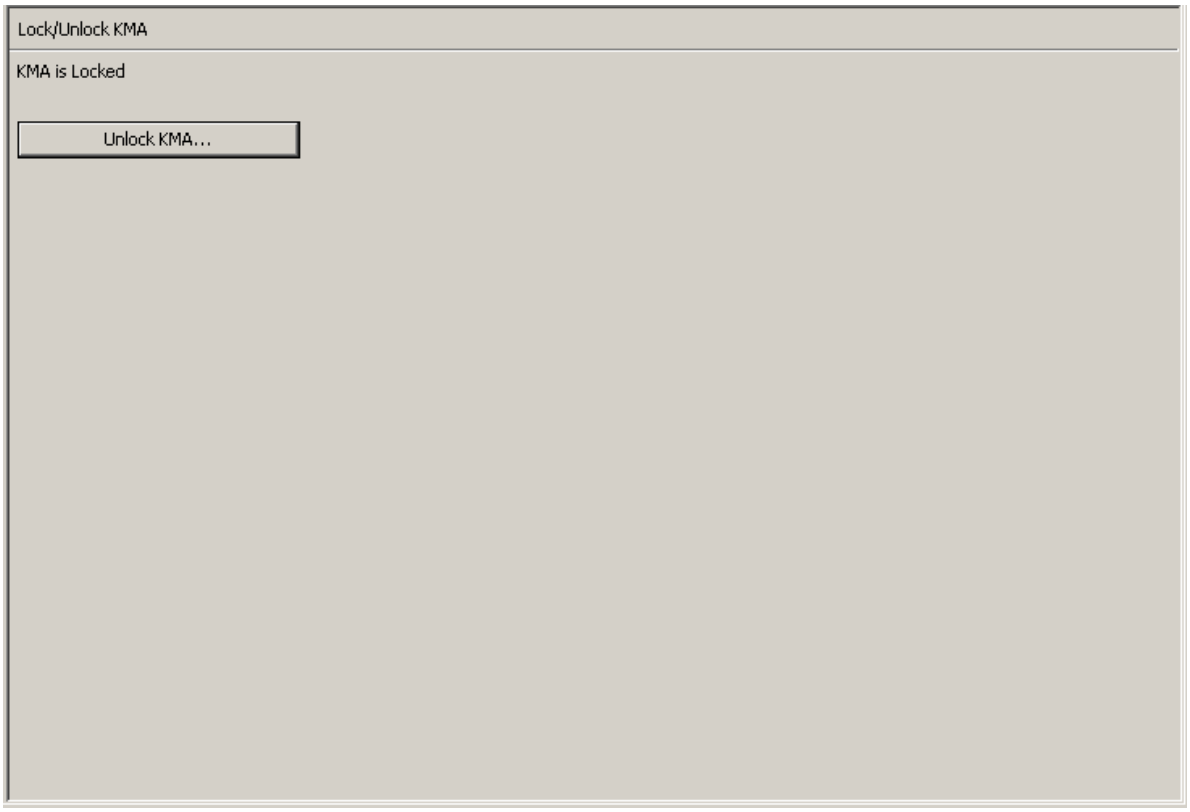
2. Click the Lock KMA button to lock the KMA. Once the button is pressed, it changes to Unlock KMA, indicating the new lock state and the allowed operation. The KMA is now locked.

Note – The Lock KMA/Unlock KMA button toggles between states and sets the KMA locked state opposite to the current state. Once a button is pressed, the text label and button label change to indicate the new lock state and the allowed operation.

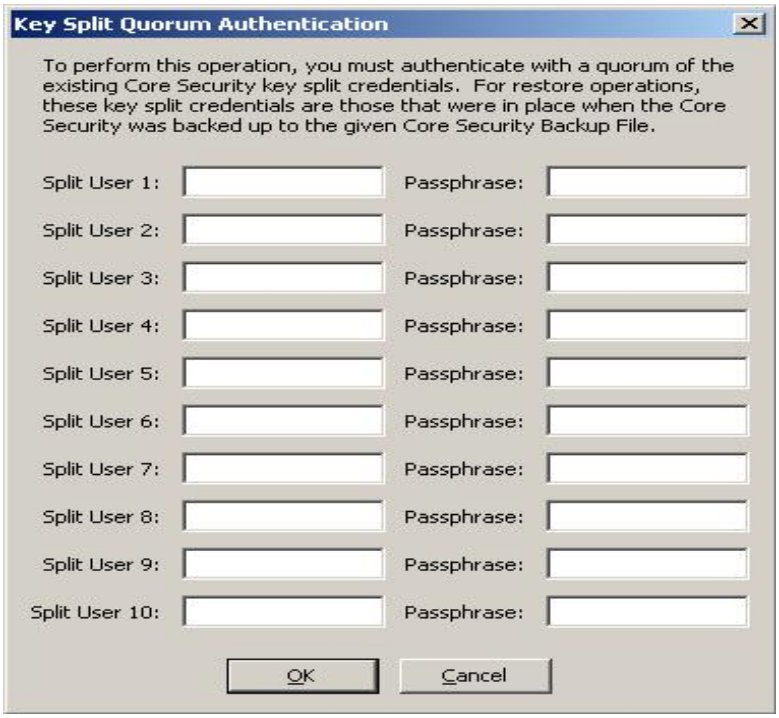
Unlocking the KMA

To unlock the KMA:

1. From the Lock/Unlock KMA screen click the **Unlock KMA** button.



2. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.

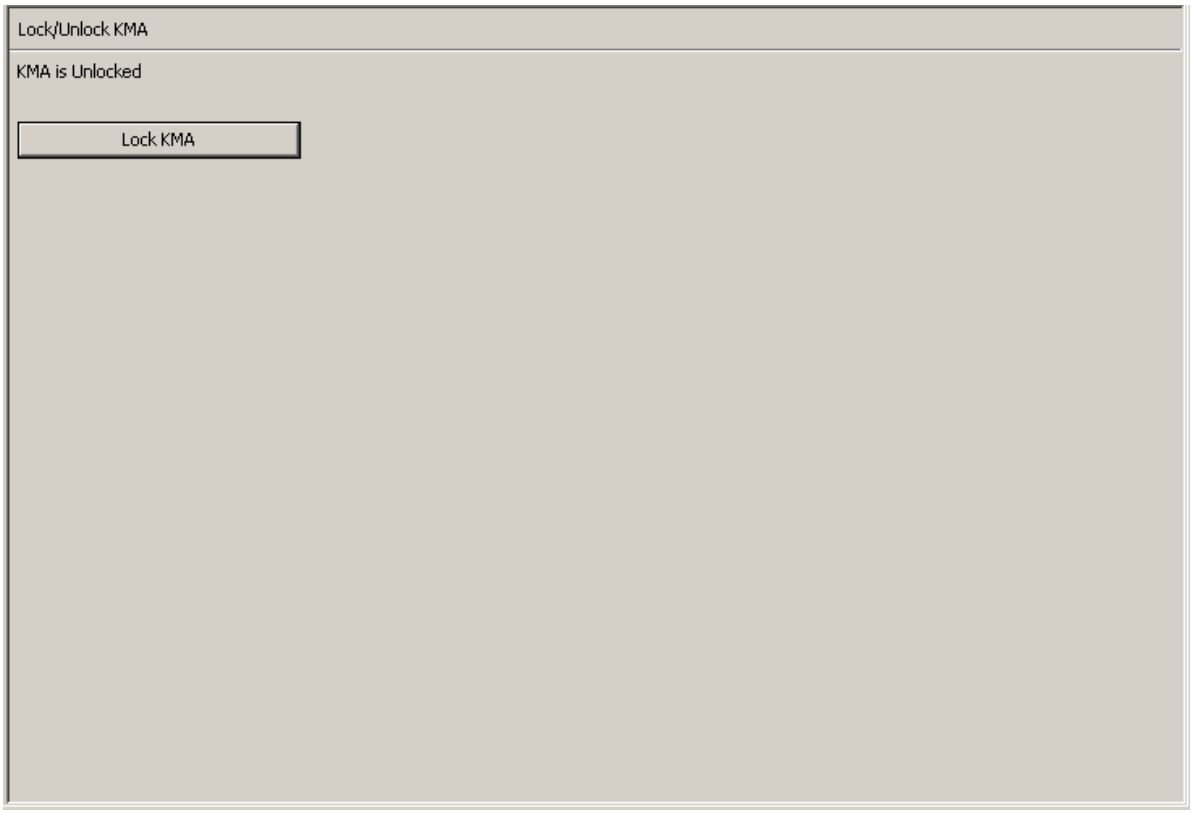


If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

3. If the authentication is successful, the Key Split Quorum Authentication dialog box closes and the KMA is unlocked.

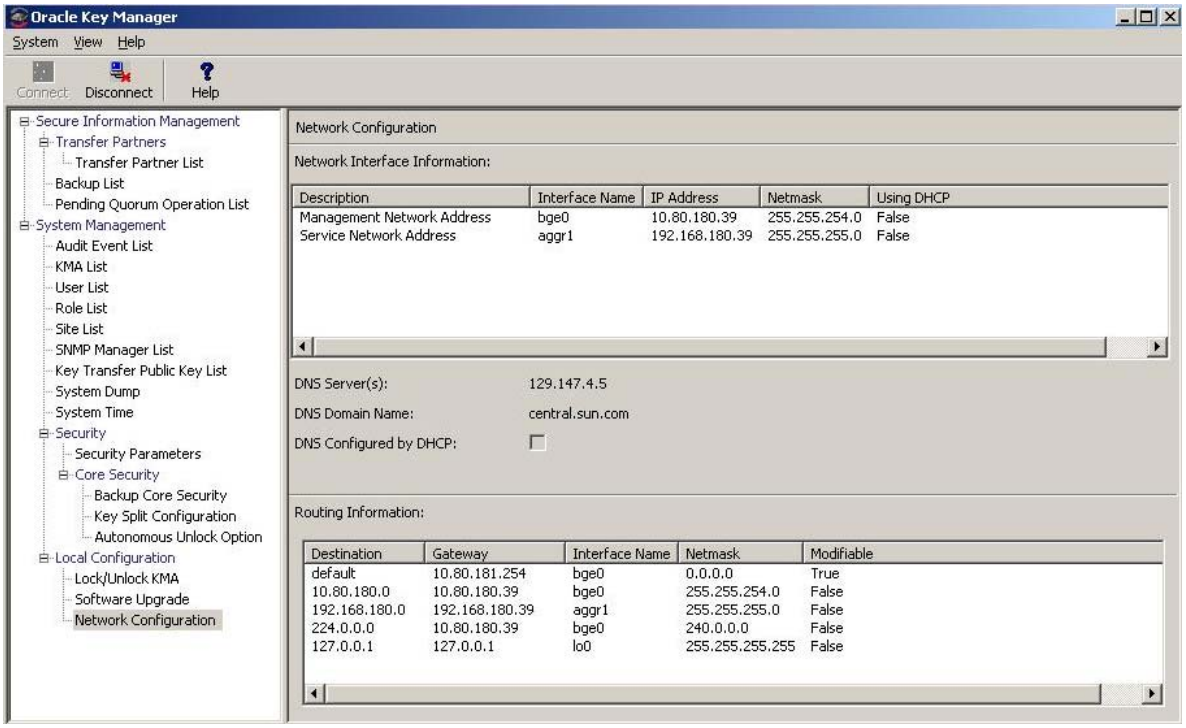


Network Configuration Information

The Network Configuration menu option shows network configuration settings for the KMA to which you are currently connected. These settings are established in the configuration screens described in "Using the OKM Console" on page 323.

Displaying the Network Configuration

To display the network configuration, from the Local Configuration menu, select **Network Configuration**. The Network Configuration screen is displayed.



The fields are described below:

Description

Displays whether the related information applies to the Management or Service Network Address.

Interface Name

The Management or Service Network Hostname established in the QuickStart program.

IP Address

The IP address of the Management or Service Network.

Netmask

The Subnet Mask address for the Management or Service Network.

DNS Server(s)

One or more DNS name servers (if any) used by this KMA.

DNS Domain Name

The DNS domain (if any) used by this KMA.

DNS Configured by DHCP

An indication whether these DNS settings were configured implicitly by DHCP.

Using DHCP

Indicates whether or not the Management or Service Network uses DHCP.

Destination

The subnet that network traffic goes to from this KMA.

Gateway

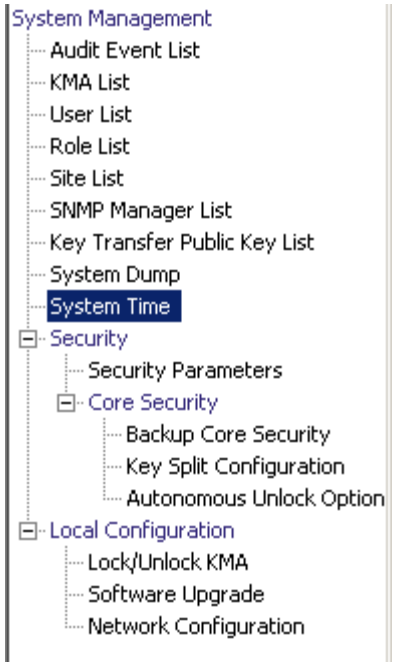
The Gateway IP address that network traffic is routed to for the Management or Service Network.

Modifiable

Indicates whether or not the Gateway configuration is modifiable. Gateways that are configured automatically are not modifiable.

System Time Menu

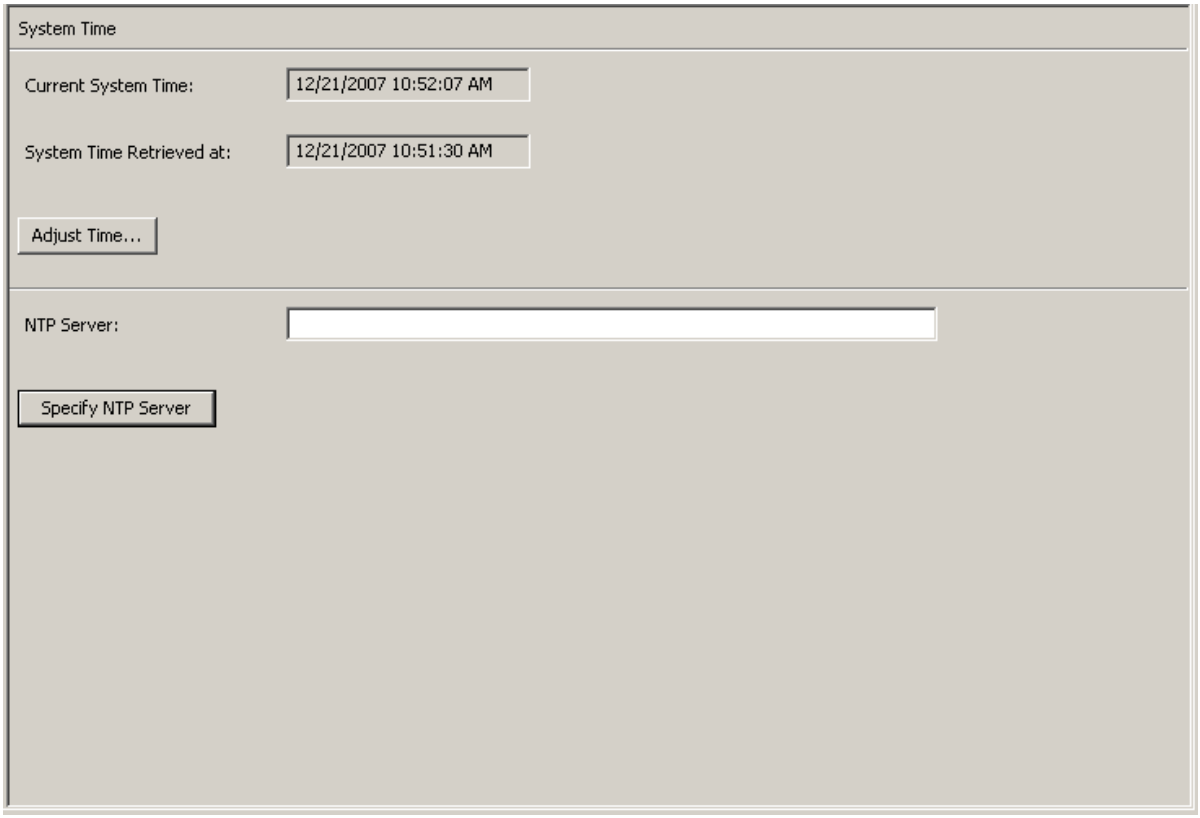
The System Time menu option gives you the ability to set the system clock to which you are connected. To ensure the correct operation of the OKM solution, it is very important to maintain the times reported by each KMA in a Cluster within five minutes of each other.



Retrieving the Local Clock Information

To retrieve the local clock information:

From the System Management menu, select **System Time**. The System Time screen is displayed.



The fields and their descriptions are given below:

Current System Time

Displays the current system time.

System Time Retrieved At

Displays the local Client time when the KMA's system time was retrieved.

Adjust Time

Click this button to modify the system time.

If you want to modify the KMA's clock, click the Adjust Time button. For more information, refer to "Adjusting the KMA's Local Clock" below.

NTP Server

Displays the NTP server that this KMA uses (if any).

Specify NTP Server

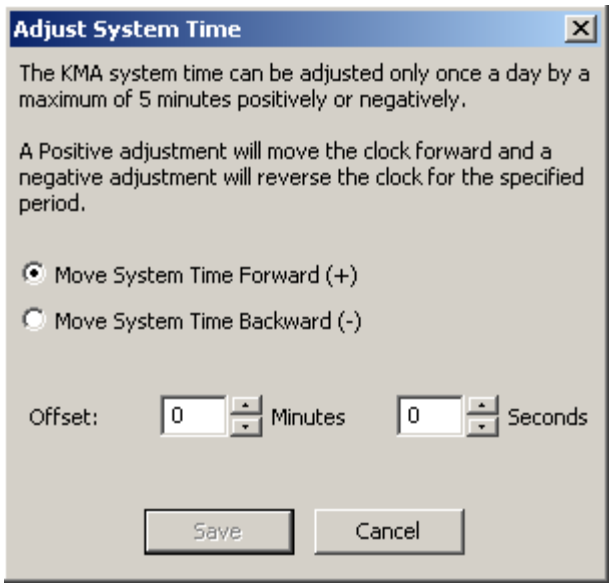
Click this button to specify the NTP server to be used by this KMA.

Adjusting the KMA's Local Clock

You can only adjust a KMA's clock once a day by a maximum of plus or minus 5 minutes. A positive (+) adjustment slowly moves the clock forward, whereas a negative (-) slowly moves the clock backward.

To adjust the KMA's local time:

1. From the System Time menu, click the Adjust Time button. The Adjust System Time dialog box is displayed.



2. Select the "Move System Time Forward (+)" radio button if you want to apply a positive adjustment to the clock. Otherwise, select the "Move System Time Backward (-)" radio button if you want to apply a negative adjustment to the clock.
3. In the Offset Minutes text box, select a numeric value.
4. In the Offset Seconds text box, select a numeric value.

Note – If the specified offset is too large, an Error message is displayed, prompting you to type a smaller value. Click the OK button to close this dialog box and type a new value.

---

5. Click the Save button to accept the changes. The System clock is adjusted.

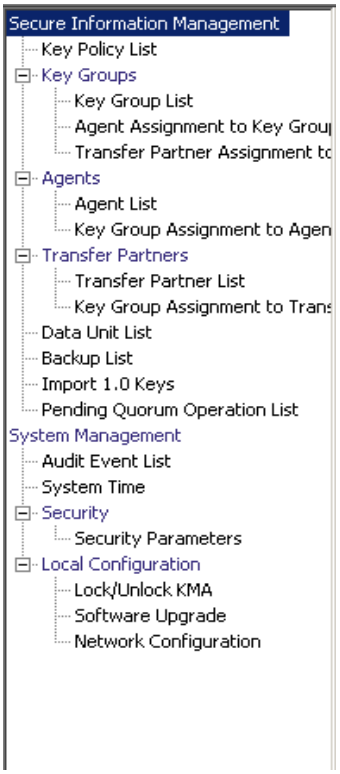
CHAPTER 6

Compliance Officer Operations

This chapter describes the operations that a user who has been given a Compliance Officer role can perform. If you have been assigned multiple roles, refer to the appropriate chapter for instructions on performing the specific role.

Compliance Officer Role

The Compliance Officer manages the flow of data through your organization and has the ability to define and deploy data contexts (Key Groups) and rules that determine how data is protected and ultimately destroyed (Key Policies). The menus that provide these functions are shown below.



Key Policies

Key Policies provide guidance for managing data. The OKM Manager uses Key Policies to determine how data is protected and destroyed. Key Policies must be created before keys can be created and delivered to agents.

Only a Compliance Officer can create and modify Key Policies. This ensures that the data complies with a policy throughout the data's lifetime.

Key Policy List Menu

The Key Policies List menu allows you to manage the Key Policies in your organizations.

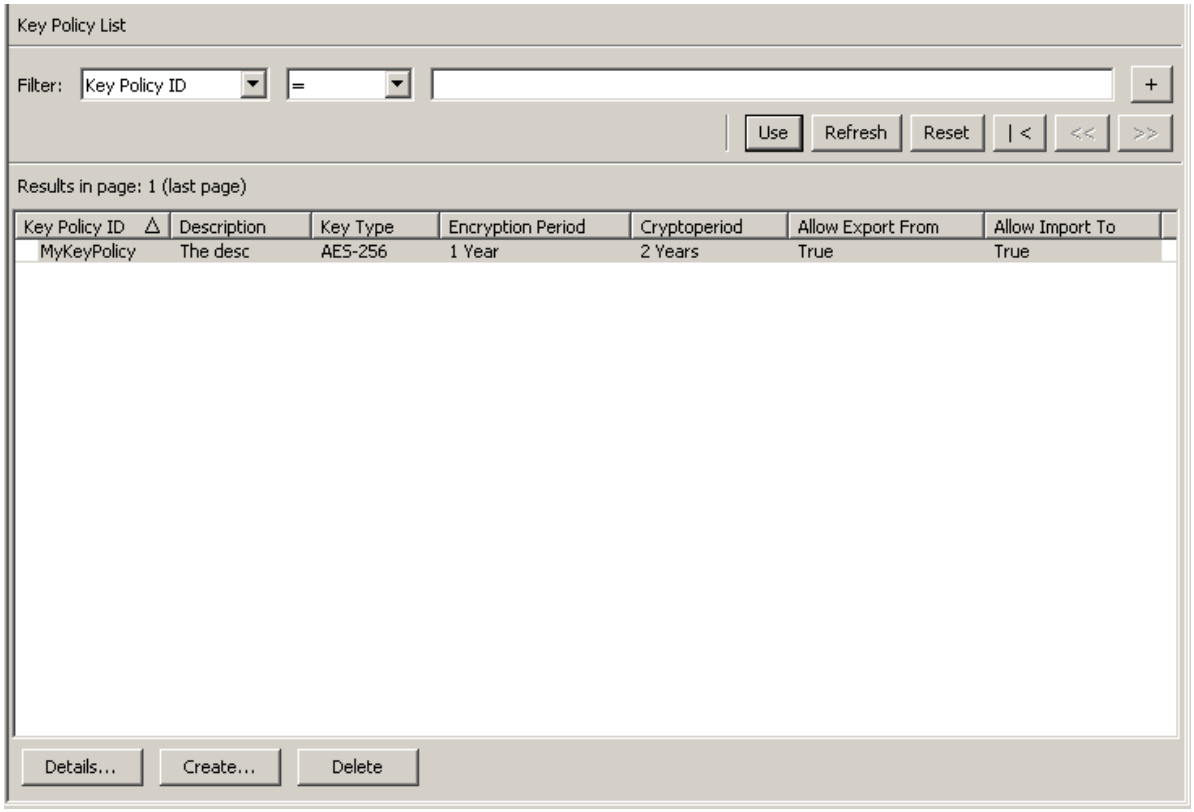
The Key Policy List menu option gives you the ability to:

- View Key Policies
- View/Modify a Key Policy's Details
- Create a Key Policy
- Delete existing Key Policies.

Viewing Key Policies

To view Key Policies:

1. From the Secure Information Management menu, select **Key Policy List**. The Key Policy List screen is displayed.



You can also scroll through the database and filter the Key Policy list by any of the following keys:

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

The **Use** button applies the filter to the displayed list for the Key Policy.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

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

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value text box:

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Click this button to add additional filters.

Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

Use:

Click this button to apply the selected filters to the displayed list and go to the first page.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Key Policy ID

Displays the unique identifier that distinguishes each Key Policy. This value can be between 1 and 64 (inclusive) characters. Key Policy IDs cannot be changed once they are created.

Description

Describes the Key Policy. This value can be between 1 and 64 (inclusive) characters.

Key Type

Indicates the type of encryption algorithm that Keys associated with this Key Policy use. Possible values are: AES-256.

Note – Encryption Period and Cryptoperiod begin when the key is first given to an Agent. Encryption period and Cryptoperiod cannot be changed for a policy. This is to avoid a change in the Key Policy from affecting large numbers of keys.

Encryption Period

Displays how long keys associated with this Key Policy can be used to encrypt or decrypt data. The time interval units are: minutes, hours, days, week, months, or years.

Cryptoperiod

Displays how long keys associated with this Key Policy can be used to decrypt (but not encrypt) data. The time interval units are: minutes, hours, days, week, months, or years.

Allow Export From

Indicates whether Data Unit keys associated with this Key Policy can be exported. Possible values are True or False.

Allow Import To

Indicates whether Data Unit keys associated with this Key Policy can be imported. Possible values are True or False.

If you want to create a Key Policy, click the Create button. For more information, refer to "Creating a Key Policy" on page 218.

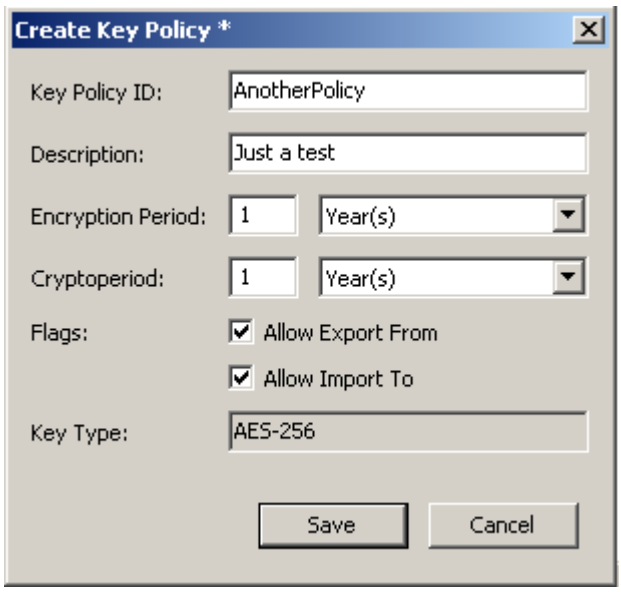
If you want to view / modify a Key Policy, highlight the Key Policy and click the Details button. For more information, refer to "Viewing/Modifying a Key Policy" on page 220.

If you want to delete a Key Policy, click the Delete button. For more information, refer to "Deleting a Key Policy" on page 221.

Creating a Key Policy

To create a Key Policy:

1. From the Key Policy List screen, click the Create button. The Create Key Policy dialog box is displayed.



2. Complete the following parameters:

Key Policy ID

Type a value that identifies the policy. This value can be between 1 and 64 (inclusive) characters.

Description

Type a value that describes the policy. This value can be between 1 and 64 (inclusive) characters. This field can be blank.

Encryption Period

Displays how long keys associated with this Key Policy can be used to encrypt or decrypt data. The time interval units are: minutes, hours, days, week, months, or years.

Cryptoperiod

Displays how long keys associated with this Key Policy can be used to decrypt (but not encrypt) data. The time interval units are: minutes, hours, days, week, months, or years.

Flags

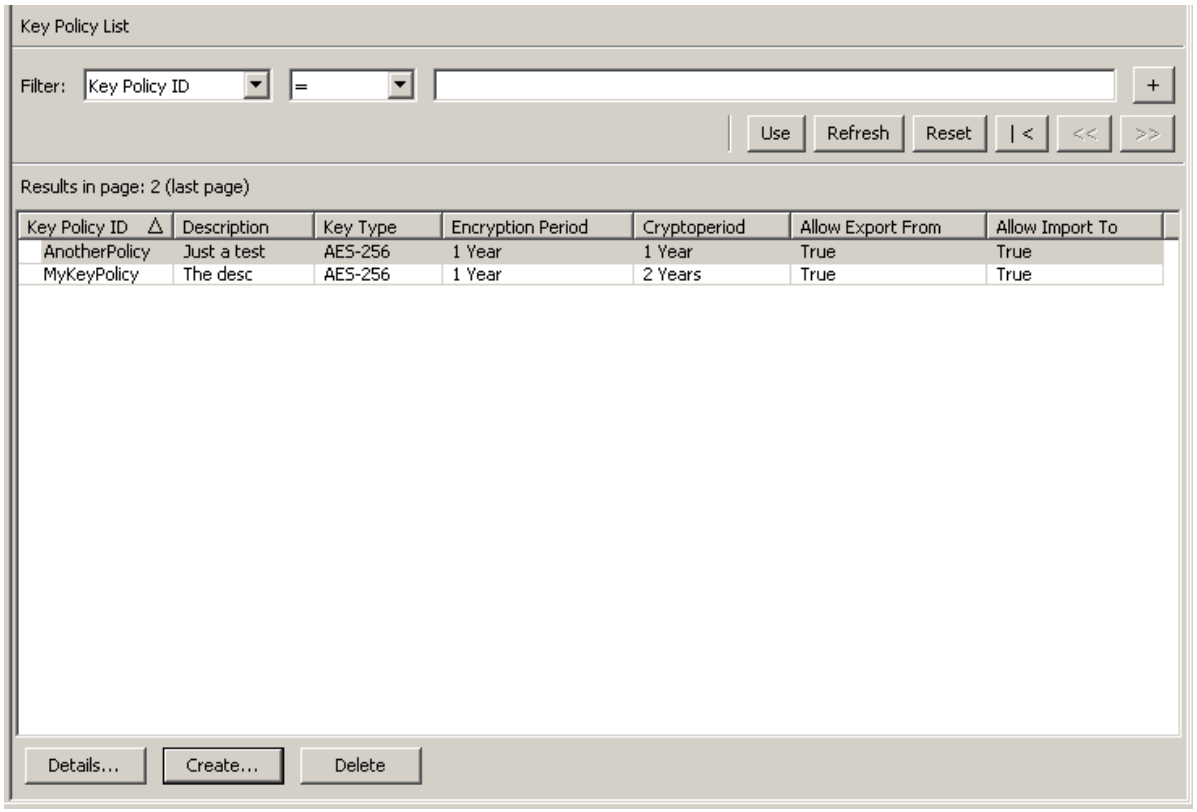
Allow Export From

Indicates whether Data Unit keys associated with this Key Policy can be exported. Possible values are True or False.

Allow Import To

Indicates whether Data Unit keys associated with this Key Policy can be imported. Possible values are True or False.

3. Click the Save button to save the Key Policy. The new Key Policy is displayed in the Key Policy List screen. It can now be used by Key Groups.

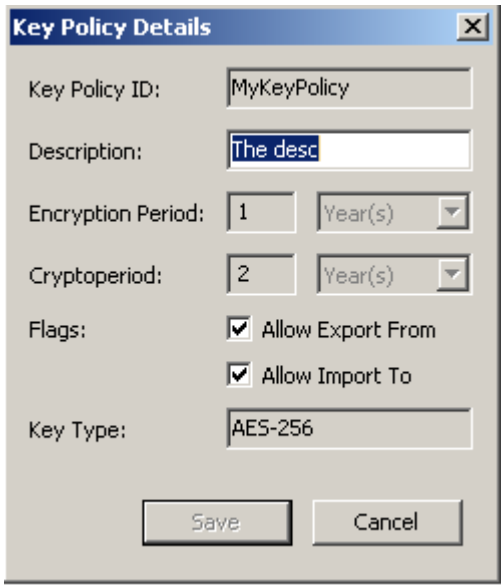


Viewing/Modifying a Key Policy

Note – Only a Compliance Officer can view a Key Policy's detailed information.

To modify a Key Policy's details:

1. From the Key Policy List screen, double-click a Key Policy for which you want more information or highlight a Key Policy and click the Details button. The Key Policy Details dialog box is displayed.



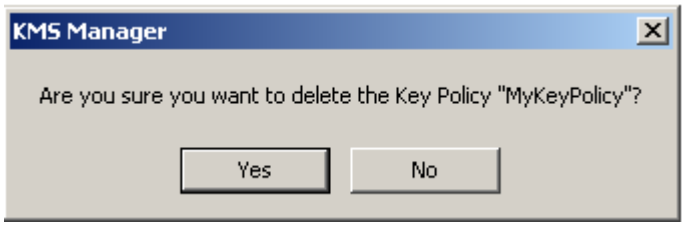
2. You can change the `Description`, `Allow Export From`, and `Allow Import To` fields, as required. When you are finished, click the Save button to save the changes. After the system verifies and validates the new Key Policy, the Key Group is associated with the new Key Policy.
3. If you click the Cancel button, your changes will not be saved and the dialog box will close.

Deleting a Key Policy

A key policy can only be deleted if it is not used by any Key Group or key.

To delete a Key Policy:

1. From the Key Policy List screen, highlight the Key Policy you want to delete and click the Delete button. The following dialog box is displayed, prompting you to confirm that you want to delete the specific Key Policy.



2. Click the Yes button to delete the Key Policy. The Key Policy is removed from the database. You are returned to the Key Policy List screen, where the Key Policy is removed from the list.

Key Groups

A Key Group represents a data context that determines the Key Policy to which it applies and the Agents that can access it. When a Key is assigned to an agent and is first used for a Data Unit, it is associated with a Key Group. When you create a Key Group, you must select a Key Policy. The selected Key Policy is applied to Keys in that Key Group.

Agents are associated with Key Groups. An Agent has one or more keys groups that it is allowed to access. An Agent can only retrieve keys belonging to Key Groups it is allowed to access. An Agent may also have a default Key Group. When an agent allocates a new key, the key is placed in the agents default Key Group. An agent can only allocate new keys if it has a default Key Group.

FIGURE 6-1 on page 223 shows the relationship between Key Groups, Key Polices, Agents, and Data Units.

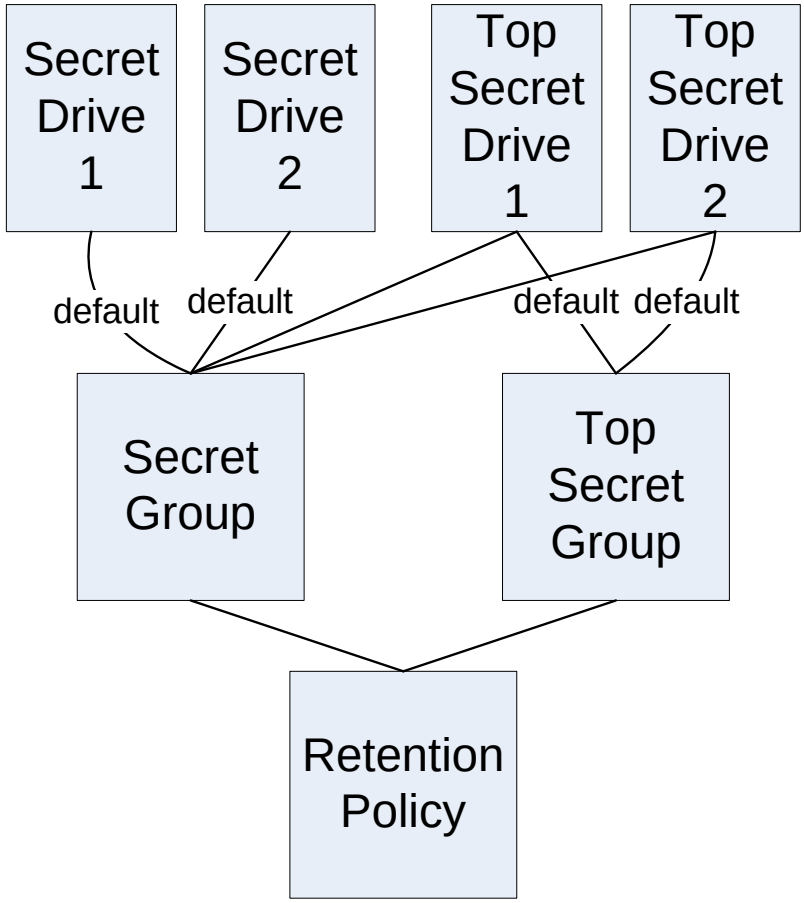
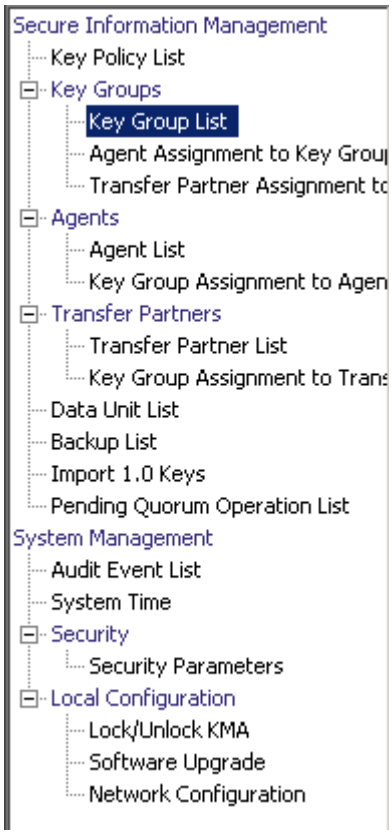


FIGURE 6-1 Key Group Relationship with Key Policies, Agents, Data Units

Key Groups Menu

The Key Groups menu includes the Key Group List menu option, which allows the Compliance Officer to manage Key Groups.



Key Group List Menu

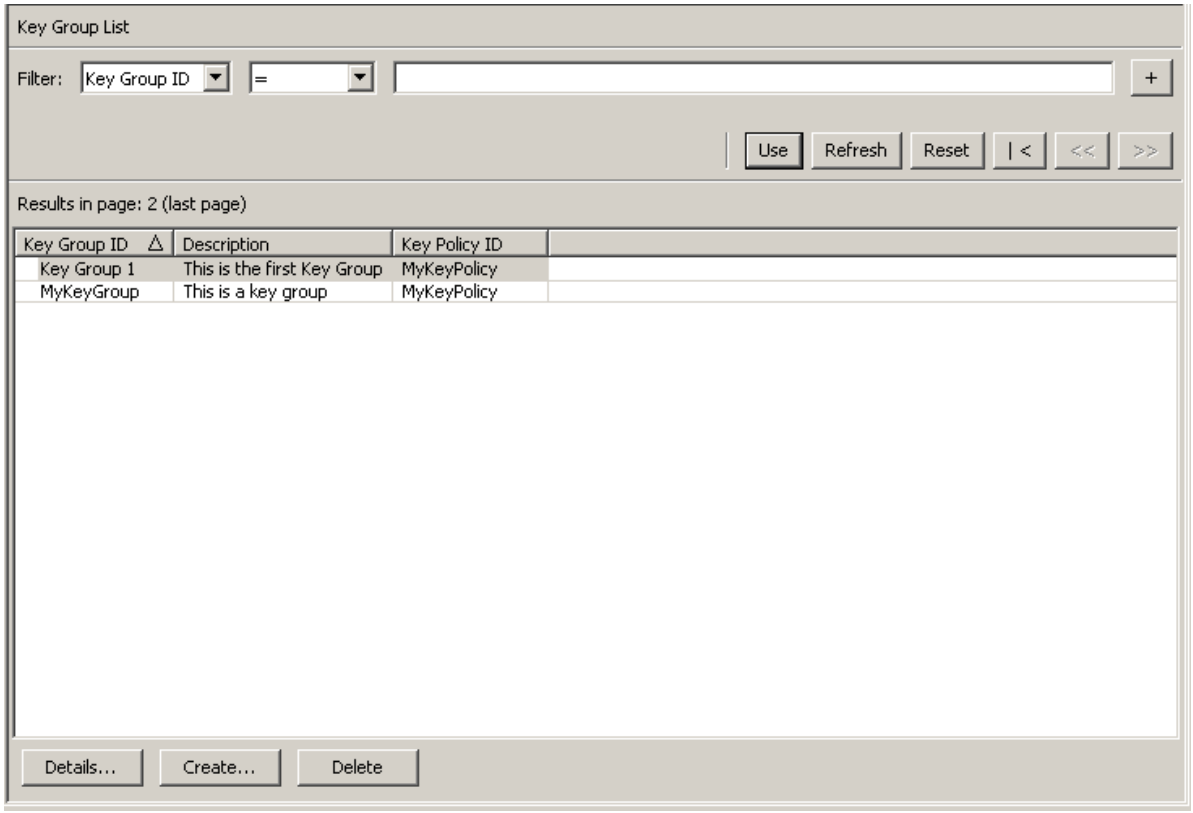
The Key Group List menu option gives you the ability to:

- View Key Groups
- Create a Key Group
- Modify existing Key Groups
- Delete existing Key Groups.

Viewing Key Groups

To view all Key Groups:

1. From the Key Groups menu, select **Key Group List**. The Key Group List screen is displayed.



You can scroll through the database and filter through the Key Group list by any of the following keys:

- Key Group ID
- Description
- Key Policy ID.

The Use button applies the filter to the displayed list for the Key Group.

The fields and their descriptions are given below:

Filter:

Select filter options to filter the displayed list of Key Groups. Only Key Groups that satisfy all filters will be displayed.

Filter Attribute combo box:

Click the down-arrow and select an attribute to filter by. Possible values are:

- Key Group ID
- Description
- Key Policy ID.

Filter Operator box:

Click the down-arrow and select the filter operation to apply to the selected attribute. Possible values are:

- Equals =
- Not equal <>;
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty.

Filter Value text box:

Type a value to filter the selected attribute by.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Click this button to add additional filters.

Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

Use:

Click this button to apply the selected filters to the displayed list and go to the first page.

Refresh:

Click this button to refresh the displayed list. This does not apply filters selected since the last Use or Reset, and does not change the page of the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of items that can be displayed on the current page. Appends "(last page)" to the number of items if you are at the end of the list. The maximum number of items displayed on a page is defined by the Query Page Size value on the Options dialog.

Key Group ID

Displays the unique identifier that distinguishes each Key Group. This value can be between 1 and 64 (inclusive) characters. The Key Group ID cannot be changed once it is defined.

Description

Describes the Key Group. This value can be between 1 and 64 (inclusive) characters.

Key Policy ID

Displays a unique identifier for an existing Key Policy that applies for every Data Unit in the Key Group.

The Key Policy ID for an existing Key Group cannot be changed. This is to avoid a change affecting a large number of keys.

If you want to create a Key Group, click the Create button. For more information, refer to "Creating a Key Group" on page 228.

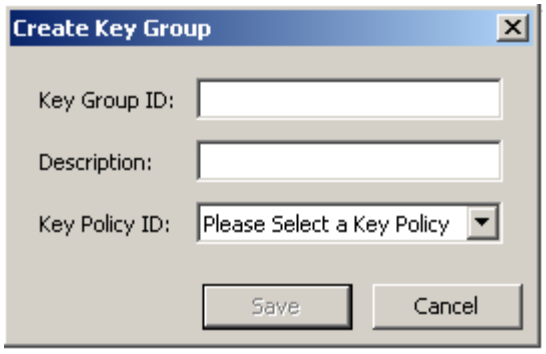
If you want to view/modify a Key Group, highlight the Key Group and click the Details button. For more information, refer to "Viewing/Modifying a Key Group's Details" on page 230.

If you want to delete a Key Group, click the Delete button. For more information, refer to "Deleting a Key Group" on page 231.

Creating a Key Group

To create a new Key Group:

1. From the Key Group List screen, click the Create button. The Create Key Group dialog box is displayed.



2. Complete the following parameters:

Key Group ID

Type a value that identifies the Key Group. This value can be between 1 and 64 (inclusive) characters.

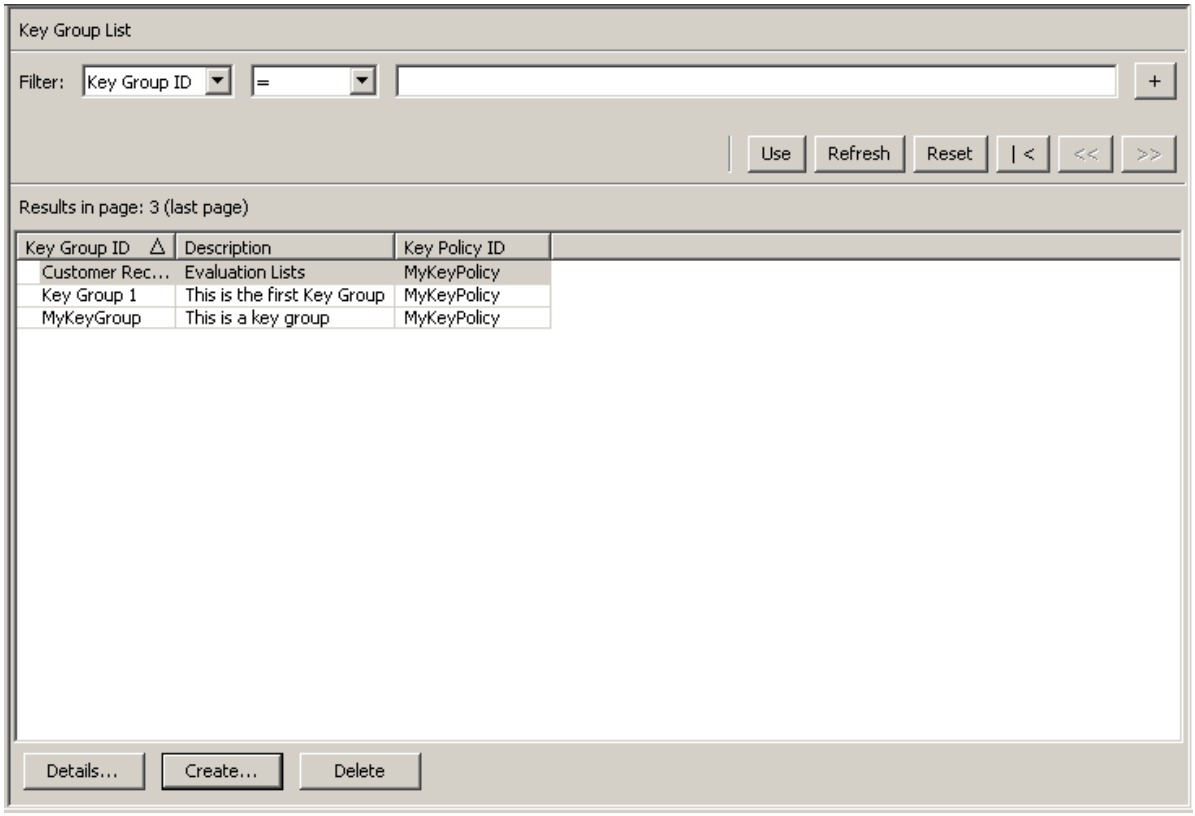
Description

Type a value that describes the Key Group. This value can be between 1 and 64 (inclusive) characters.

Key Policy ID

Click the down-arrow and select the Key Policy with which you want to associate this Key Group. When creating a new Key Group, existing Key Policies are displayed.

3. Click the Save button. The new Key Group is created and saved in the database and is displayed in the Key Group List screen. It can now be used by Data Units, Agents, etc.

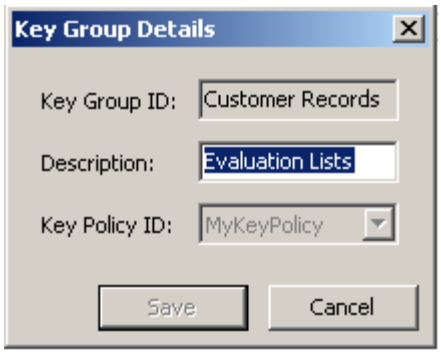

Key Group List
Filter:
Key Group ID
=
+
Use
Refresh
Reset
| <
<<
>>
Results in page: 3 (last page)
Key Group ID
Description
Key Policy ID
Customer Rec...
Evaluation Lists
MyKeyPolicy
Key Group 1
This is the first Key Group
MyKeyPolicy
MyKeyGroup
This is a key group
MyKeyPolicy
Details...
Create...
Delete

Viewing/Modifying a Key Group's Details

Note – If you are not a Compliance Officer, when you view a Key Group's detailed information, all fields, including the Save button are disabled.

To modify a Key Group:

1. From the Key Group List screen, double-click a Key Group entry for which you want more information or highlight a Key Group entry and click the Details button. The Key Group Details dialog box is displayed.



The following parameters are displayed:

Key Group ID:

Uniquely identifies the Key Group. This field is read-only.

Description:

Type a value that describes the Key Group. This value can be between 1 and 64 (inclusive) characters. This field can be blank.

Key Policy ID:

Displays a unique identifier for an existing Key Policy that is associated with the Key Group and all the Keys in the Key Group. This field is read-only.

2. The Description field is the only field that can be modified. When you are finished, click the Save button to save the changes. You are returned to the Key Group List screen.

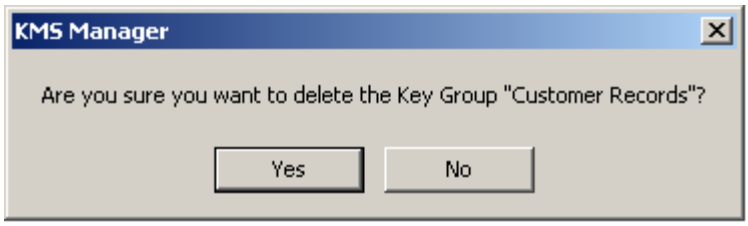
Deleting a Key Group

Note – You cannot delete a Key Group if it is active, that is, to which Agents or Data Units are assigned.

To delete a Key Group:

1. From the Key Groups List screen, highlight the Key Group you want to delete and click the Delete button.The following Confirmation dialog box is displayed, prompting you to confirm that you want to delete the selected Key Group.

   A Key Group can only be deleted if it is not used by any key and is not associated with any Agent.

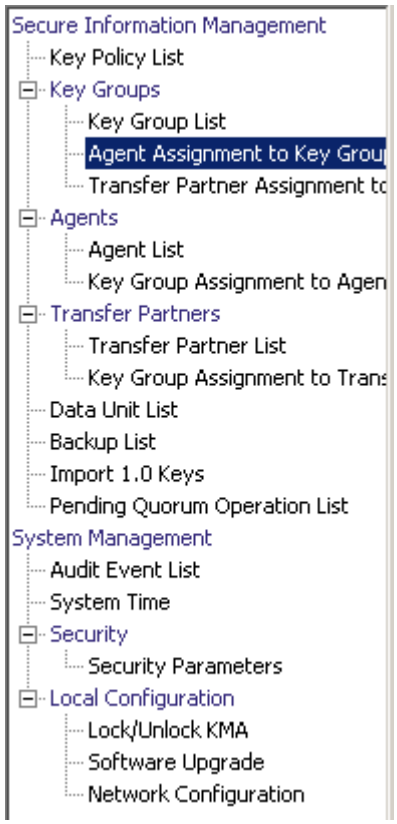


2. Click the Yes button to delete the Key Group. The Key Group and its associated entries are deleted from the database. You are returned to the Key Groups List screen, where the Key Group is no longer listed.

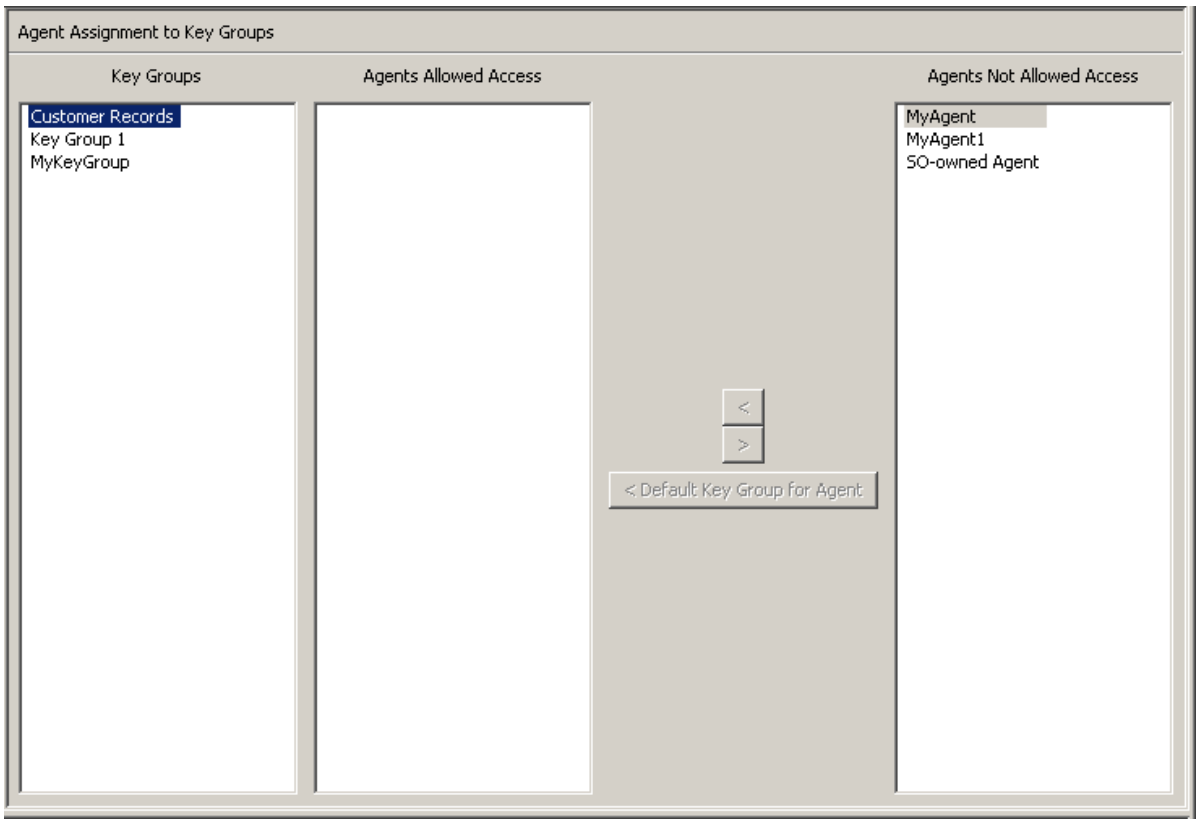
Agent Assignment to Key Groups Menu

The Agent Assignment to Key Groups menu option gives you the ability to assign Agents to Key Groups. When you assign Agents to Key Groups, it determines the storage devices that the Agent can access. It is the converse of the Key Group Assignment menu option under the Agents menu, both accomplishing the same result.

Important – You must set a default Key Group for an Agent before that Agent can allocate keys.



To view Agents assignments, from the Key Groups menu, select Agent Assignment to Key Groups. The Agent Assignment to Key Groups screen is displayed.

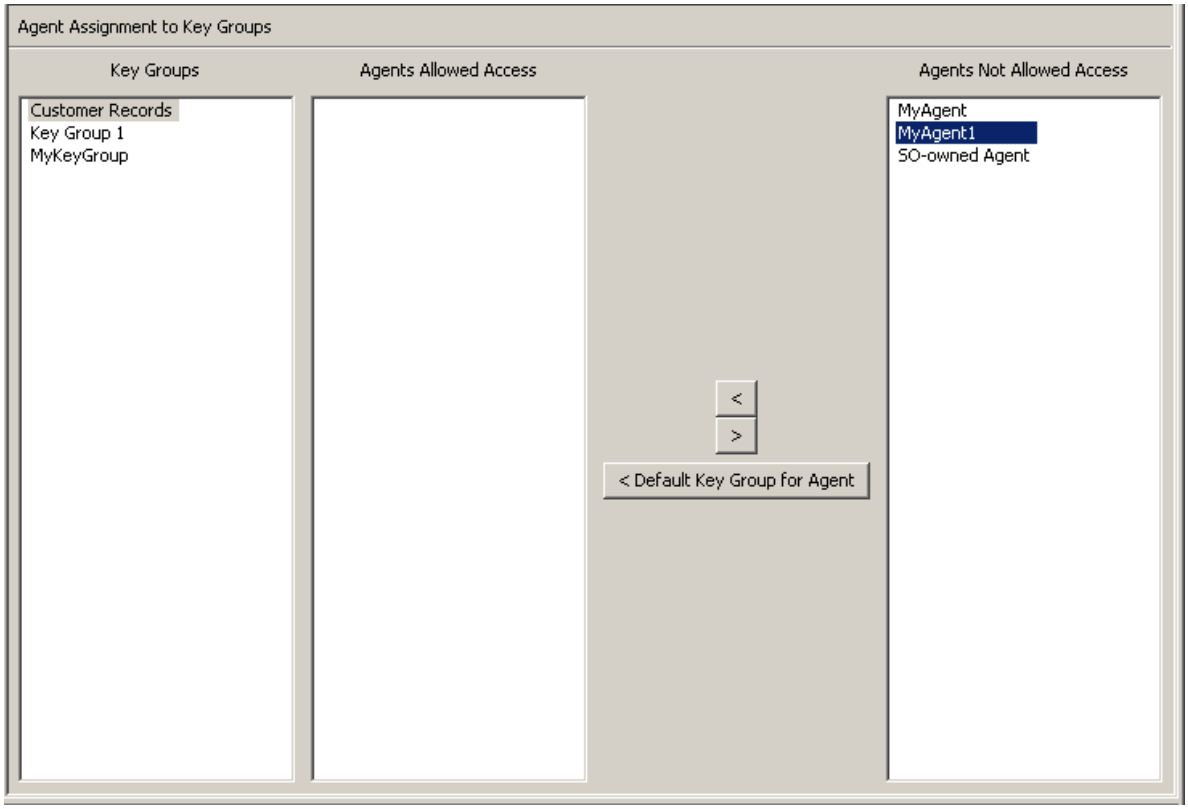


The Key Groups column lists the Key Groups. The Agents Allowed Access column lists the Agents that are assigned to the selected Key Group(s). The Agents Not Allowed Access column lists the Agents that are not assigned to the selected Key Group(s).

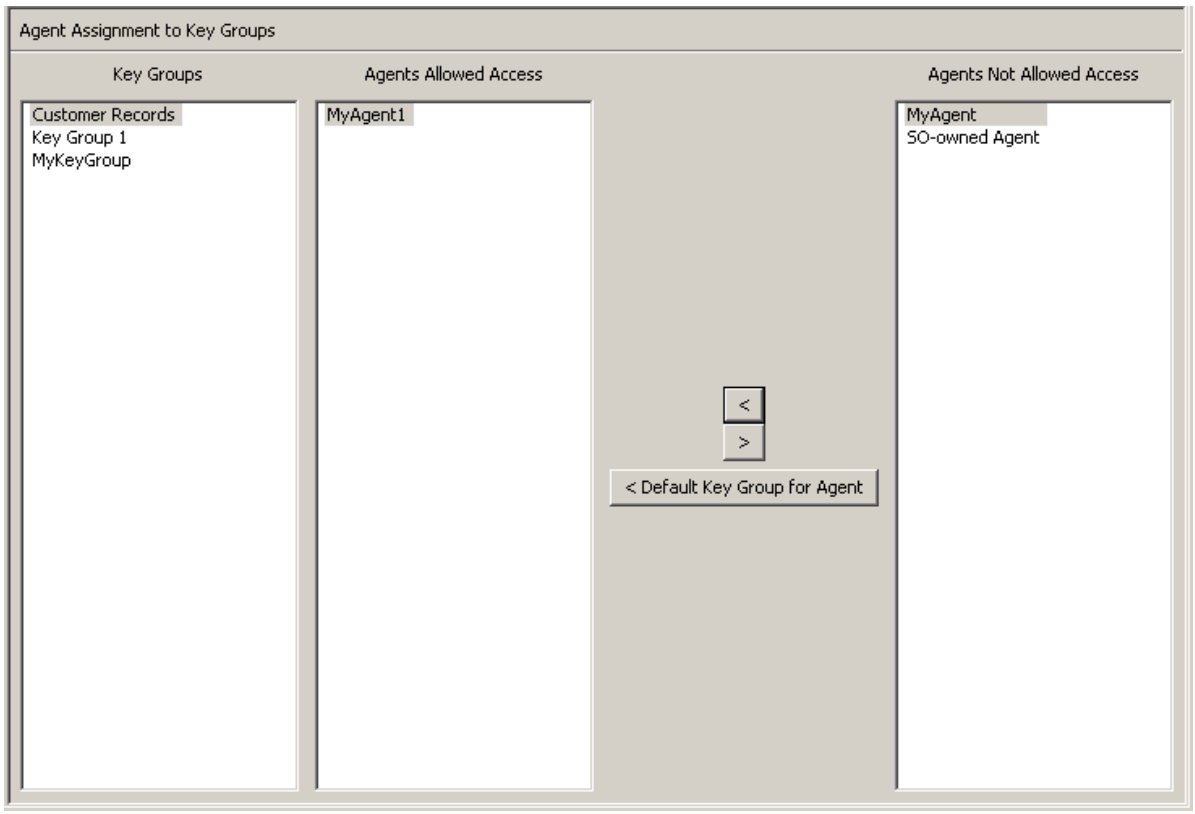
Assigning an Agent to a Key Group

To assign an Agent to a Key Group:

1. In the Key Groups column, highlight the Key Group you want. In the Agents Not Allowed Access column, highlight the Agent you want to add and click the Move to < button.



2. The selected Agent is moved to the Agents Allowed Access column, indicating that the Agent is successfully added to the selected Key Group's Agent list.



To assign Agents to a Key Group and set the Default Key Group:

1. From the Agent Assignment to Key Groups screen, select the Key Group you want in the Key Groups list.
2. In the Agents Not Allowed Access list, select one or more Agents you want to add and set the Default Key Group for.
3. Click the Default Key Group for Agent button. The selected Agents are moved to the Agents Allowed Access list and their Default Key Group is set to the Key Group. The Agents are now allowed access to the Key Group.

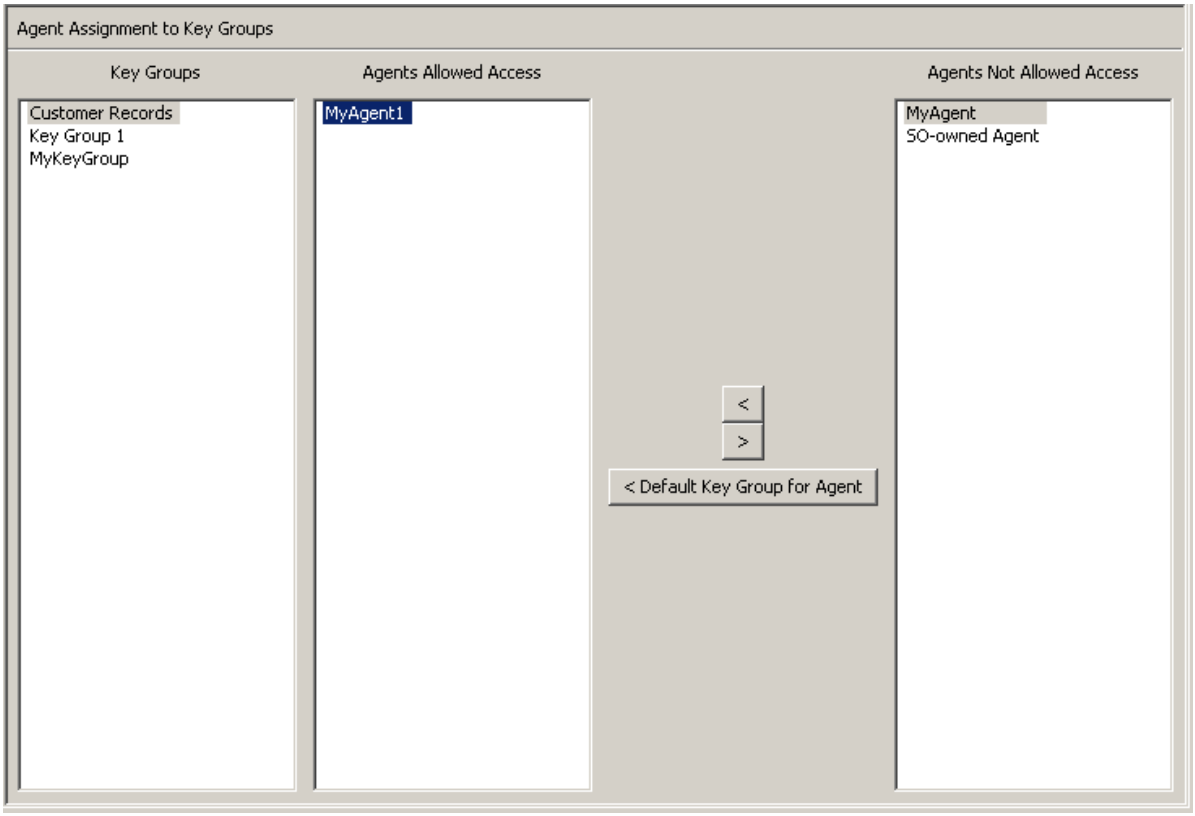
To set the Default Key Group for already assigned Agents:

1. From the Agent Assignment to Key Groups screen, select the Key Group you want in the Key Groups list.
2. In the Agents Allowed Access list, select one or more Agents that do not have the selected Key Group as their Default Key Group.
3. Click the Default Key Group for Agent button. The selected Agents' Default Key Group is set to the Key Group.

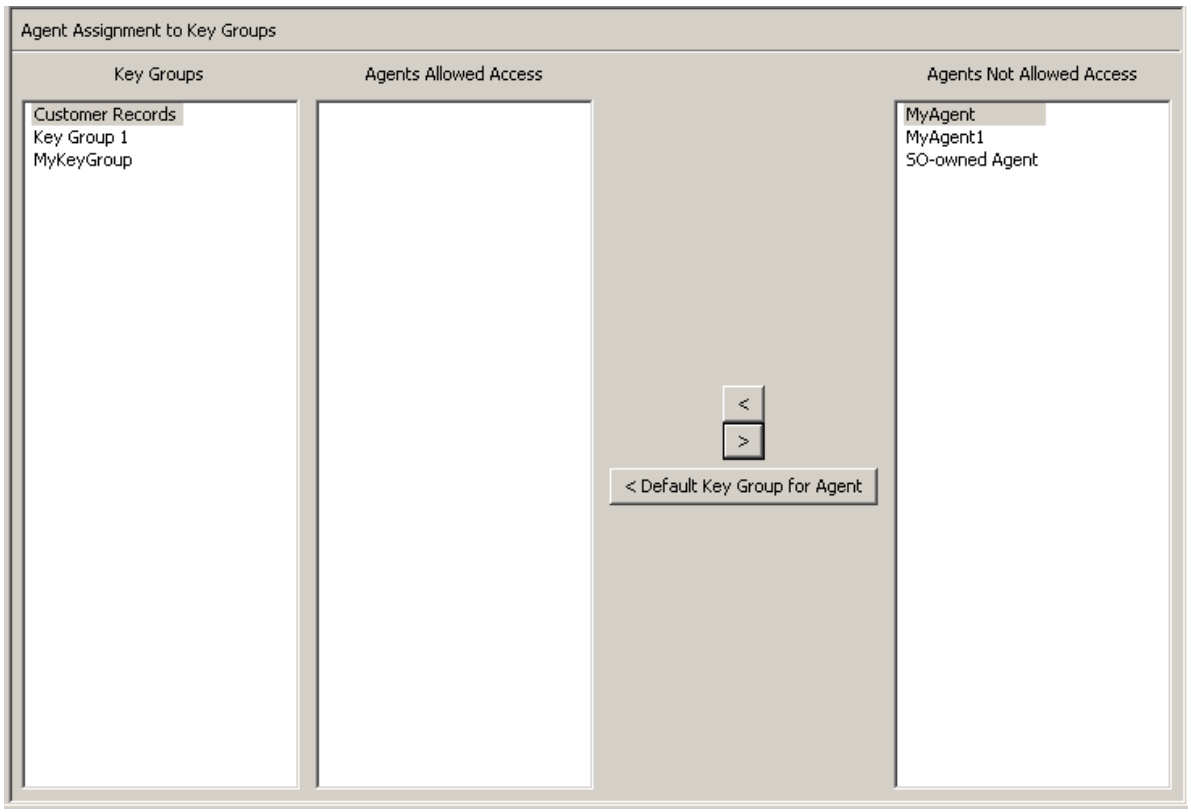
Removing an Agent from a Key Group

To remove an Agent from a Key Group's Agent list:

1. In the Key Groups column, highlight the Key Group you want. In the Agents Allowed Access column, highlight the Agent you want to remove, and click the Move from > button.

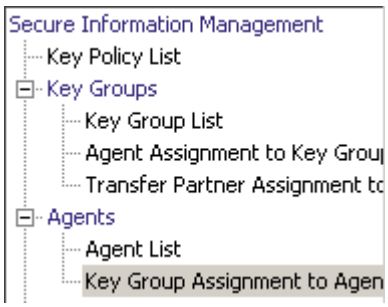


2. The selected entry is removed from the Agents Allowed Access column and is listed in the Agents Not Allowed Access column. It is no longer assigned to the selected Key Group.


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

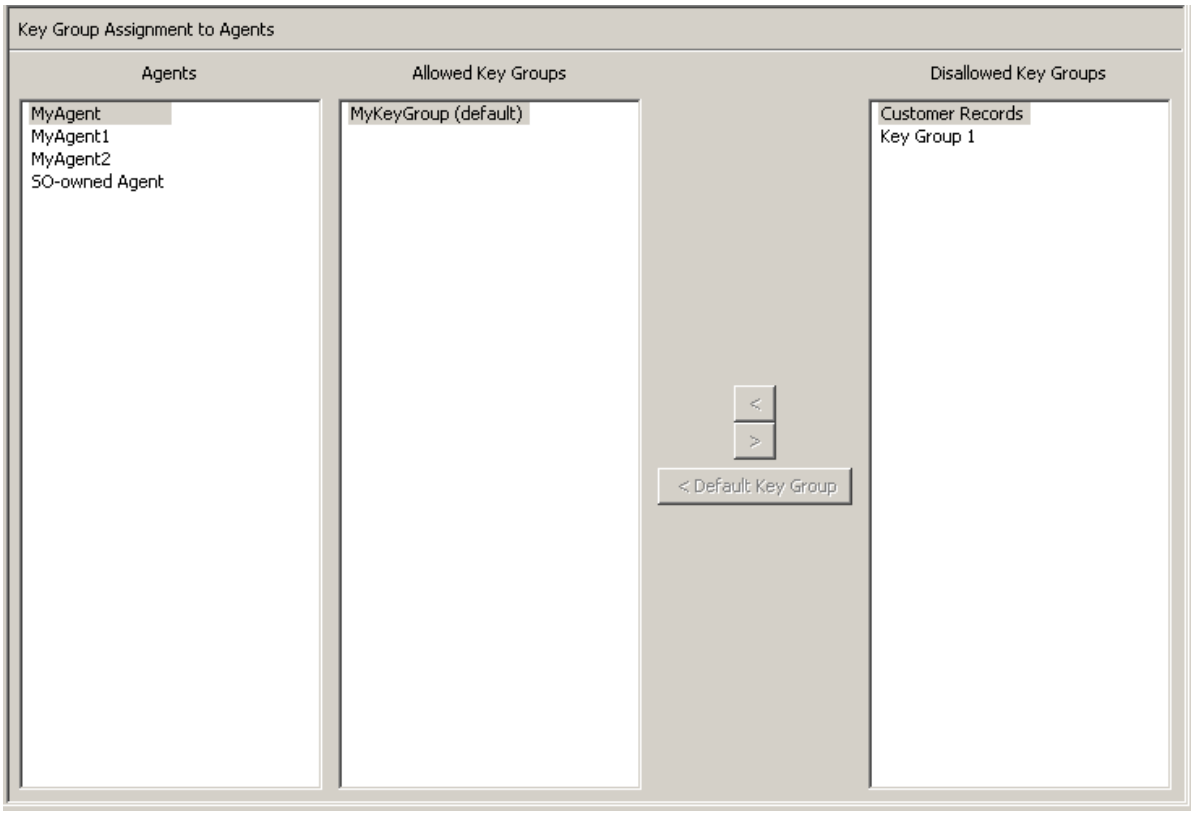
Key Group Assignment to Agents Menu

The Key Group Assignment to Agents menu option allows you to assign Key Groups to Agents. It is the converse of the Agent Assignment to Key Groups menu option, both accomplishing the same result.



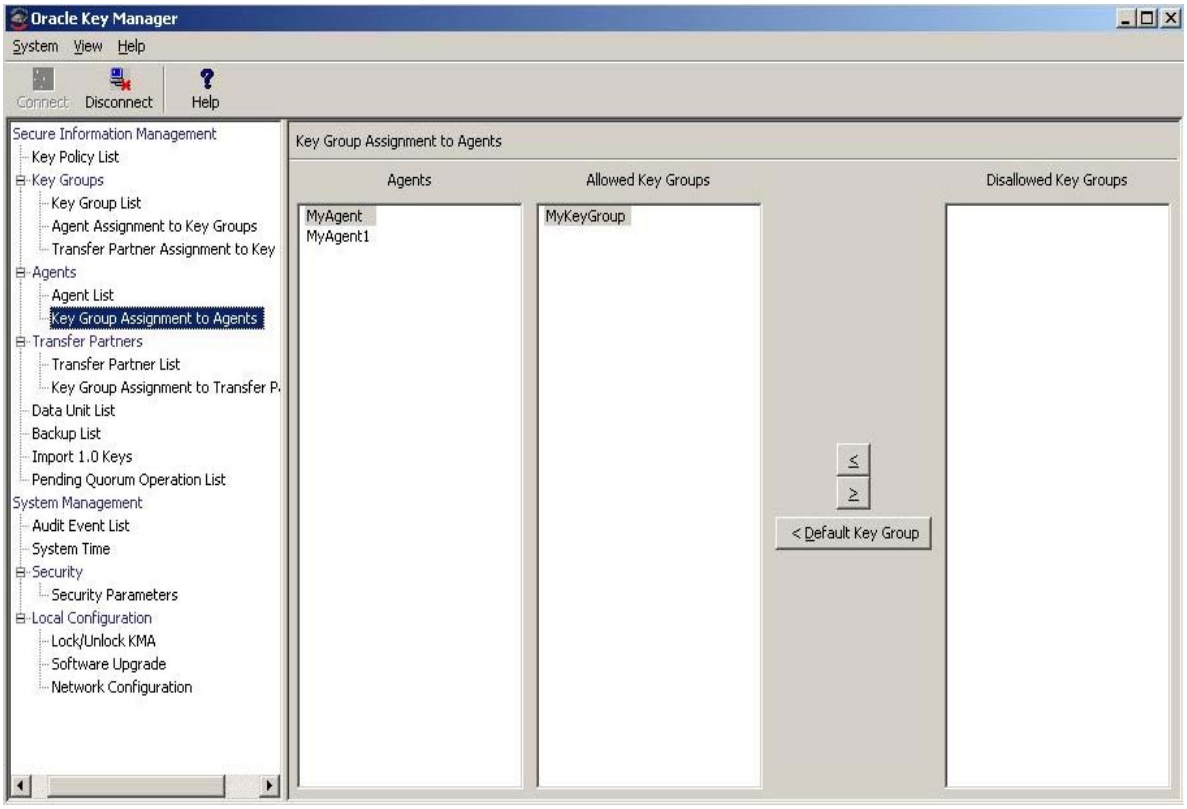
To view the Key Groups:

1. From the Agents menu, select Key Group Assignment. The Key Group Assignment to Agents screen is displayed.



The Agents column lists the Agents in the database. The Allowed Key Groups column lists the Key Groups which the Agent can access. The Disallowed Key Groups column lists the Key Groups which the Agent cannot access.

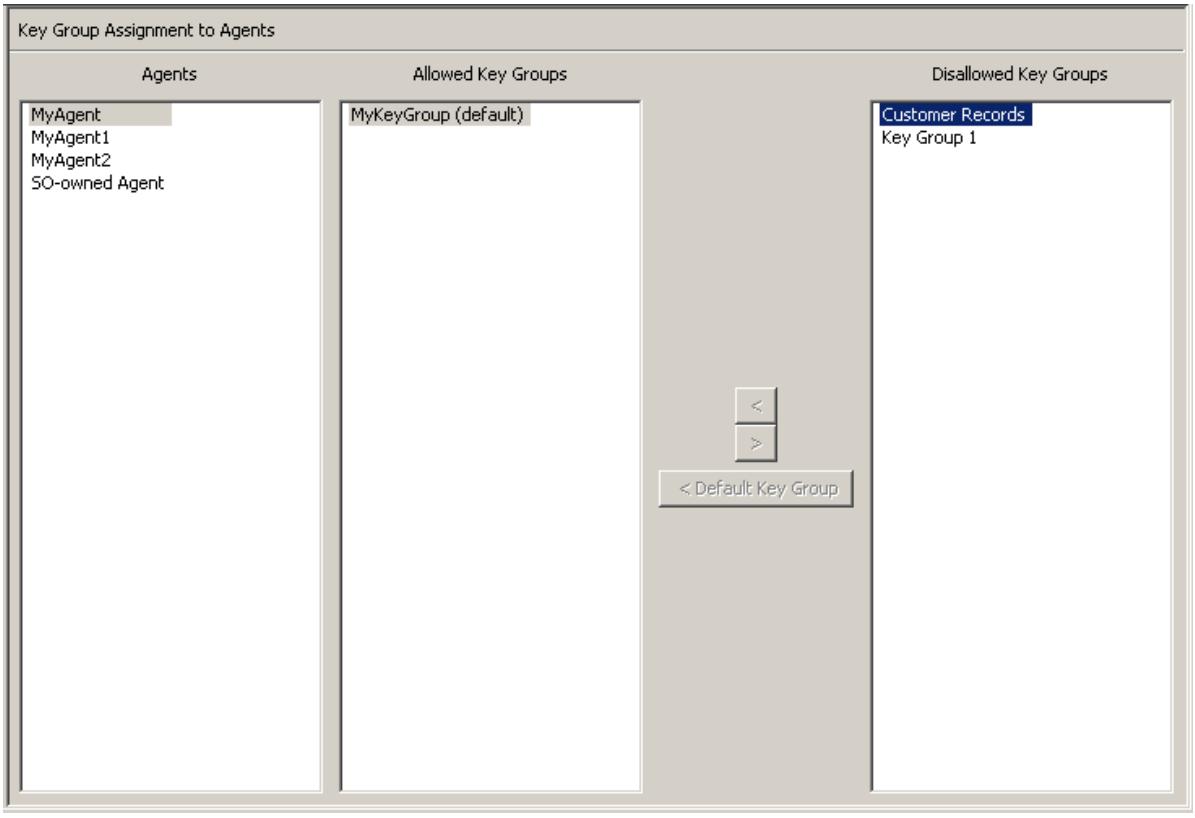
2. Clicking an Agent entry displays the Key Group that are members or non-members of the selected Agent.


Oracle Key Manager
System View Help
Connect Disconnect Help
Secure Information Management
Key Policy List
Key Groups
Key Group List
Agent Assignment to Key Groups
Transfer Partner Assignment to Key
Agents
Agent List
Key Group Assignment to Agents
Transfer Partners
Transfer Partner List
Key Group Assignment to Transfer P.
Data Unit List
Backup List
Import 1.0 Keys
Pending Quorum Operation List
System Management
Audit Event List
System Time
Security
Security Parameters
Local Configuration
Lock/Unlock KMA
Software Upgrade
Network Configuration
Key Group Assignment to Agents
Agents
Allowed Key Groups
Disallowed Key Groups
MyAgent
MyAgent1
MyKeyGroup
< Default Key Group

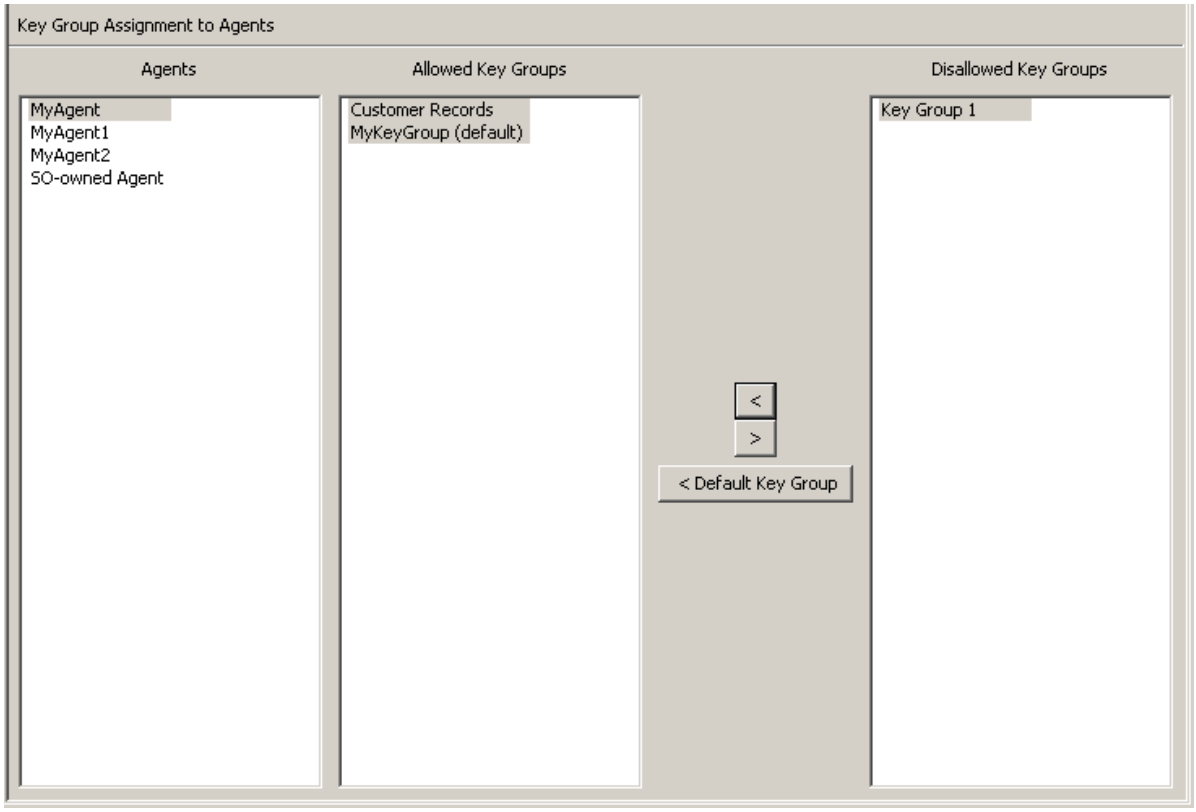
Assigning a Key Group to an Agent

To assign a Key Group to an Agent:

1. From the Key Group Assignment to Agents screen, in the Agents column, highlight the Agent you want. In the Disallowed Key Groups column, highlight the Key Group you want to add and click the Move to < button.



2. The selected entry is moved to the Allowed Key Groups column and the Key Group is successfully added to the selected Agent.



To assign a Key Group to an Agent as the Default Key Group:

1. From the Key Group Assignment to Agents screen, select the Agent you want in the Agents list.
2. In the Disallowed Key Groups list, select one Key Group you want to add and set the Default Key Group for.
3. Click the Default Key Group button. The selected Key Group is moved to the Allowed Key Groups list and is set as the Default Key Group for the Agent. The Agent is now allowed access to the Key Group.

To set an already assigned Key Group to the Default Key Group:

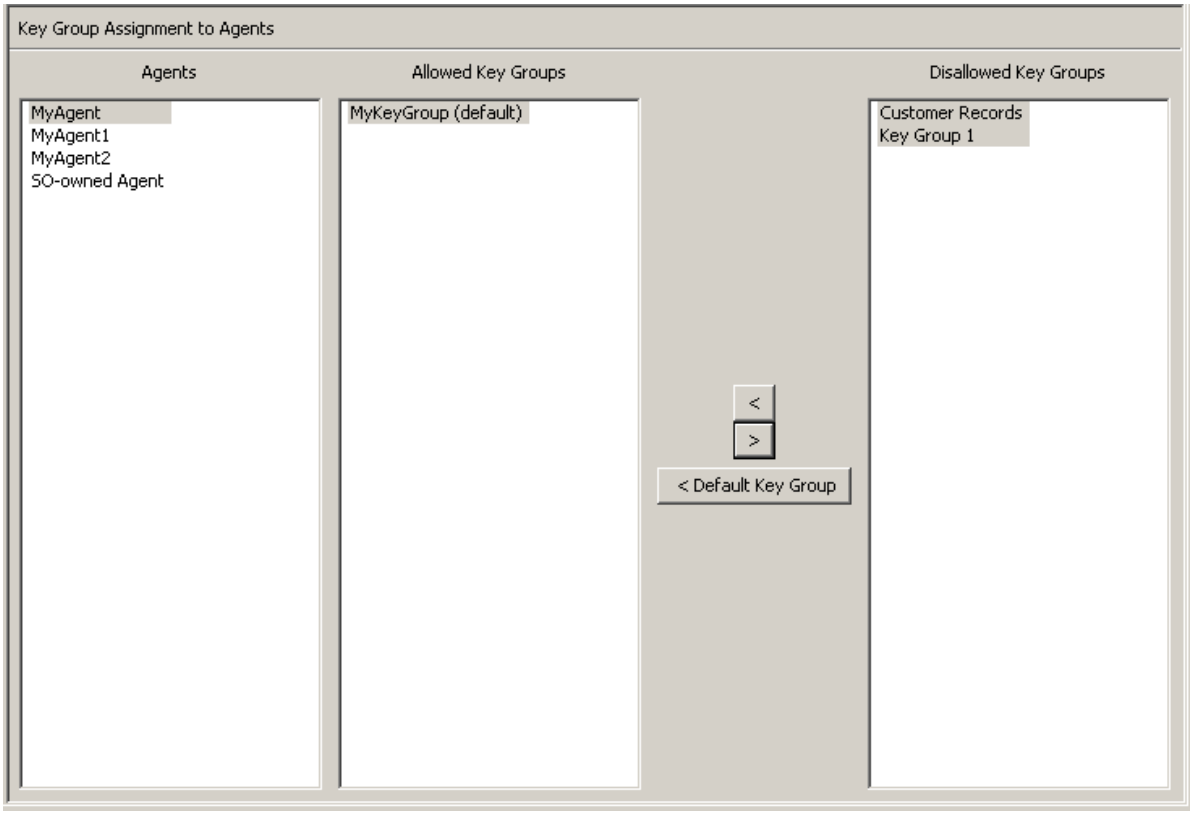
1. From the Key Group Assignment to Agents screen, select the Agent you want in the Agents list.
2. In the Allowed Key Groups list, select one Key Group that is not the Default Key Group for the Agent.

Click the Default Key Group button. The Agent's Default Key Group is set to the selected Key Group.

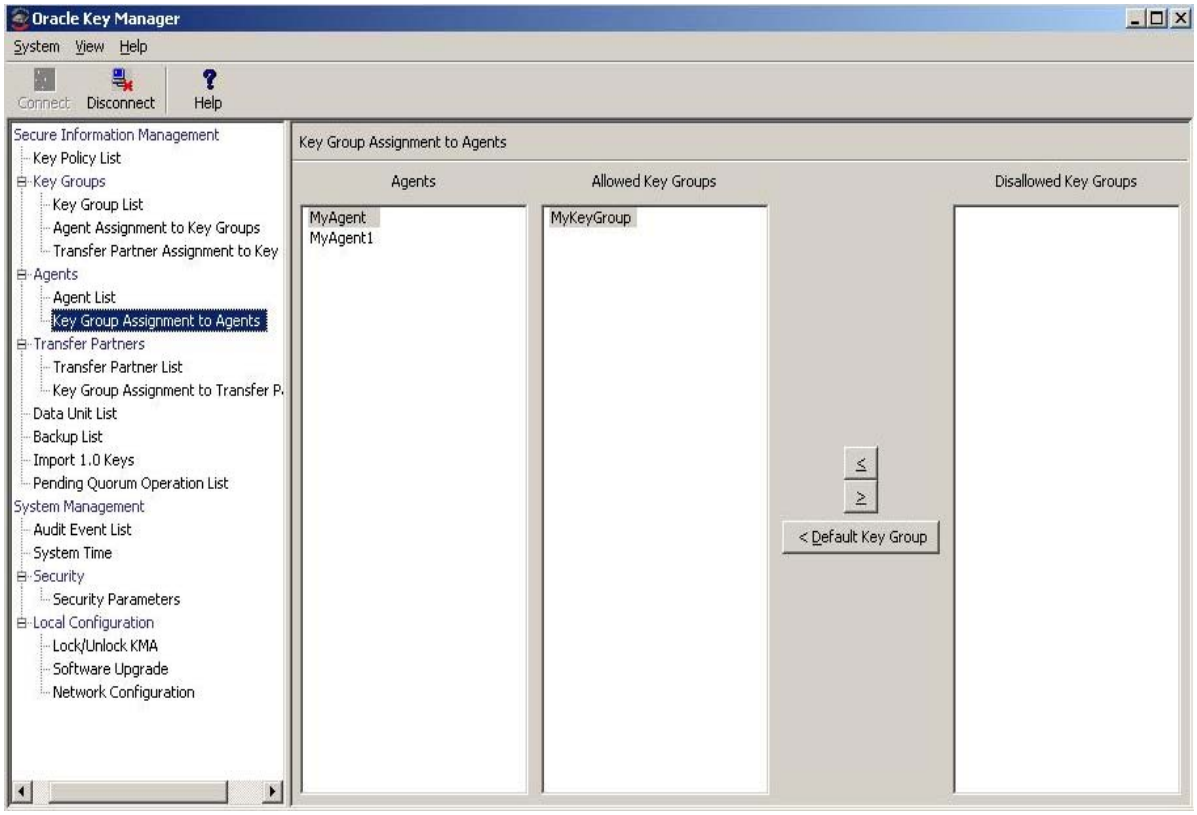
Removing a Key Group from an Agent

To remove a Key Group to an Agent:

1. From the Key Group Assignment to Agents screen, in the Agents column, highlight the Agent you want. In the Allowed Key Groups column, highlight the Key Group you want to remove and click the Move from > button.

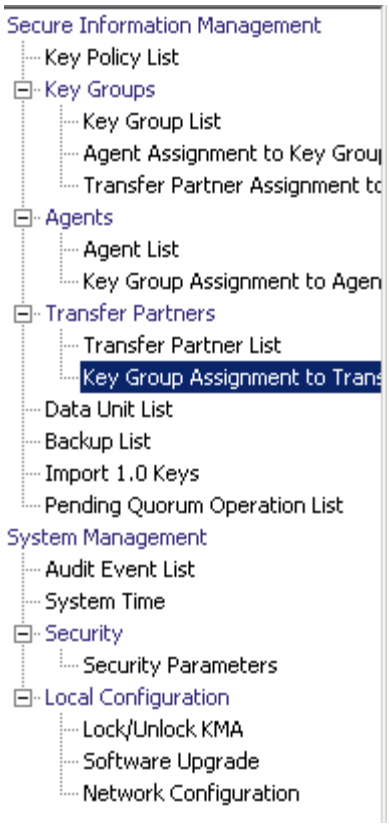


2. The selected entry is removed from the Allowed Key Groups column to the Non-member of Info. Groups column and is no longer assigned to the Agent.


Oracle Key Manager
System View Help
Connect Disconnect Help
Secure Information Management
Key Policy List
Key Groups
Key Group List
Agent Assignment to Key Groups
Transfer Partner Assignment to Key
Agents
Agent List
Key Group Assignment to Agents
Transfer Partners
Transfer Partner List
Key Group Assignment to Transfer P
Data Unit List
Backup List
Import 1.0 Keys
Pending Quorum Operation List
System Management
Audit Event List
System Time
Security
Security Parameters
Local Configuration
Lock/Unlock KMA
Software Upgrade
Network Configuration
Key Group Assignment to Agents
Agents
Allowed Key Groups
Disallowed Key Groups
MyAgent
MyAgent1
MyKeyGroup
≤
≥
< Default Key Group

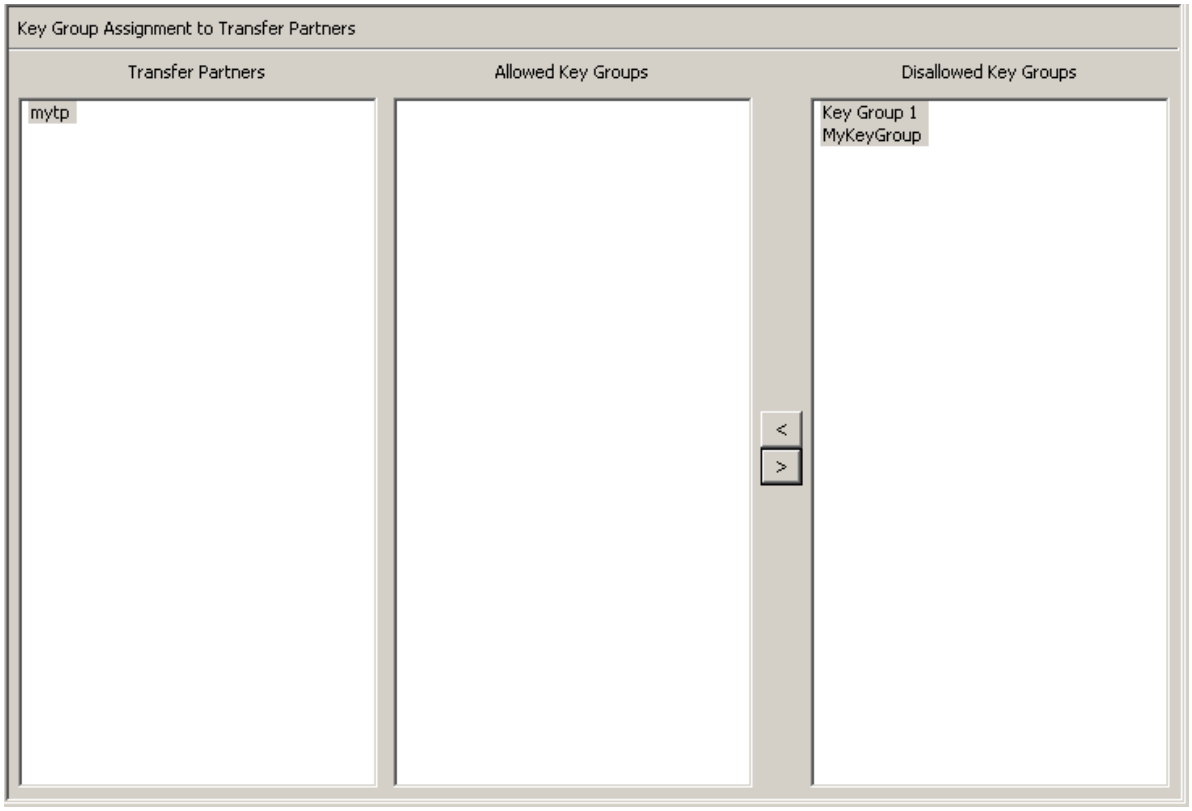
Key Group Assignment to Transfer Partners Menu

The Key Group Assignment to Transfer Partners menu option allows you to assign Key Groups to Transfer Partners.



Viewing Key Group Assignments

To view Key Group assignments, from the Transfer Partners menu, select Key Group Assignment to Transfer Partners. The following screen is displayed.

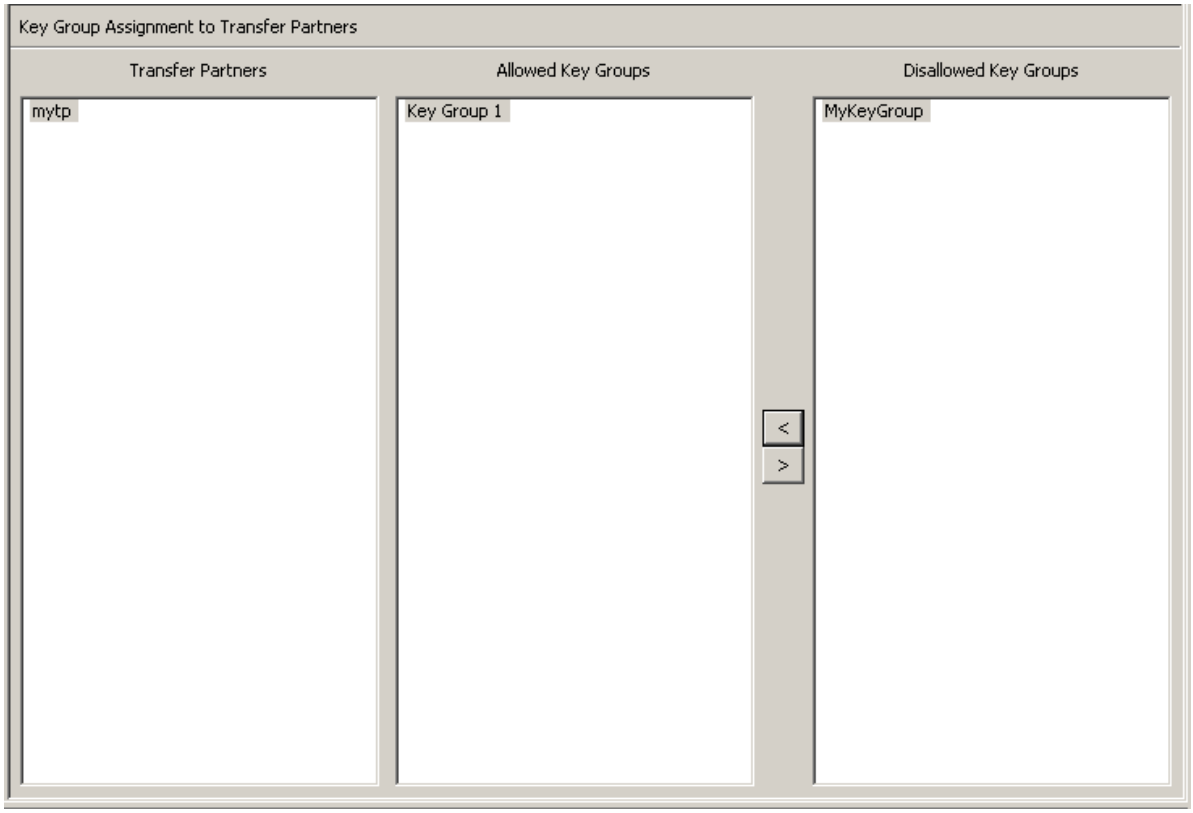


The screen shows the Key Groups that can access a Transfer Partner. The Allowed Key Groups column lists the Key Groups assigned to the selected Transfer Partner. The Disallowed Key Groups column displays the Key Groups not assigned to the Transfer Partner.

Adding a Key Group to a Transfer Partner

To add a Key Group to a Transfer Partner list:

1. In the Transfer Partners column, highlight the Transfer Partner you want to affect. In the Disallowed Key Groups column, highlight the Key Group you want to add and click the Move to < button.

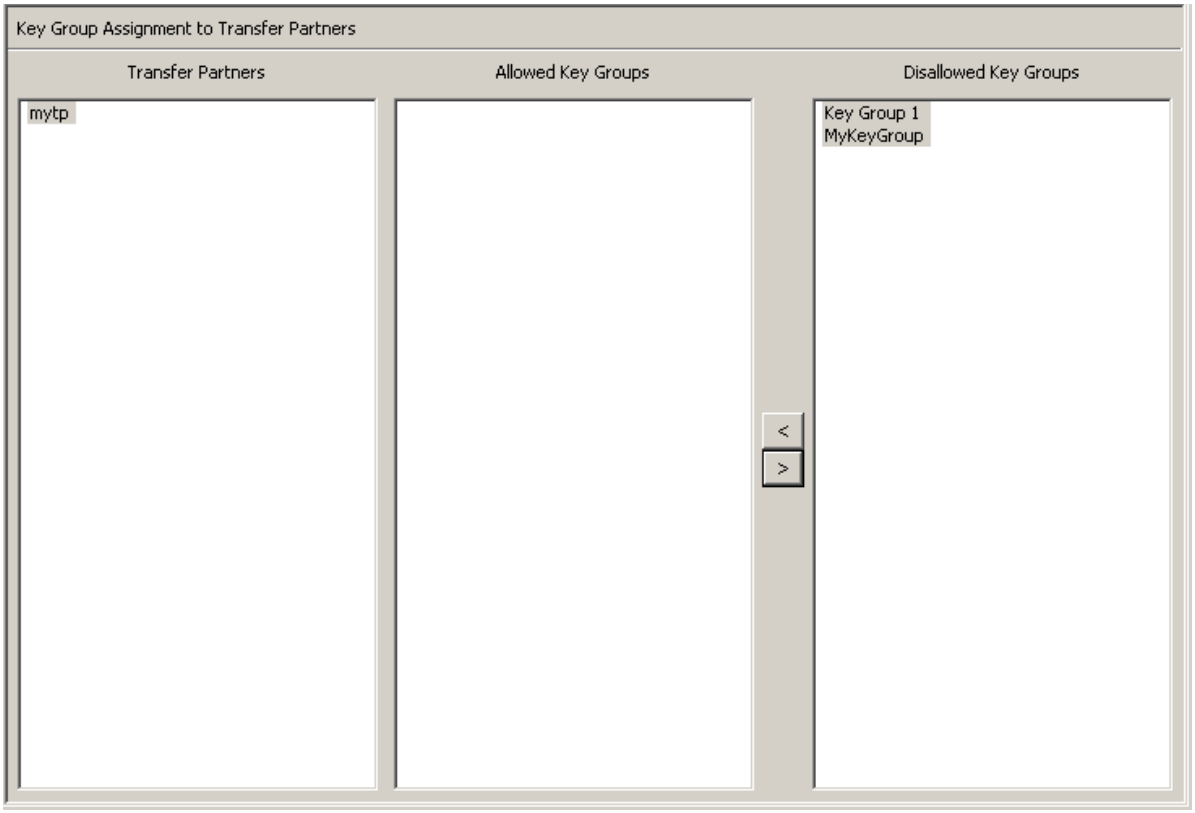


2. The selected Key Group is moved to the Allowed Key Groups column, indicating that the Transfer Partner can now access that Key Group.

Removing a Key Group from a Transfer Partner

To remove a Key Group list from a Transfer Partner:

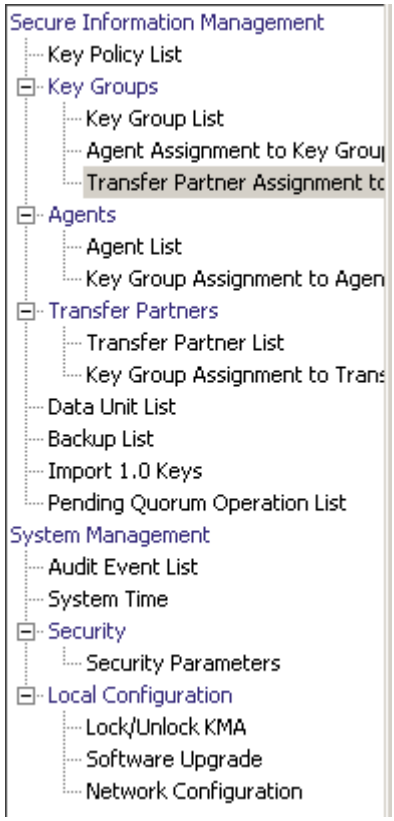
1. In the Transfer Partners column, highlight the Transfer Partner you want to affect. In the Allowed Key Groups column, highlight the Key Group you want to remove and click the Move from > button.



2. The selected Key Group is moved to the Disallowed Key Groups column, indicating that the Transfer Partner cannot access that Key Group.

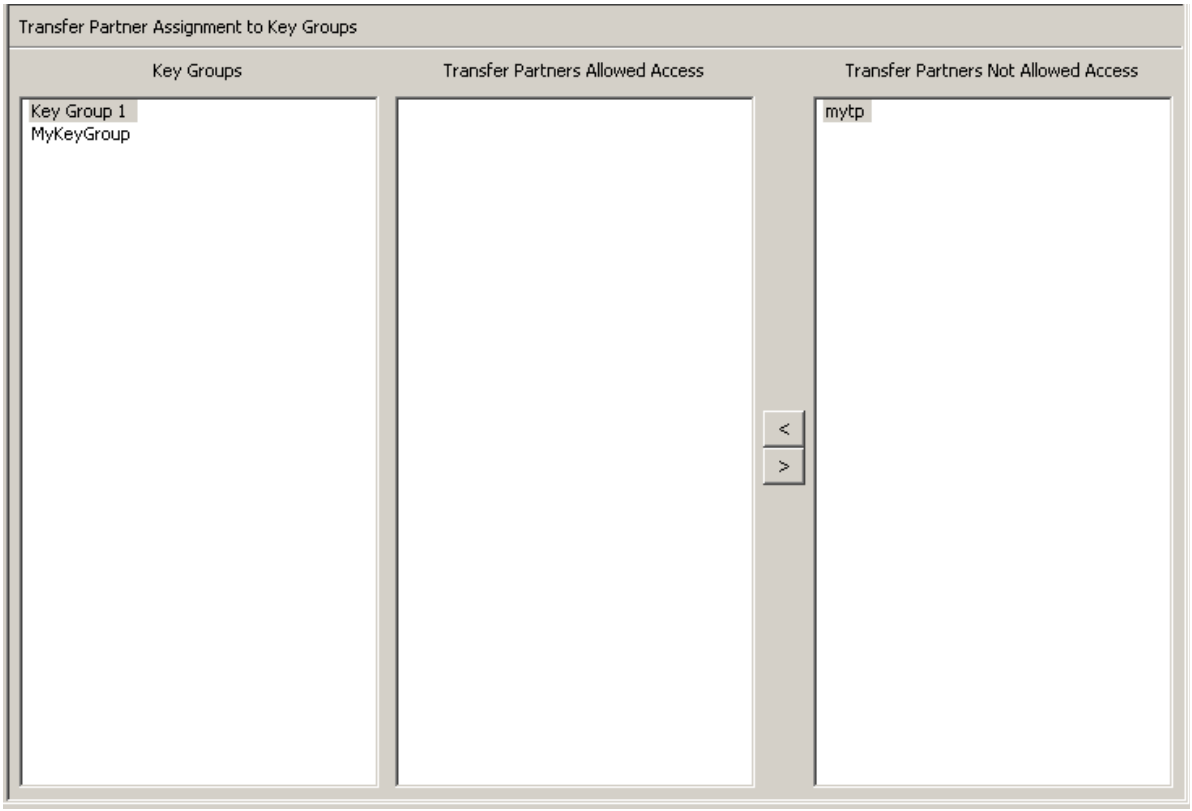
Transfer Partner Assignment to Key Groups Menu

The Transfer Partner Assignment to Key Groups menu allows you to add a key Transfer Partner to the set of Key Transfer Partners that are permitted access to a specific Key Group.



Viewing Transfer Group Assignments

To view Transfer Group assignments, from the Key Groups menu, select Transfer Partner Assignment to Key Groups. The following screen is displayed.

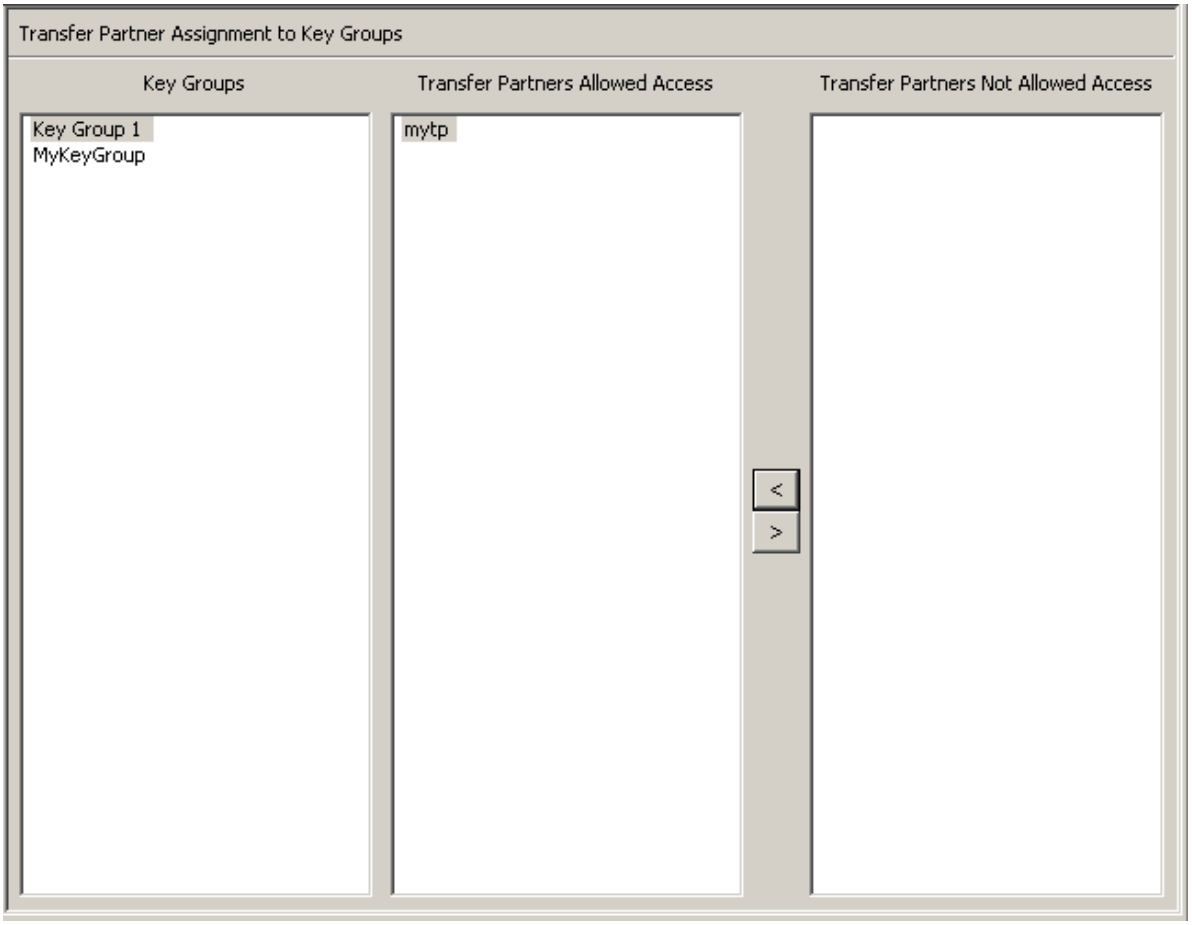


The screen shows the Transfer Partners that can access a Key Group. The Transfer Partners Allowed Access column lists the Transfer Partners assigned to the Key Group. The Transfer Partners Not Allowed Access column displays the Transfer Partners not assigned to the Key Group.

Adding a Transfer Partner to a Key Group

To add a Transfer Partner to a Key Group:

1. In the Key Groups column, highlight the Key Group you want to affect. In the Transfer Partners Allowed Access column, highlight the Key Group you want to add and click the Move to < button.

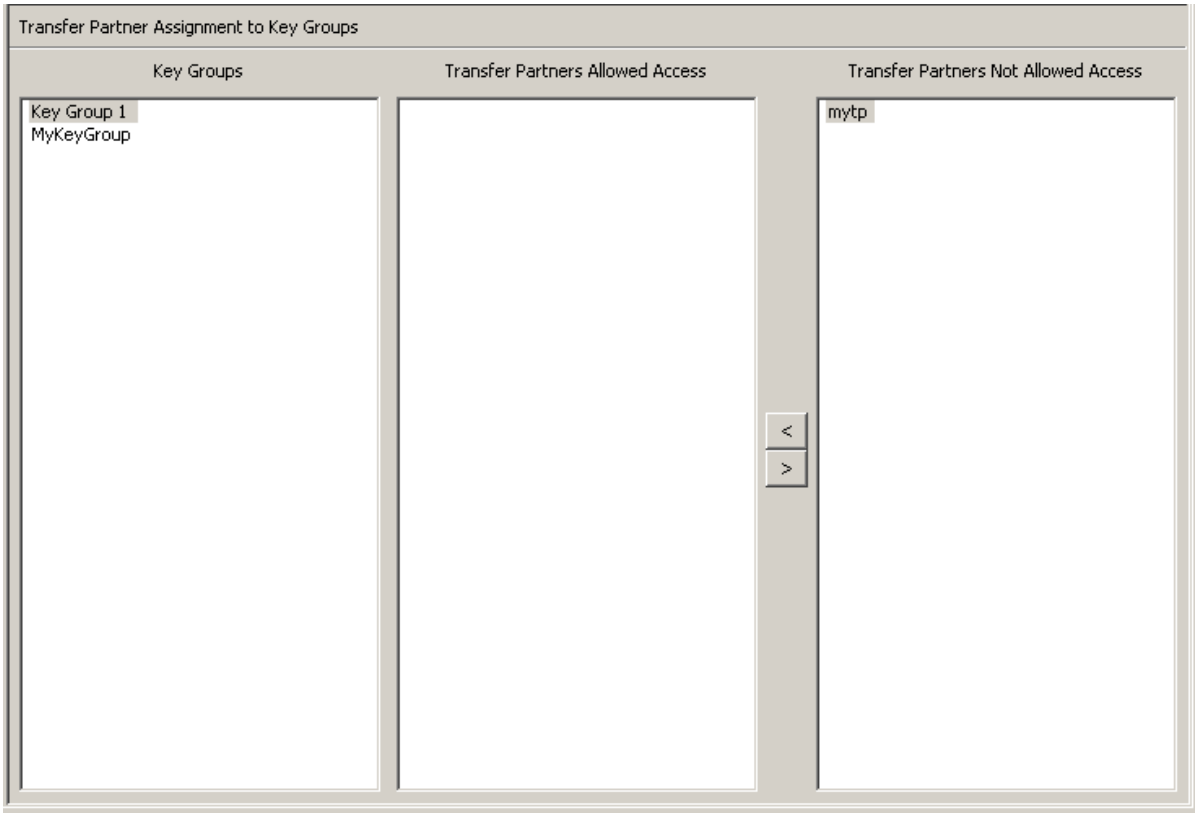


2. The selected Transfer Partner is moved to the Transfer Partners Allowed Access column, indicating that the Key Group can now access that Transfer Partner.

Removing a Transfer Partner from a Key Group

To remove a Transfer Partner from a Key Group:

1. In the Key Groups column, highlight the Key Group you want to affect. In the Transfer Partners Allowed Access column, highlight the Transfer Partner you want to remove and click the Move from [>] button.

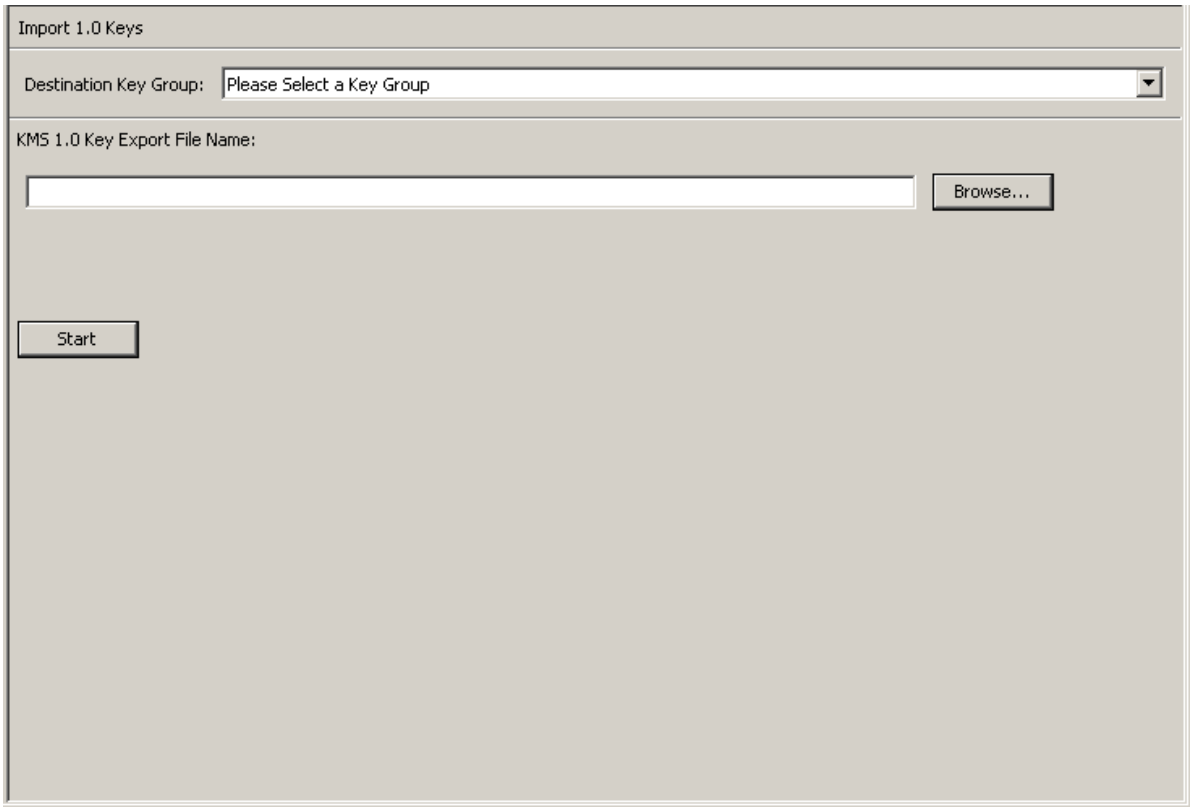


2. The selected Transfer Partner is moved to the Transfer Partners Not Allowed Access column, indicating that the Key Group cannot access that Transfer Partner.

Importing a KMS 1.0 Key Export File

To import a KMS 1.0 Key Export file to the KMA and to create a new Key for each Key in this file:

1. Go to the KMS 1.2 system and export the keys into a file. Only keys exported from KMS 1.2 systems can be imported. KMS 1.0 and 1.1 systems must be upgraded to 1.2 before exporting keys.
2. From the Secure Information Management menu, select **Import 1.0 Keys**.



3. Complete the following parameters:

Destination Key Group

Select the Destination Key Group into which these keys will be imported.

KMS 1.0 Key Export File Name

Type the name of the KMS 1.0 Key Export file.

Browse

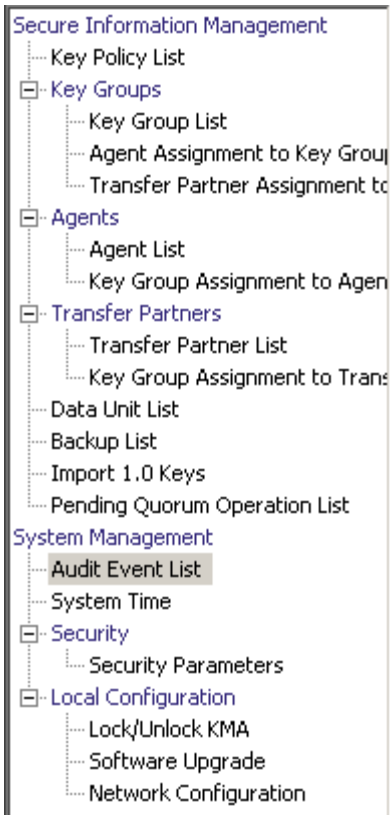
Click this button to locate the file.

Start

Click this button to begin to upload the KMS 1.0 keys file to the KMA, and a new Key is created for each Key it contains. Each new Key is associated with the Key Group you selected. Messages are displayed indicating when the file is uploaded and applied.

Audit Event List Menu

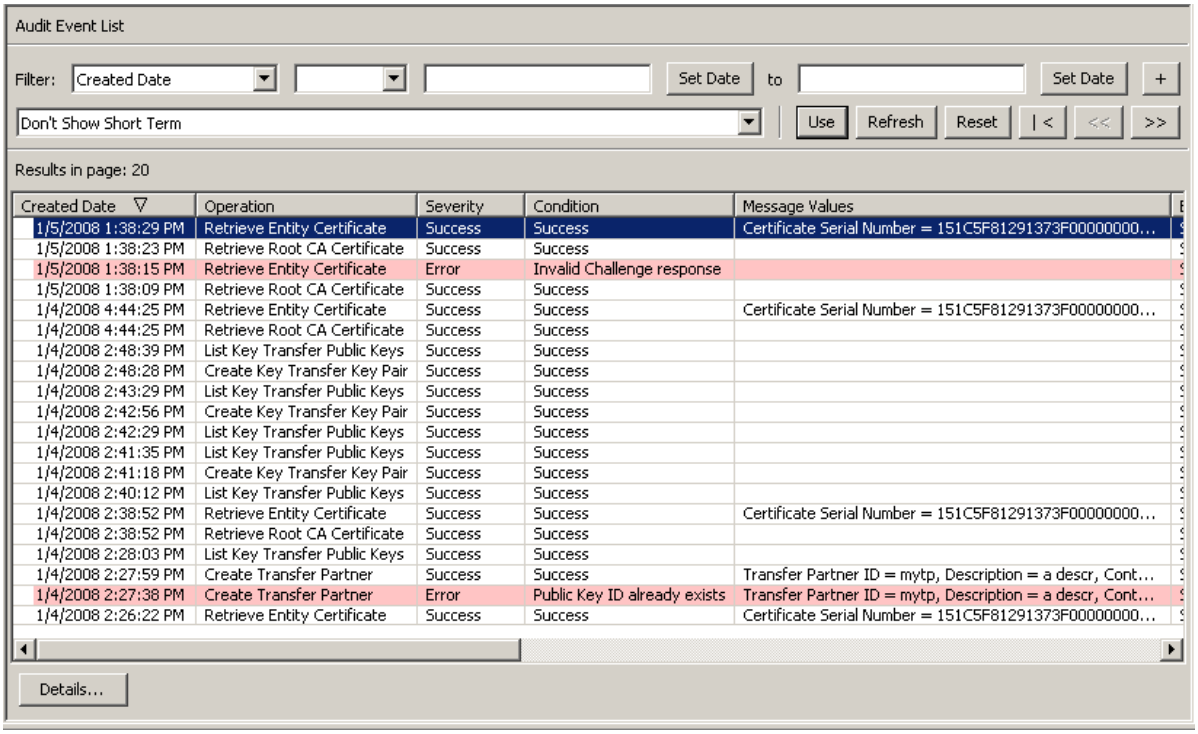
The Audit Event List menu gives you the ability to view the Audit Log events.



Viewing Audit Logs

To view the Audit Log events:

From the System Management menu, select Audit Event List. The Audit Event List screen is displayed.



You can also scroll through the database and filter the Audit Event list by any of the following keys:

- Created Date
- Operation
- Severity
- Condition
- Entity ID
- Entity Network Address
- KMA ID
- KMA Name
- Class
- Retention Term
- Audit Log ID.

The **Use** button applies the filter to the displayed list for the Audit Log.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Created Date
- Operation
- Severity
- Condition
- Entity ID
- Entity Network Address
- KMA Name
- Class
- Retention Term
- Audit Log ID

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Empty
- Not empty

Filter Value 1 box:

If you selected the Date filter, click Set Date to specify start date and time. The value appears as a starting value of the filter key range. If you selected any other filter, type a value in this field.

Filter Value 2 box:

If you selected the Date filter, click Set Date to select an end date and time. The value appears as a ending value of the filter key range.

Filter Value 3 box:

Click the down-arrow and select one of the following filters:

- Don't Show Short Term
- Show All Retentions

Created Date

Displays the date and time that the Audit Event was created.

Operation

Displays the operation that resulted in the creation of the Audit Event record.

Severity

Indicates the severity of the condition if the operation was not successful. Possible values are Success (no error), Warning, or Error.

Condition

Indicates whether the operation was successful or not.

Note – Errors are highlighted in red; Warnings are highlighted in yellow. If you hover the cursor over an error message, a more detailed description of the error is displayed.

Event Message

Displays detailed information of the Audit Event entry.

Entity ID

If this Audit Event is generated in response to an operation requested by a user, Agent, or peer KMA, then this field displays the user-specified identifier of that entity. Otherwise, this field is blank.

Entity Network Address

If this Audit Event is generated in response to an operation requested by a user, Agent, or peer KMA, then this field displays the network address of that entity. Otherwise, this field is blank.

KMA ID

Displays the name of the KMA that generated this audit event. This KMA name is the user-supplied identifier that distinguishes each KMA in a Cluster.

KMA Name

Displays the user-supplied identifier that distinguishes each Appliance in a Cluster.

Class

Identifies the class of operations to which the Audit Event entry belongs. Possible values are:

- Agent Access Control Management Operations
- Agent Client Generated Audits
- Agent Management Operations
- Appliance Management Operations
- Audit Log Agent Operations
- Audit Log Management Operations
- Audit Log Operations

- Backup Management Operations
- CA Operations
- Cluster Client Communication
- Cluster Operations
- Communication and Authentication
- Console Security Management Operations
- Data Unit Agent Operations
- Data Unit Management Operations
- Discovery Operations
- Key Group Agent Operations
- Key Group Management Operations
- Key Policy Management Operations
- License Key Management Operations
- Local Management Operations
- Management Client Generated Audits
- Passphrase Agent Operations
- Replication Operations
- Retrieve Certificate Operations
- Role Management operations
- SNMP Management Operations
- Security Management Operations
- Security Parameter Management Operations
- Security Violation
- Site Management Operations
- System Messages
- User Management Operations.

Retention Term

Displays the defined length of time that the Audit Event record is retained. Possible values are and their descriptions are:

Long Term

Event records that must be stored for a lengthy period of time.

Medium Term

Event records that must be stored for a medium length period of time.

Short Term

Event records that must be stored for a short period of time.

Audit Log Entry ID

Displays a system-generated unique identifier that distinguishes each type of Audit Event entry.

Audit Log ID

Displays a system-generated unique identifier that distinguishes each Audit Event entry.

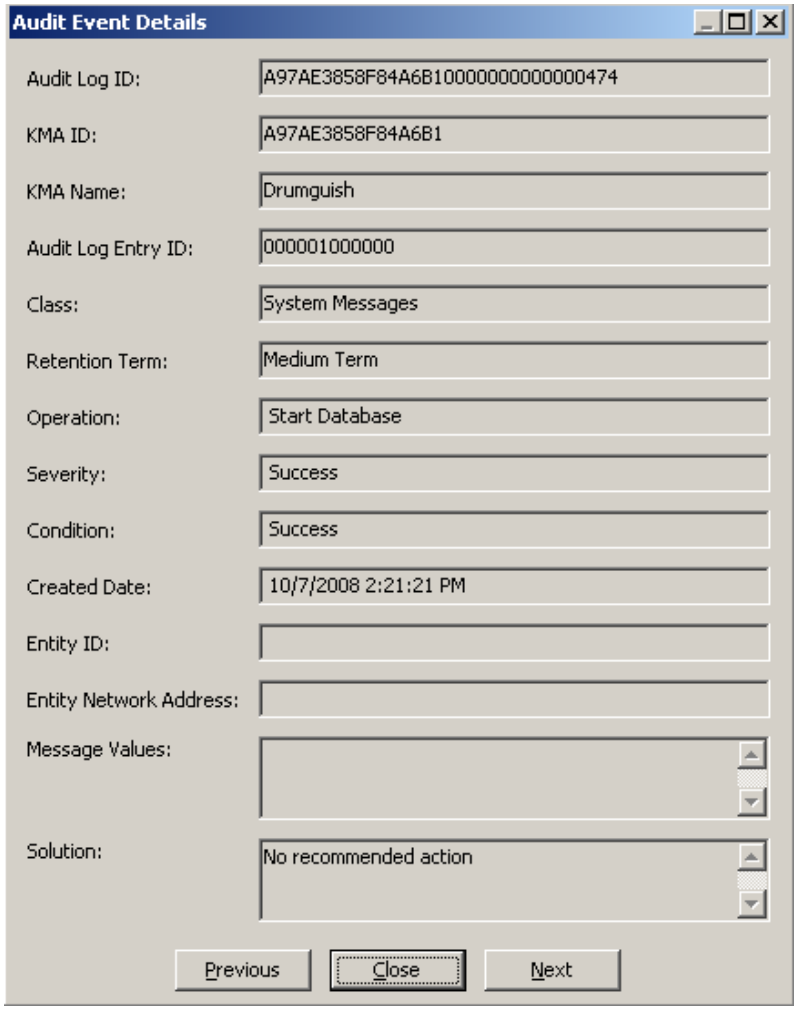
If you want more detailed information on an Audit Log, highlight the Audit Log and click the Details button. For more information, refer to "Viewing Audit Log Details" below.

Click the Export button to export the Audit Log. For more information, refer to "Exporting an Audit Log" on page 262.

Viewing Audit Log Details

To view Audit Log details:

1. From the Audit Event List screen, select the Audit Log entry on which you want more information and click the Details button or double-click the entry. The Audit Event Details dialog box is displayed, where all fields are disabled, except for the Previous, Close, and Next buttons.



2. Click the Previous or Next buttons to access the previous or next Audit Event, or the Close button to return to the Audit Event List screen.

Exporting an Audit Log

The Export function allows you to export all or specific Audit Log entries to a text file on your workstation. You can then bring up the file in a spreadsheet application.

To export an Audit Log:

1. From the Audit Event List screen, either select `Save Report...` from the View menu or press Ctrl-S.
2. When you are finished, click the Start button to initiate the export process. If you have filtered the entries in the Audit Event List screen, only those entries are exported. Otherwise, all audit events are exported.
3. When the export process is completed, the number of Audit Logs that have been exported is shown at the bottom of the dialog box.
4. Click the Close button to close this dialog box and return to the Audit Event List screen.

Data Unit List Menu

The Data Unit List menu allows you to:

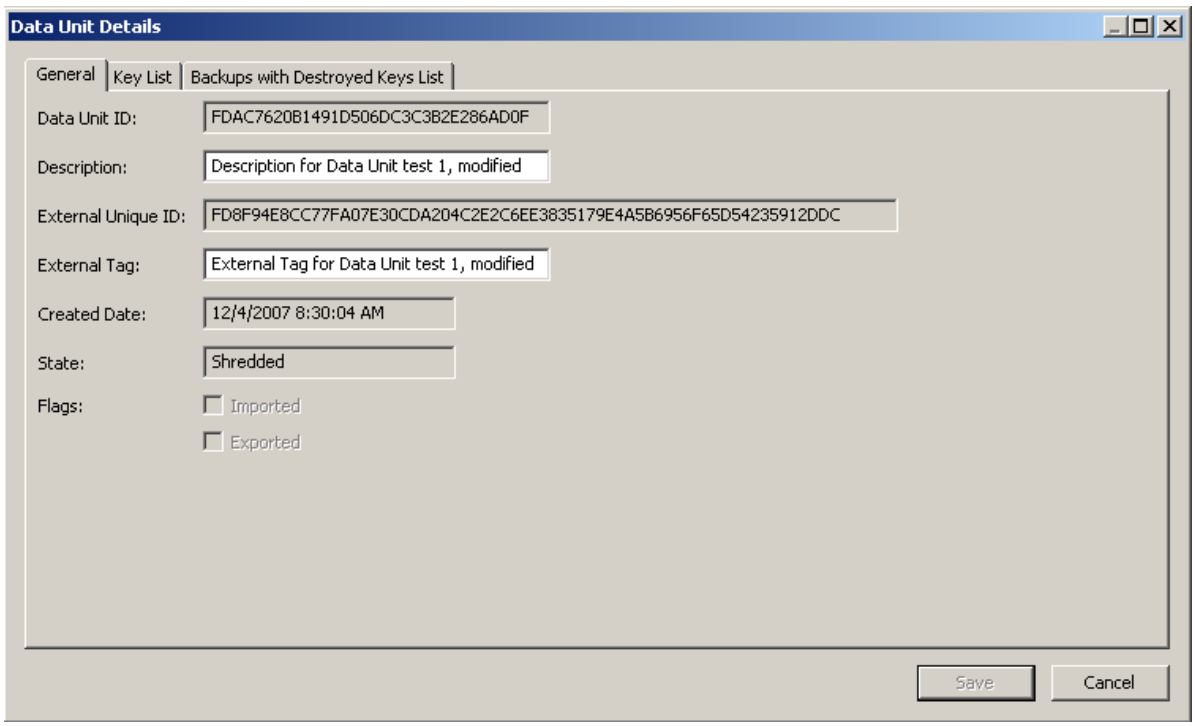
- View Data Units
- View/Modify Data Unit details
- View the activity history for a Data Unit
- Destroy post-operational keys for a Data Unit.

For procedures on using the Data Units menu, refer to "Data Unit List Menu" on page 282.

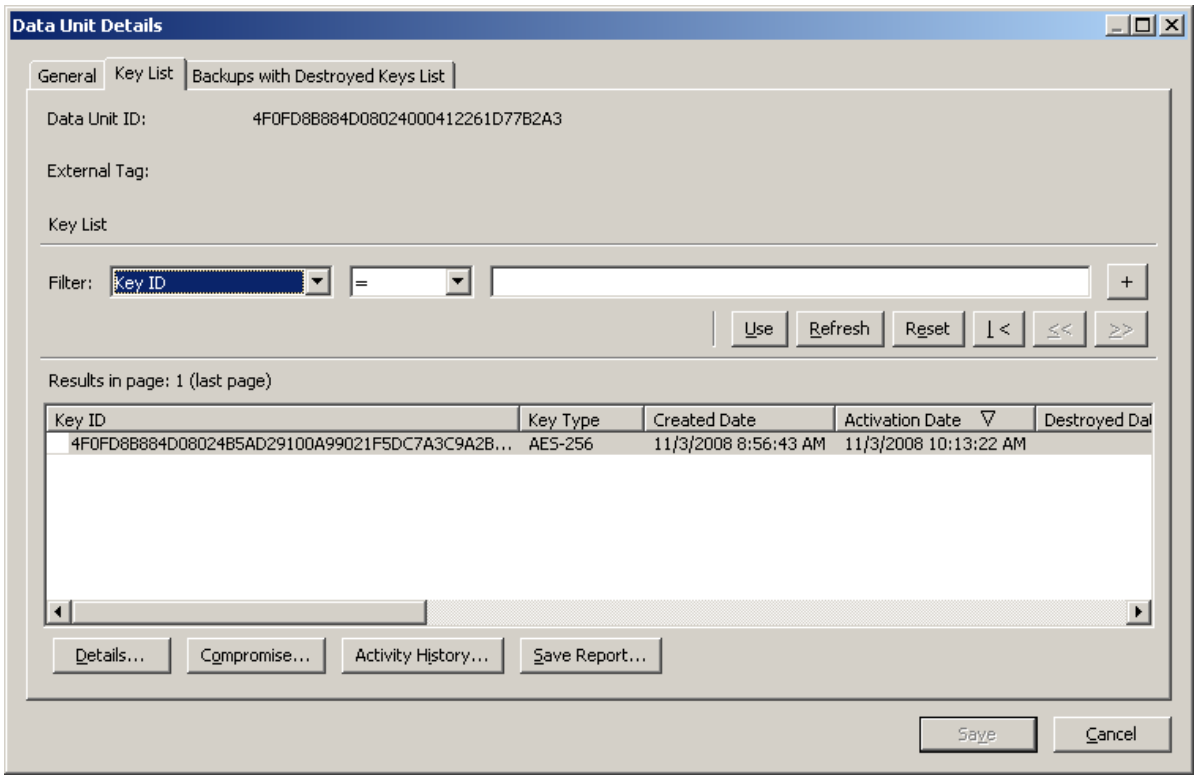
Compromising Keys

Compliance Officers are authorized to compromise keys.

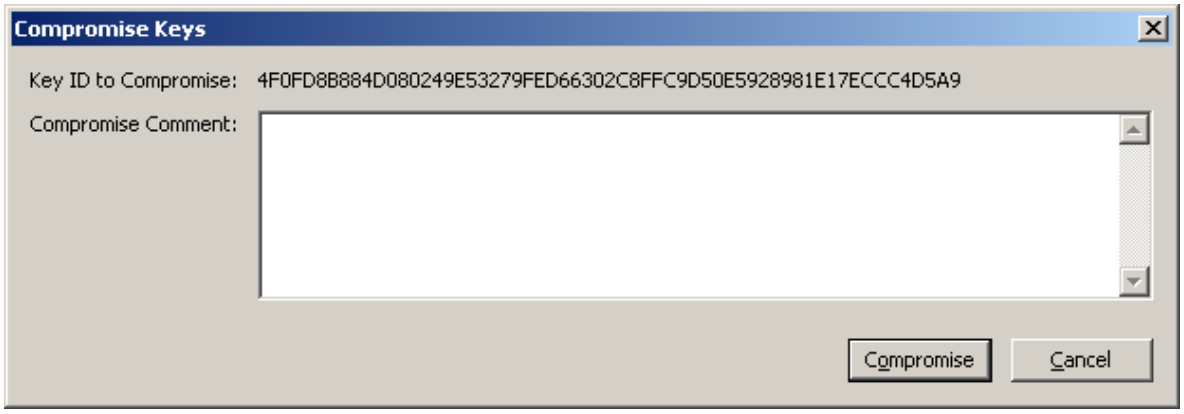
1. From the Data Unit List screen, select the Data Unit you want to modify and click the Details button. The Data Unit Details dialog box is displayed.



2. Click the Key List tab to view the key(s) associated with this Data Unit.



3. Select the key(s) you want to compromise and click the Compromise button. A dialog box is displayed confirming the compromise of the key(s).
4. Click the Yes button. The following dialog box is displayed, prompting you to enter a comment.



5. Type a comment about the compromise of the selected key(s). If you click the Compromise button, another dialog box is displayed confirming the compromise of the key(s).
6. Click the Yes button. A dialog box is displayed showing the number of keys that have been compromised.

Other Functions

A Compliance Officer can also:

- View the Audit Event List
- View the System Time
- Lock/Unlock KMA status.

For procedures on viewing the these functions, refer to Chapter 5, “Security Officer Operations”.

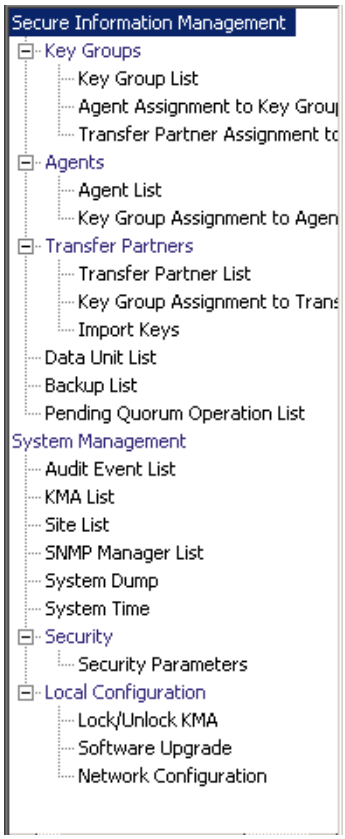
CHAPTER 7

Operator Operations

This chapter describes the operations that a user who has been given an Operator role can perform. If you have been assigned multiple roles, refer to the appropriate chapter for instructions on performing the specific role.

Operator Role

As the Operator, you are responsible for managing the day-to-day operations of the system.



Key Groups Menu

The Key Groups menu allows you to:

- View a list of Key Groups
- View Agent to Key Group Assignments
- View Transfer Partner to Key Group Assignments.

Key Group List

The Key Group List menu option gives you the ability to manage your Key Group. For procedures, refer to "Key Group List Menu" on page 224.

Agent Assignment to Key Groups

The Agent Assignment to Key Groups menu option gives you the ability to view Agents to Key Groups. For procedures, refer to "Agent Assignment to Key Groups Menu" on page 232.

Transfer Partner Assignment to Key Groups

The Transfer Partner Assignment to Key Groups option allows you to view a Key Transfer Partner to the set of Key Transfer Partners that are allowed access to a specific Key Group. For procedures, refer to "Transfer Partner Assignment to Key Groups Menu" on page 249.

Agent List Menu

The Agent List menu option allows you to:

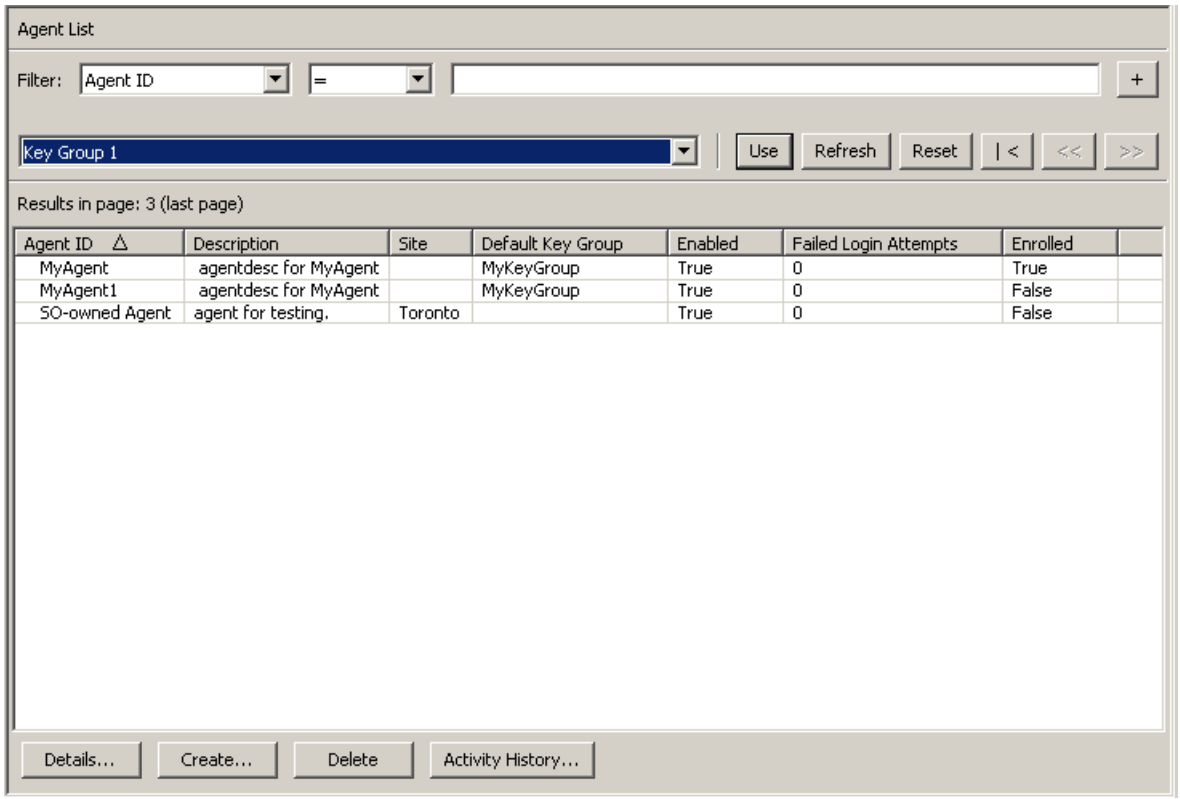
- View Agents
- Create Agents
- View/Modify an Agent
- Delete existing Agents.

Viewing the Agent List

The Agent List menu option allows you to view all Agents associated with a specific Key Group.

To view this screen:

1. From the Agents menu, select **Agent List**. The Agent List screen is displayed.
2. Click the down-arrow beside the Key Group field and select a Key Group. The Agents that are associated with the Key Group are displayed.



You can also scroll through the lists and filter the Agents lists by any of the following keys:

- Agent ID
- Description
- Site
- Default Key Group
- Enabled
- Failed Login Attempts
- Enrolled.

The **Use** button applies the filter to the displayed list for the Agent.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Agent ID
- Description
- Site
- Default Key Group
- Enabled
- Failed Login Attempts
- Enrolled

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value text box:

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Click this button to add additional filters.

Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

Use:

Click this button to apply the selected filters to the displayed list and go to the first page.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Agent ID

Displays the user-specified unique identifier that distinguishes each Agent.

Description

Describes the Agent.

Site

Displays a unique identifier that indicates the Site to which the Agent belongs.

Default Key Group

The Key Group associated with all keys created by this agent if the agent does not explicitly specify a different Key Group.

Enabled

Indicates the status of the Agent. Possible values are: True or False. If this field is False, the Agent cannot establish a session with the KMA.

Failed Login Attempts

Displays the number of times that an attempted logon has failed

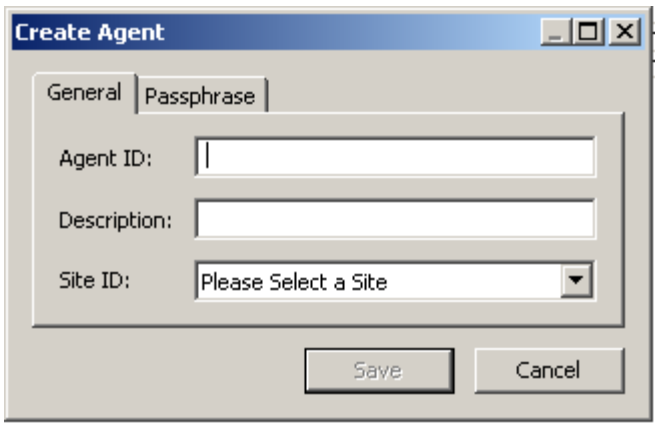
Enrolled

Indicates whether the Agent has enrolled successfully with the OKM Cluster. Possible values are True or False. This field is False if the Agent is the first created or if the Agent's passphrase is changed.

Creating an Agent

To create an Agent:

1. From the Agents List screen, click the Create button. The Create Agent dialog box is displayed with the General tab open.



2. Complete the following parameters:

Agent ID

Type a value that uniquely identifies the Agent. This value can be between 1 and 64 (inclusive) characters.

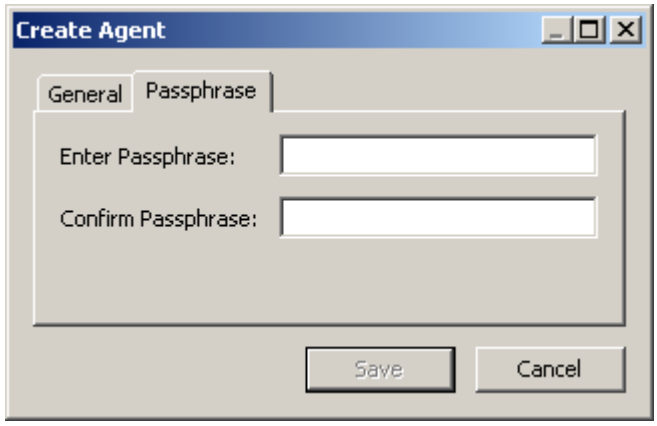
Description

Type a value that describes the Agent. This value can be between 1 and 64 (inclusive) characters.

Site ID

Click the down-arrow and highlight the Site to which the Agent belongs. This field is optional.

3. Open the Passphrase tab.



4. Complete the following parameters:

Passphrase

Type the passphrase for this user. The minimum value is 8 characters; the maximum value is 64 characters. The default value is 8.

Passphrase requirements:

- A passphrase must not contain the user's Agent ID.
- A passphrase must contain three of the four character classes: uppercase, lowercase, numeric, or special characters.

  The following special characters are allowed:

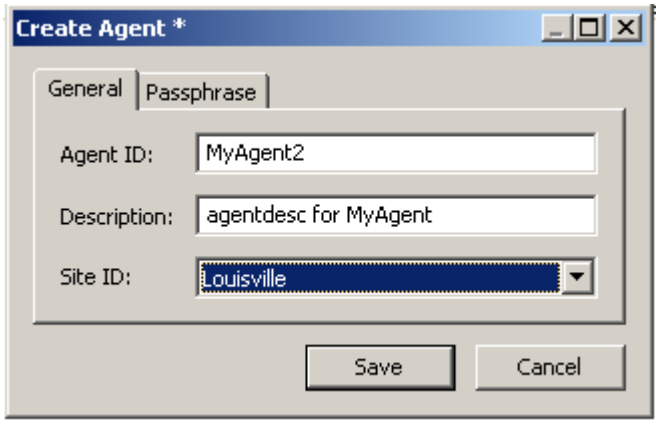
  ' ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ' " < > , . / ?
- Control characters, including tabs and linefeeds, are not allowed.

Note – To modify the minimum length requirement for passphrases, see "Modifying the Security Parameters" on page 192.

Confirm Passphrase

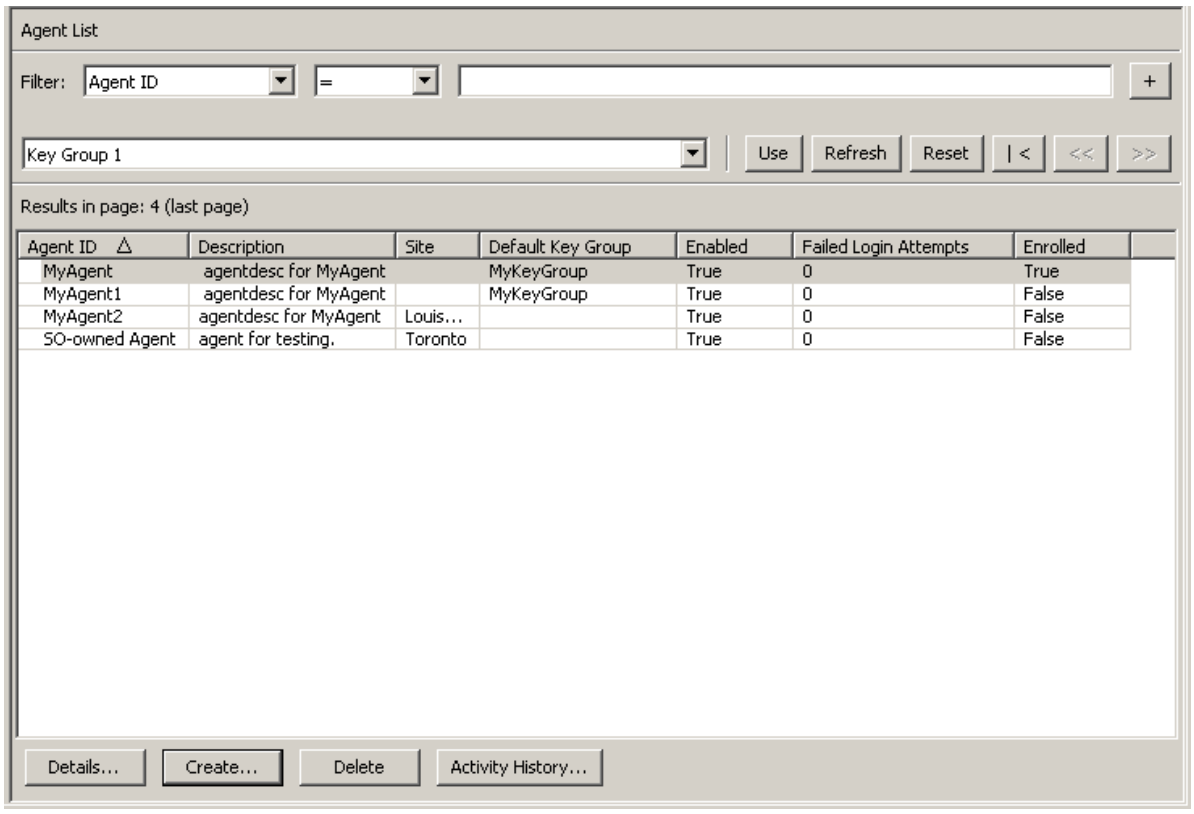
Type the same value that you entered in the Enter Passphrase field.

An example of a completed Create Agent dialog box is shown below.



5. Click the Save button. The Agent record is added to the database and is displayed in the Agent List screen.

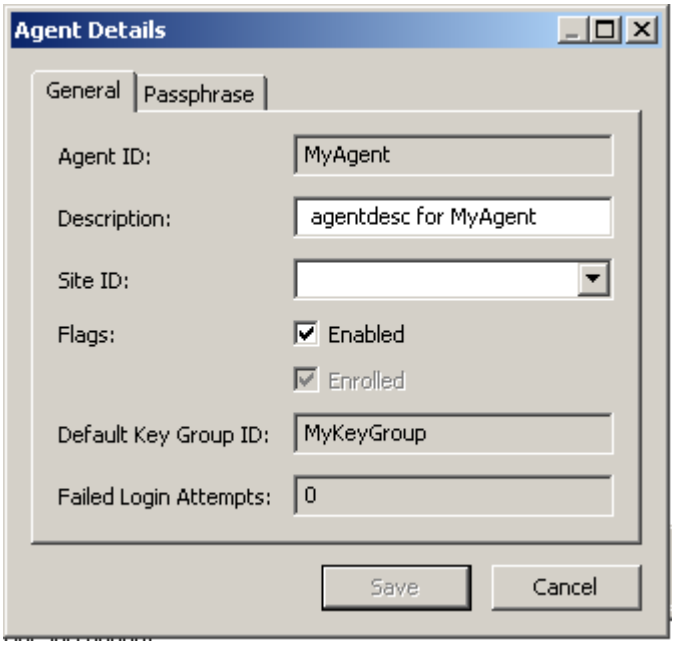
6. Complete the agent-specific enrollment procedure using the agent-specific interface. For example, for StorageTek drives, the VOP (Virtual Operator Panel) must be used to complete the enrollment procedure.


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...

Viewing/Modifying an Agent

To modify an Agent's details:

1. From the Agents List screen, double-click an Agent entry for which you want more information or highlight an Agent entry and click the Details button. The Agents Details dialog box is displayed.



2. Open the General tab and modify the following fields, as required:

- Description
- Site ID
- Flags - Enabled.

Note – You should only change the Agent's passphrase if you believe that the passphrase has been compromised. For procedures, refer to "Setting an Agent's Passphrase" on page 277.

---

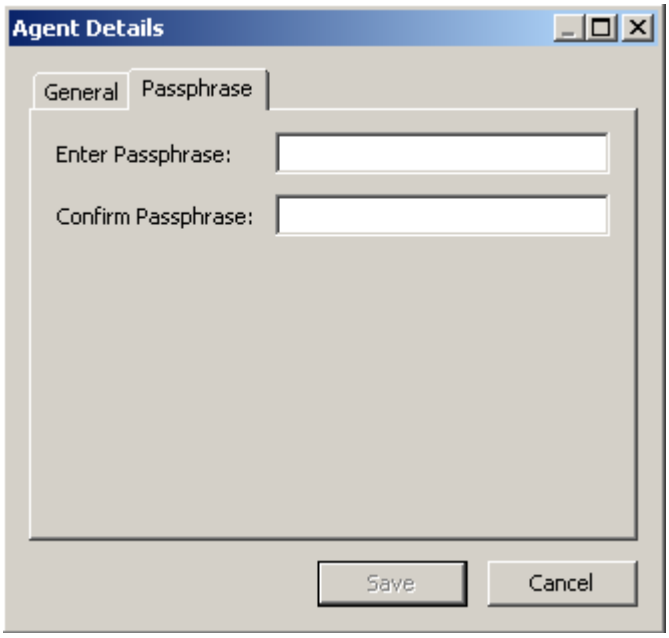
3. When you are finished, click the Save button. The changes are made to the OKM Manager database and you are returned to the Agents List screen.

Setting an Agent's Passphrase

When you set an Agent's passphrase, you are effectively revoking the Agent certificate that enables the Agent to authenticate itself with the KMA. As the Operator, you may want to set an Agent's passphrase certificate if you believe that the Agent certificate and/or passphrase has been compromised.

To set an Agent's passphrase:

1. From the Agents List screen, double-click the Agent entry whose passphrase you want to set or highlight the Agent entry and click the Details button. The Agent Details dialog box is displayed. Open the Passphrase tab.

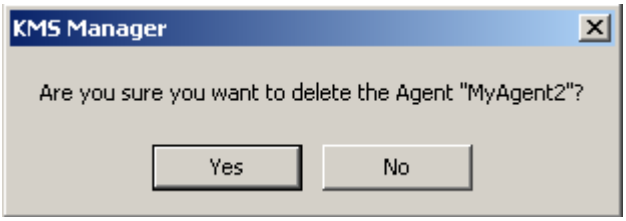


2. Modify the following fields and click the Save button:
   - Enter Passphrase
   - Confirm Passphrase.
3. The changes are made to the database and you are returned to the Agents List screen.
4. Re-enroll the Agent using the agent-specific procedure. For example, for StorageTek tape drives, the VOP (Virtual Operator Panel) must be used to re-enroll the Agent with the OKM Cluster. After changing an Agent's passphrase, the Agent will not be able to make requests to the OKM Cluster until it is re-enrolled.

Deleting Agents

To delete an Agent:

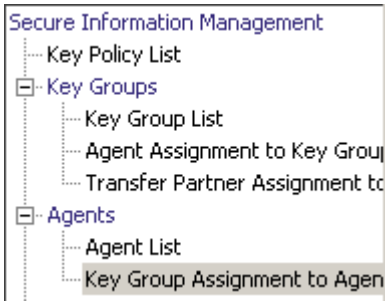
1. From the Agents List screen, highlight the Agent you want to delete. The following dialog box is displayed, prompting you to confirm that you want to delete the selected Agent.



2. Click the Yes button to delete the Agent. The Agent is removed from the database and you are returned to the Agents List screen, where the deleted Agent is no longer listed.

Key Group Assignment to Agents Menu

The Key Group Assignment to Agents menu option allows you to view Key Groups assigned to Agents. For procedures, refer to "Key Group Assignment to Agents Menu" on page 238.



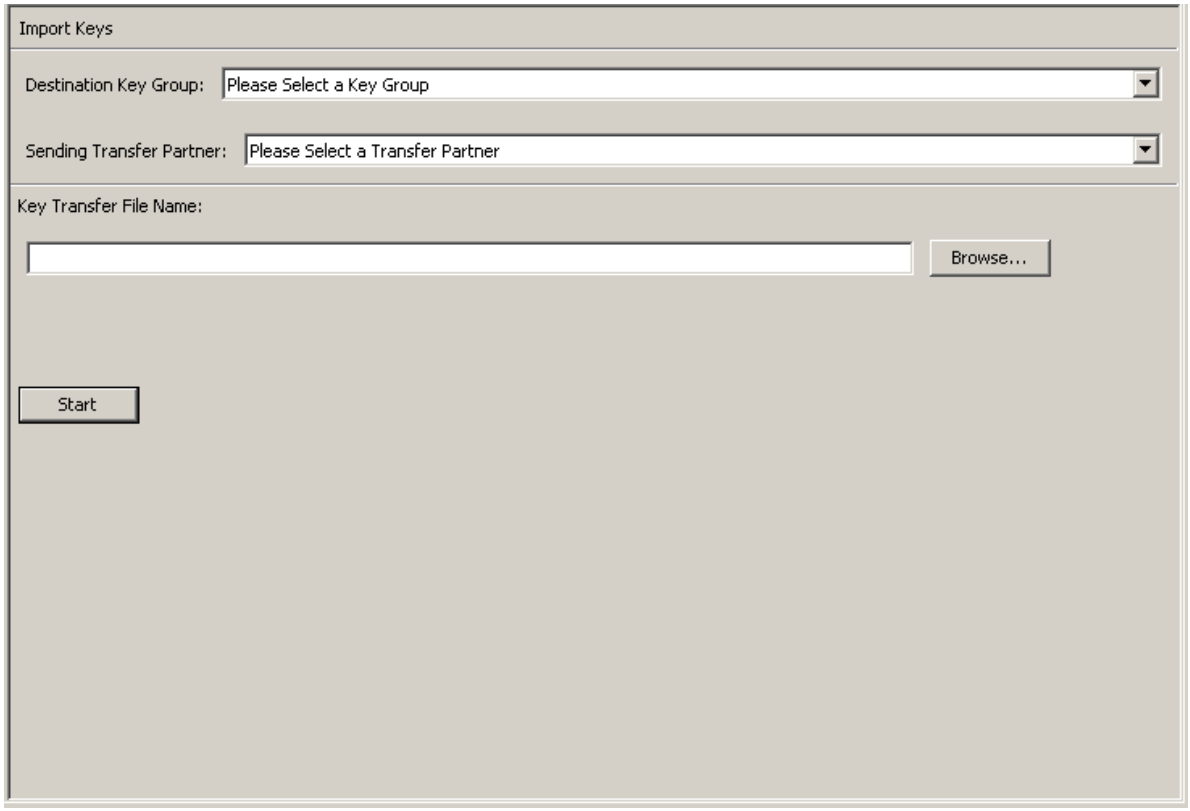
Import Keys Menu

This menu option imports keys and data units into a OKM Cluster. The keys and data unit information are contained in a key transfer file received from a Key Transfer Partner.

Note – Use this screen to upload and import keys to the OKM Cluster. These keys are exported from another OKM Cluster.

To import keys:

1. From the Transfer Partners menu, select Import Keys. The Import Keys screen is displayed.



2. Complete the following parameters:

Destination Key Group:

Select the Destination Key Group into which these keys will be imported.

The “Allow Imports” flag for this Key Group's key policy must be checked. This Key Group must be an allowed Key Group for the selected sending Transfer Partner.

Sending Transfer Partner:

Select the Sending Transfer Partner which exported these keys.

Key Transfer File:

Type the name of the Key Transfer file. You can also click Browse to select a destination path.

3. Click the Start button to begin the upload and key import process. Messages are displayed, indicating when the file is uploaded and applied.

Data Units

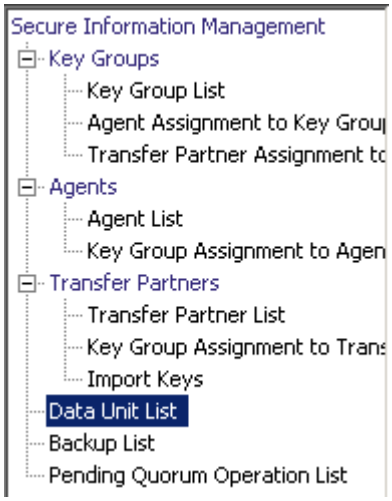
Data Units are logical storage devices, such as disks, tapes, objects. Data Units are secured by valid Key Policies that are associated with their Key Groups. Agent must have access to the selected Data Unit.

Note – An Operator can perform all functions, except modify a Data Unit's Key Group. Only a Compliance Officer can modify a Data Unit's Key Group.

Data Unit List Menu

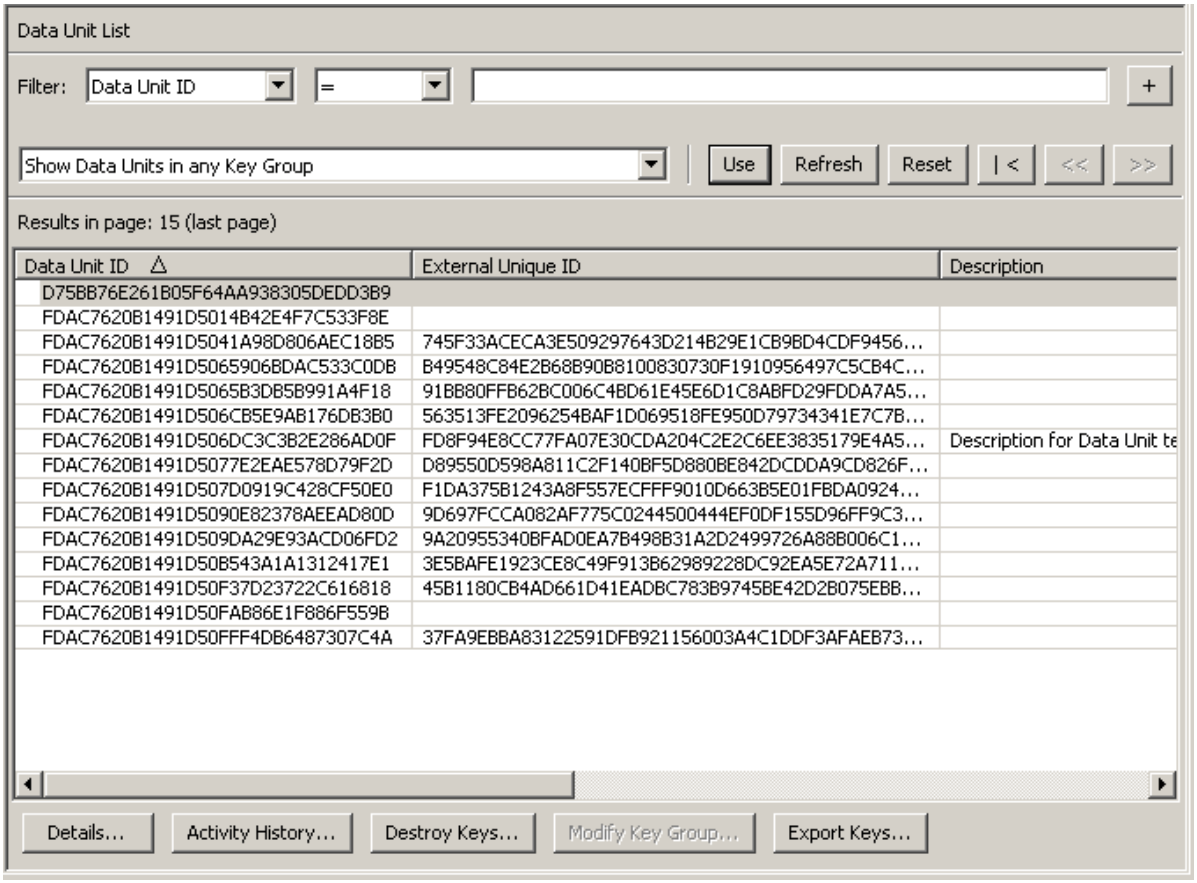
The Data Unit List menu allows you to:

- View Data Units
- View/Modify Data Unit details
- View the activity history for a Data Unit
- Destroy post-operational keys for a Data Unit.



Viewing Data Units

To view Data Units, from the Data Units menu, select Data Unit List. The Data Unit List screen is displayed.



You can also scroll through the database and filter the Data Unit list by any of the following keys:

- Data Unit ID
- External Unique ID
- Description
- External Tag
- Created Date
- Exported
- Imported
- State.

The **Use** button applies the filter to the displayed list for the Data Unit.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Data Unit ID
- External Unique ID
- Description
- External Tag
- Created Date
- Imported
- Exported
- State

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Show Data Units in Any Key Group. Use:

Click this button to apply the filter to the displayed list.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Data Unit ID

Displays a system-generated unique identifier that distinguishes each Data Unit.

External Unique ID

Displays a unique external identifier for the Data Unit.

This value is sent to the OKM by the Agent and may not be externally visible to an end user. For LTO Gen 4 and Gen 5 tapes, this is the cartridge serial number burned into the cartridge when it is manufactured. Do not confuse this value with a volser on an optical barcode or in an ANSI tape label. This value is not used for StorageTek tape drives.

Description

Describes the Data Unit.

External Tag

Describes a unique external tag for the Data Unit.

For tapes that are in a StorageTek tape library, or tapes that have ANSI standard labels, this field will be the volser. If the tape is in a library and has an ANSI label, the library volser (i.e., optical bar code) will be used if it differs from the volser contained in the ANSI label. For tapes written in stand-alone drives without ANSI labels, this field will be blank.

Note – For Data Units written by LTO Gen 4 and Gen 5 tape drives, this field is padded on the right with blanks to fill in 32 characters. It may be more convenient for you to use the "Starts With ~" filter operator instead of the "Equals =" filter operator, so that you do not have to add the blanks to pad the External Tag.

For example, if you use the "Starts With" filter, you could enter:

```
"External Tag" ~ "ABCDEF"
```

If you use the "Equals" filter for the same example, you would need to enter:

```
"External Tag" = "ABCDEF                                "
                          (padded to fill 32 characters)
```

Created Date

Indicates the date and time when the Data Unit was created/registered.

Exported

Indicates whether the keys associated with this Data Unit have been exported.

Imported

Indicates whether the keys associated with this Data Unit have been imported.

State

Indicates the state of the Data Unit. Possible values are:

- No Key: Set when the Data Unit has been created, but has not yet had any keys created.
- Readable: Set when the Data Unit has keys that allow at least some parts of the Data Unit to be decrypted (read).
- Normal: Set when the Data Unit has keys that allow at least some parts of the Data Unit to be decrypted (read). In addition, the Data Unit has at least one protect-and-process state key that can be used to encrypt data. The Data Unit is therefore writable.
- Needs ReKey: Set when the Data Unit has keys that allow at least some parts of the Data Unit to be decrypted (read). However, the Data Unit does not have at least one protect-and-process state key.

  If data is written to this tape, it will automatically be given a new protect and process key.
- Shredded: Set when all of the keys for this Data Unit are destroyed. The Data Unit cannot be read or written. However, a new key can be created for this Data Unit, moving its state back to Normal.

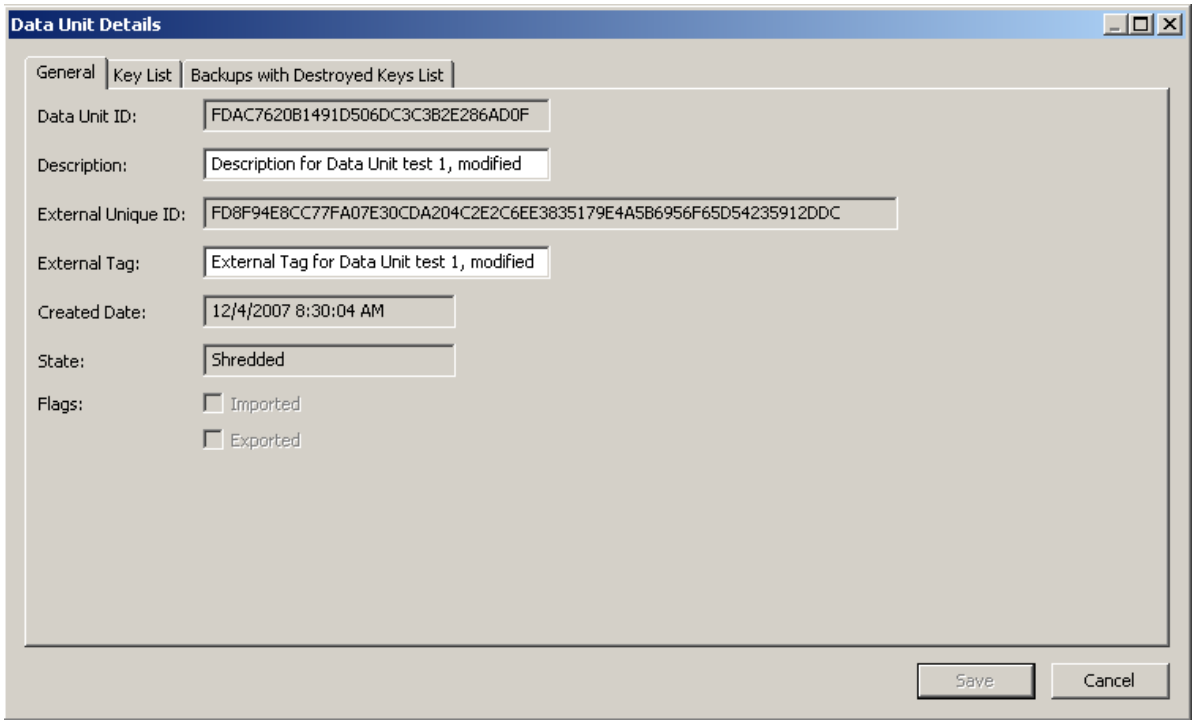
Viewing/Modifying Data Unit Details

Note – If you are not an Operator, when you view a Data Unit's detailed information, all fields, including the Save button, are disabled. If you are a Compliance Officer, the Key Group field is enabled.

Under the Key List tab, the Compromise button is enabled if you are a Compliance Officer; otherwise, it is disabled.

To modify a Data Unit's information:

1. From the Data Unit List screen, select the Data Unit you want to modify and click the Details button. The Data Unit Details dialog box is displayed.



2. You can modify the following parameters:

Description

Type a new value. The original information is provided by the Software Encryption Driver during registration. This value can be between 1 and 64 (inclusive) characters or blank.

Important – If the Description field contains the string "`PKCS#11v2.20`," this represents a special key used for Oracle Database Transparent Data Encryption (TDE). **Do not change this field.** Doing so can alter the way OKM interacts with TDE.

External Tag

Type a unique external identifier for the Data Unit. This value can be between 1 and 64 (inclusive) characters or blank. This field typically contains the label or barcode of the tape cartridge.

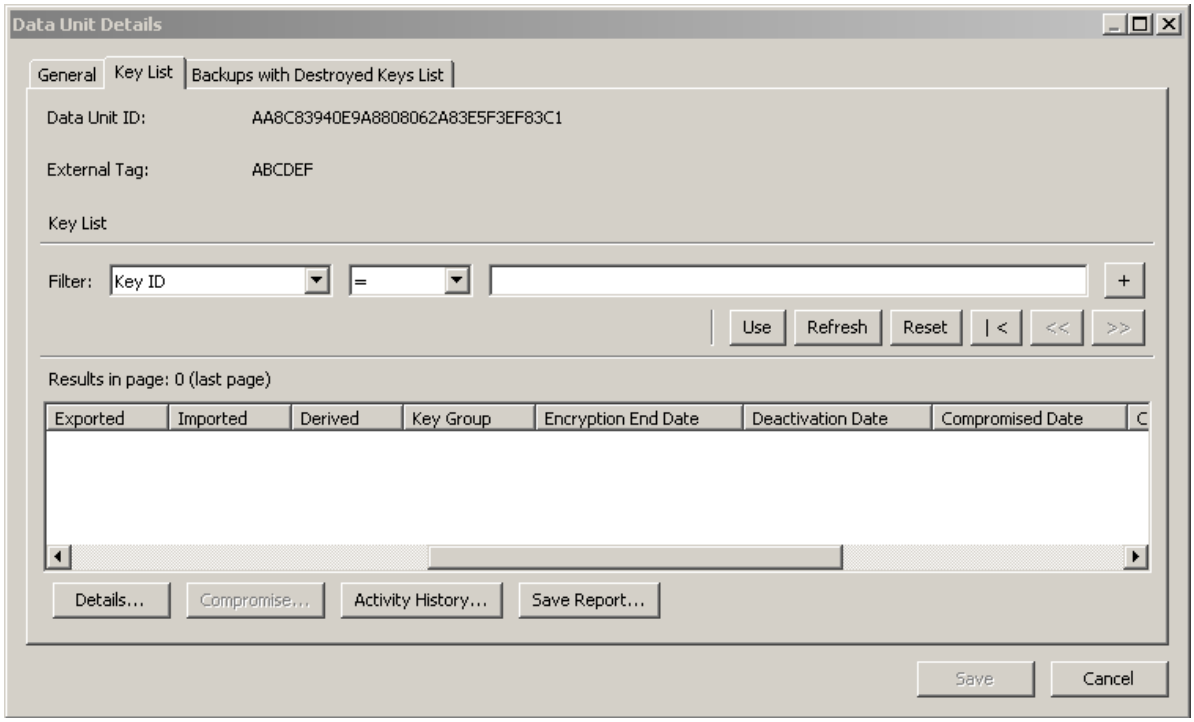
3. Click the Save button to save your changes.

The following are non-editable fields:

General Tab

- Data Unit ID
- External Unique ID
- Created Date
- State
- Flags Imported/Exported.

Key List Tab



Data Unit ID

Uniquely identifies the Data Unit.

Data Unit Description

Describes the Data Unit.

Key ID

Displays the key information for the Data Unit.

Key Type

Indicates the type of encryption algorithm that this key uses. Possible values are: AES-256.

Created Date

Displays the date and time when the key was created.

Activation Date

Displays the date and time when the key was activated. This is the date and time when the key was first given to an Agent. It is the starting date and time for the key's encryption period and cryptoperiod.

Destroyed Date

Displays the date when the key was destroyed. If the field is blank, then the key is not destroyed.

Destruction Comment

Displays any user-supplied information about the destruction of the key. If the field is blank, then the key is not destroyed.

Exported

Indicates whether the Data Unit has been exported.

Imported

Indicates whether the Data Unit has been imported.

Derived

Indicates whether the Key has been derived from a Master Key generated by the Master Key Provider. Refer to the *OKM-ICSF Integration Guide* for detailed information.

Key Group

Displays the Key Group associated with the Data Unit.

Encryption End Date

Displays the date and time when the key will no longer be used or was stopped from being used for encrypting data.

Deactivation Date

Displays the date and time when the key will be or was deactivated.

Compromised Date

Displays the date when the key was compromised. If the field is blank, then the key is not compromised.

Compromised Comment

Displays any user-supplied information about compromising the key. If the field is blank, then the key is not compromised.

Key State

Indicates the Data Unit’s key state. Possible values are:

Generated

Set when the Key has been created on one KMA in a OKM Cluster. It remains generated until it has been replicated to at least one other KMA in a multi-OKM Cluster. In a Cluster with only a single KMA, the Key remains generated until it has been recorded in at least one backup.

Ready

Set when the Key has been protected against loss by replication or a backup. A ready Key is available for assignment.

Protect and Process

Set when the Key has been assigned when an encryption agent requests a new key be created. A Key in this state can be used for both encryption and decryption.

Process Only

Set when the Key has been assigned but its encryption period has expired. A Key in this state can be used for decryption but not for encryption.

Deactivated

Set when the Key has passed its cryptoperiod but may still be needed to process (decrypt) information.

Compromised

Set when the Key has been released to or discovered by an unauthorized entity. A Key in this state can be used for decryption but not for encryption.

Incompletely Destroyed

Set when the Key has been destroyed but it still appears in at least one backup.

Completely Destroyed

Set when all of the backups in which the destroyed Key appears have been destroyed.

Compromised and Incompletely Destroyed

Set when the compromised Key still appears in at least one backup.

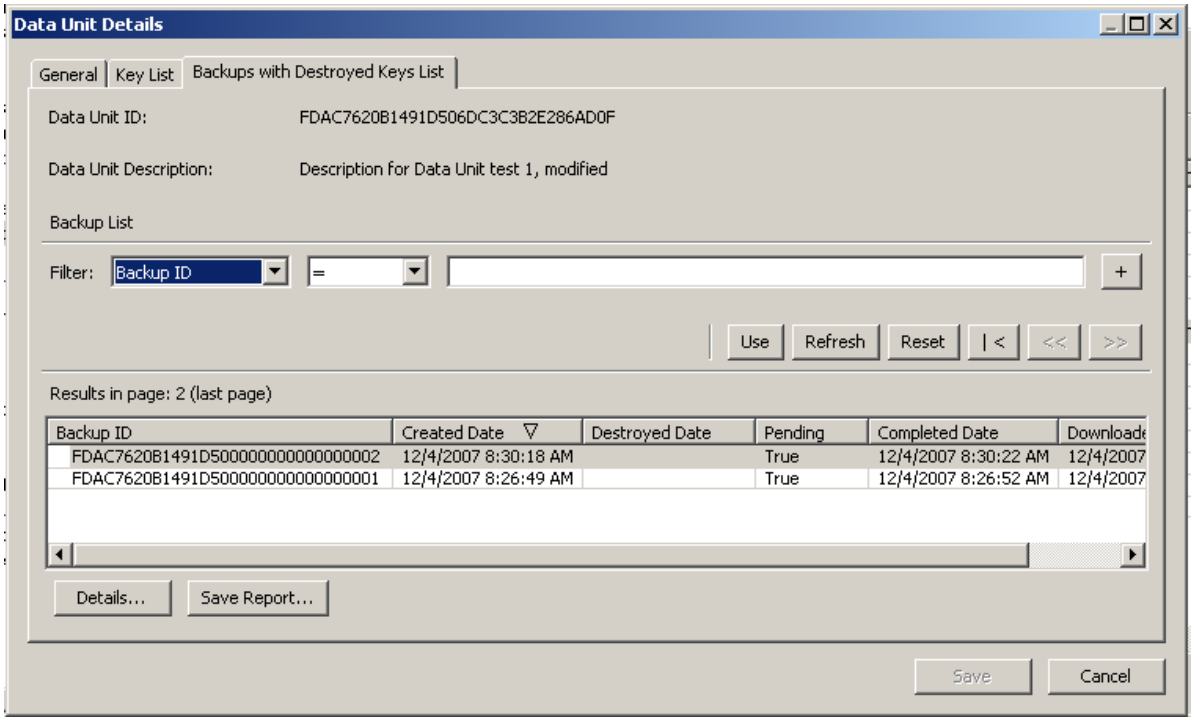
Compromised and Completely Destroyed

Set when all of the backups in which the compromised Key appears have been destroyed.

Recovery Activated

Indicates whether the Key has been linked to the data unit by a recovery action. This condition occurs when a Key is used for a Data Unit by one KMA in a OKM Cluster and then, due to a failure, the Key is later requested for the Data Unit from a different KMA. If the failure (such as a network outage) has prevented the allocation of the Key to the data from being propagated to the second KMA, the second KMA will create the linkage to the data unit. Such a Key is “recovery activated,” and an administrator may want to evaluate the system for KMA or network outages. Possible values are: True and False.

Backups with Destroyed Keys List Tab



A Data Unit cannot be considered "completely destroyed" until all Backups containing the Data Unit Key(s) have been destroyed.

The Backups with Destroyed Keys List tab of the Data Unit Details dialog helps you identify those Backups that contain Data Unit Key(s) for the selected Data Unit and the destruction status of those Backups.

The logic for determining if a Backup does contain a particular Data Unit Key is as follows:

> A Backup contains a Data Unit Key, if the Backup was created after the Data Unit Key was created **and** the Data Unit Key has not been destroyed, or if it has been destroyed **and** its destruction took place after the Backup was created.

However, the date-time comparison needs to take into consideration that the clocks of the various KMAs in a Cluster might not be synchronized automatically (if an NTP server is not specified) and hence may be reporting different times. To account for the possibility of time discrepancies among KMAs, a Backup Time Window is used in the comparison. The Backup Time Window is fixed at five minutes. Using the Backup Time Window, the comparison check behaves as follows:

> A Backup contains a Data Unit Key if the Backup was created within five minutes of the backup creation or later **and** the Data Unit Key was destroyed within five minutes of the Backup creation or later.

The Backup Time Window is used to minimize the likelihood of falsely reporting that a Data Unit does not exist in a particular backup when in fact it does. Such a case is known as a "false negative" and seriously undermines compliance requirements for data destruction. Utilization of the Backup Time Window does, however, increase the

likelihood of falsely reporting that a Data Unit Key does belong in a Backup when in fact it does not. Unlike “false negatives,” “false positives” do not undermine compliance requirements for data destruction.

Data Unit ID

Uniquely identifies the Data Unit.

Data Unit Description

Describes the Data Unit.

Data Unit Destruction Status

Indicates the Destruction status of the Data Unit.

Backup ID

Identifies the backup.

Created Date

Displays when the date and time when the backup file was created (that is, when the backup started).

Destroyed Date

Displays the date and time when the backup file was destroyed.

Pending:

Indicates whether the backup is still pending. Possible values are True or False.

Completed Date:

Displays the date and time when the backup file was completed.

Downloaded Date:

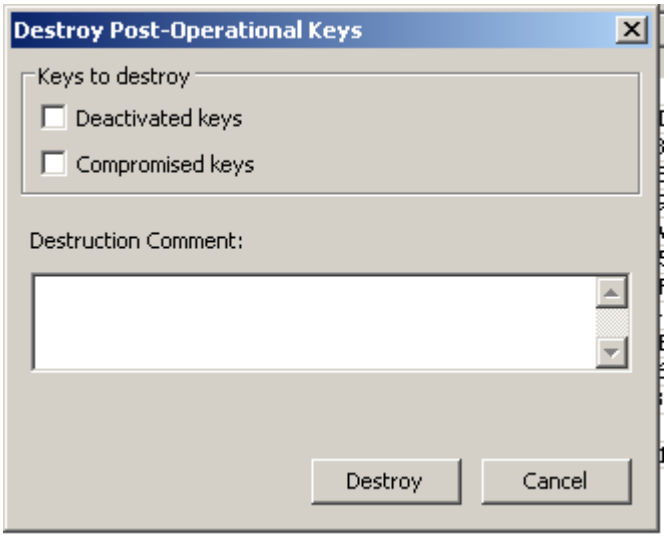
Displays the date and time when the backup file was downloaded.

4. Click the Save button to save your changes.

Destroying Post-operational Keys

To destroy post-operational keys associated with a data unit:

1. From the Data Unit List screen, highlight the Data Unit you want to destroy and click the Destroy Keys button.
2. The following dialog box is displayed, prompting you to specify the keys to destroy.



Deactivated keys

Select this checkbox if you want to destroy the keys that have passed their cryptoperiod but still may be needed to process (decrypt) data information.

Compromised keys

Select this checkbox if you want to destroy the keys that have been released to or discovered by an unauthorized entity.

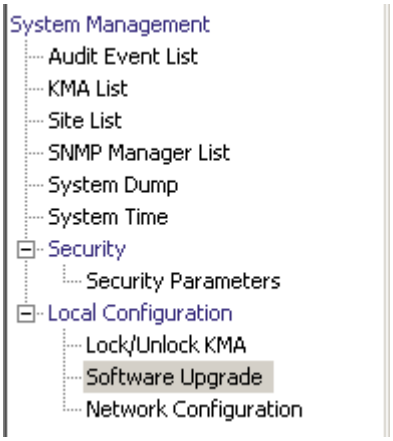
Destruction Comment

Type a comment about the destruction of these keys.

3. If you click the Destroy button, another dialog box is displayed confirming the destruction of these keys.
4. Click the Yes button. Another dialog box is displayed showing the number of Keys that have been destroyed.

Software Upgrade Menu

The Software Upgrade menu option allows the Operator to upload a software upgrade file to the KMA and immediately apply the upgrade. The software updates are signed by Oracle and verified by the KMA before they are applied.



Guidelines for Performing Software Upgrades

- Before you execute this function, back up your system. For procedures, refer to "Creating a Backup" on page 305.
- Use a OKM Manager GUI release that matches the upgrade version you want to load on the KMA(s).
- KMAs running KMS 2.1 or earlier must be upgraded to KMS 2.2 before they can be upgraded to OKM 2.3.
- The upload and apply process can be lengthy if the OKM Manager is remotely connected to the KMA or if the connection between the OKM Manager and KMA is slow. To mitigate this, the software upgrade file can be downloaded to a laptop or workstation that has the OKM Manager installed and the laptop or workstation connected to the same subnet as the KMA. The presence of a router between the OKM Manager and the KMA may slow down the upgrade process.
- The upload and apply processes, with a good connection between the OKM Manager and the KMA, optimally take about 30 minutes. The activate process optimally takes about 5 to 15 minutes. If the uploading process is very slow, try connecting to the same subnet as the KMA.
- Upload and apply the software upgrade file on each KMA one at a time (to help to spread out the network load), and then activate the software upgrade on each KMA one at a time (to minimize the number of KMAs that are offline concurrently).
- If any of the upgrade processes fail (upload, verify, apply, activate, switch replication version), the OKM Manager will generate audit messages describing the reason for the failure and a suggested solution.
- Technical Support accounts will be disabled on the upgraded KMAs and the accounts and will need to be re-enabled if needed.

Uploading and Applying Software Upgrades

To upgrade the KMA:

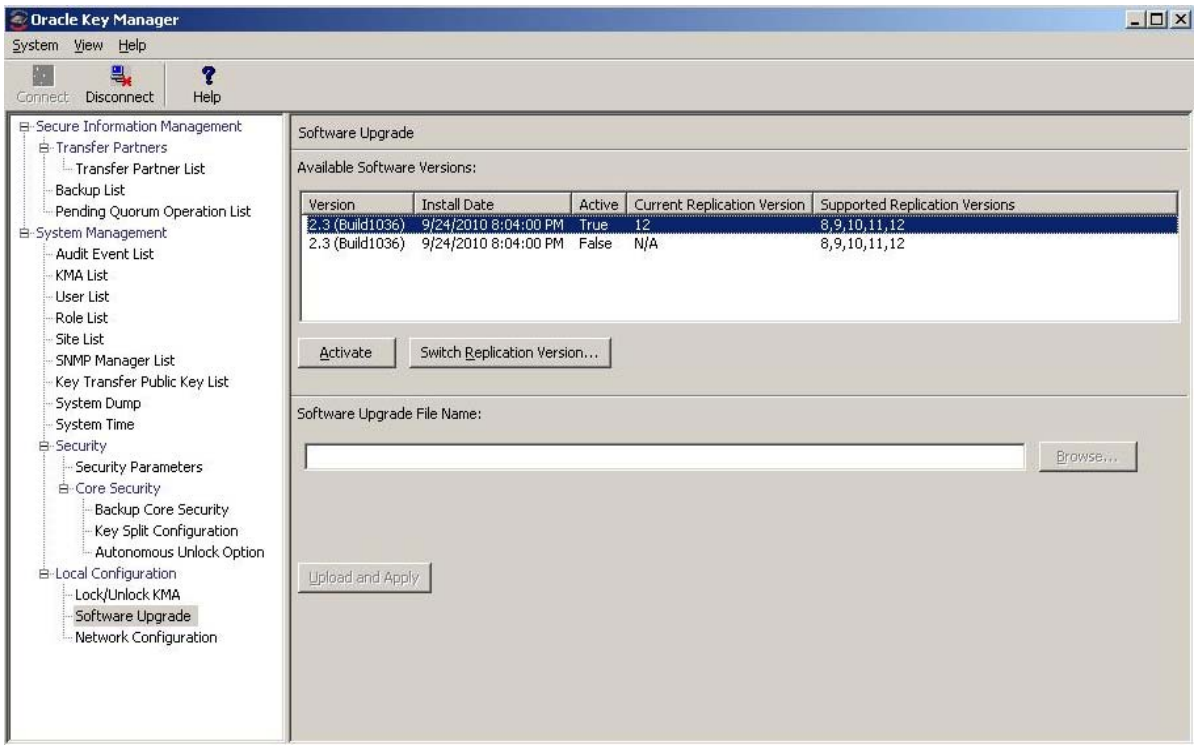
1. Download the software upgrade file to your PC or workstation from the delivery location. The version is visible in the file name.

Note – Save the file to a location where you can navigate from the OKM Manager GUI.

---

2. From the Local Configuration menu, select **Software Upgrade**. The Software Upgrade screen is displayed.

   The active version of the software is highlighted, the **Active** column is set to **True,** and an inactive version is shown.



The buttons appearing on this screen include:

Activate

Select an inactive software version and then click this button to activate the selected software version. Messages are displayed, indicating when this software version is activated and the KMA reboots.

Switch Replication Version

Select the active software version and then click this button to switch the current replication version.

Software Upgrade File Name

Type the name of the software upgrade file.

Browse

Click this button to locate the software upgrade file on your local system.

Upload and Apply

Click this button to begin the upload and apply process. Messages are displayed, indicating when the software upgrade file is uploaded and applied.

3. In the Software Upgrade File Name field, type the name of the software upgrade file. You can also select the Browse button to locate the file. Click the Upload and Apply button.

   The OKM starts the upload, verify, and apply process and displays a progress indicator showing which step the process is at.

Note – Since the upload process adds some traffic to the network, you may not want to upload KMAs simultaneously in a busy Cluster.

---

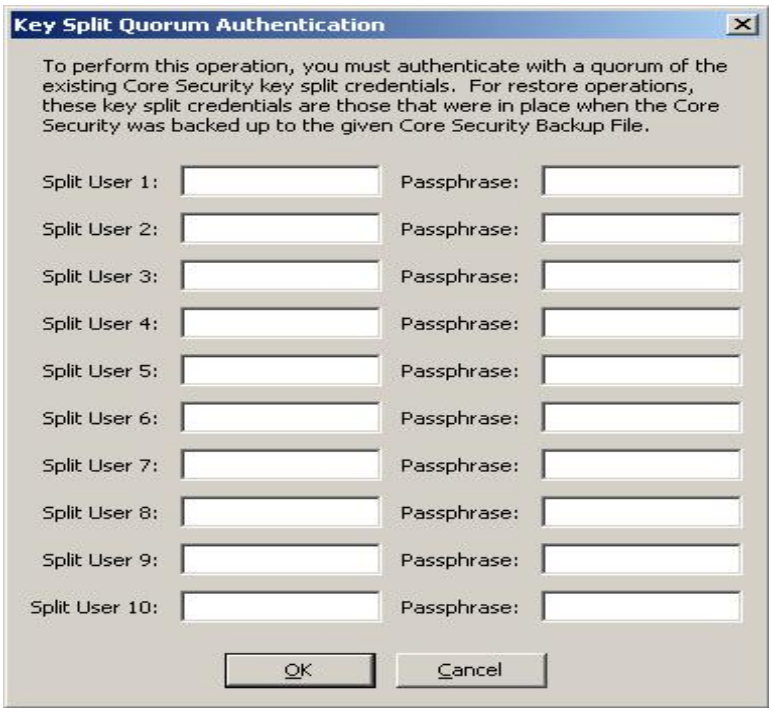
4. Make sure there is a current backup of the OKM Cluster.

   To activate the upgrade file, select the new version from the list of available versions at the top of the screen and click the **Activate** button. Until activated, the new version will remain inactive on the system.

Note – The KMA reboots as part of the activate process. Since the KMA is offline while it reboots, you may not want to activate KMAs simultaneously in a Cluster.

   Users remain connected until you reboot the KMA. When you access the Software Upgrade screen again, the new uploaded software version is shown as the active version.

5. The Key Split Quorum Authentication dialog box is displayed. The quorum must type their user names and passphrases to authenticate the operation.



If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

The new software version may include new features available only when the OKM Cluster replication version is changed to a higher value. The OKM Cluster must be switched to the new replication version to enable all new features in the new software version.

6. Log in to a KMA that has been activated and navigate to the Software Upgrade screen. If the **Supported Replication Versions** column includes a higher version than the **Current Replication Version** column, click the **Switch Replication Version** button.

   The **Current Replication Version** will now display the higher version, and the successful replication switch is sent to all other KMAs in the OKM Cluster.

Backup List Menu

For procedures on viewing a Backup file's detailed information, refer to "Backup List Menu" on page 301.

Audit Event List Menu

For procedures to view an audit event list, refer to "Audit Event List Menu" on page 255.

KMA List Menu

For procedures to view the list of KMAs, refer to "KMA List Menu" on page 103.

Site List Menu

For procedures to view a list of sites, refer to "Site List Menu" on page 135.

SNMP Manager List Menu

For procedures to view the list of SNMP managers, refer to "SNMP Manager List Menu" on page 143.

System Time Menu

For procedures on viewing the KMA's time, refer to "System Time Menu" on page 210.

Lock/Unlock KMA Menu

For procedures on viewing the KMA locking status, refer to "Lock/Unlock KMA" on page 204.

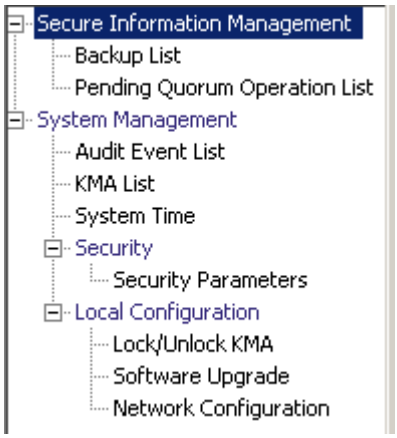
CHAPTER 8

Backup Operator Operations

This chapter describes the operations that a user who has been given a Backup Operator role can perform. If you have been assigned other roles, refer to the appropriate chapter for instructions on performing the specific role.

Backup Operator Role

As the Backup Operator, you are responsible for securing and storing data and their keys.



Backup List Menu

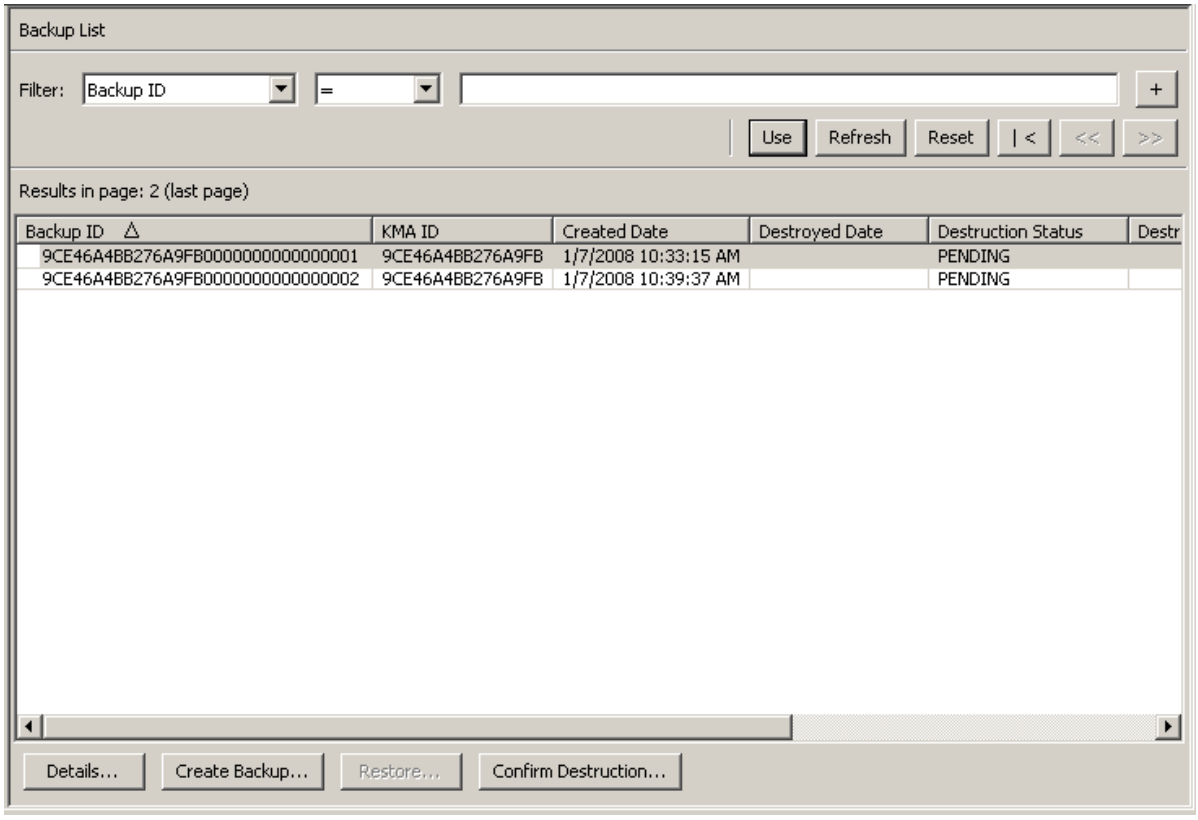
The Backups List menu option allows the Backup Operator to:

- View the history of the Backups and confirm their destruction status
- Create Backups.

Viewing Backup Files History

To view Backup files history:

From the Backups menu, select **Backup List**. The Backup List screen is displayed.



If you want more detailed information on a Backup, highlight the Backup and click the Details button. For more information, refer to "Viewing Backup Details".

Click the Create Backup button to create a Backup. For more information, refer to "Creating a Backup" on page 305.

Click the Confirm Destruction button to confirm the destruction of a Backup. For more information, refer to "Confirming a Backup's Destruction" on page 306.

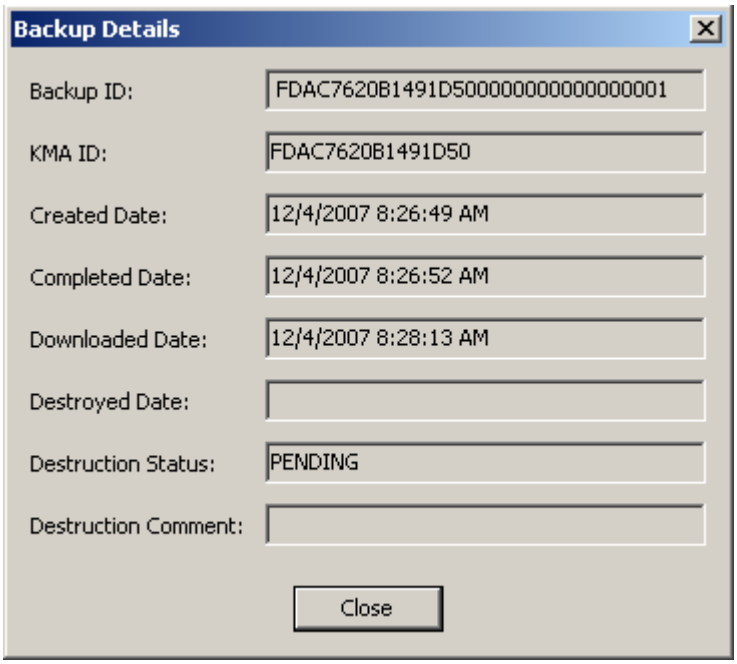
Viewing Backup Details

The Backup Details dialog box is used to view the details of a Backup file.

Note – Backup files are downloaded to the machine where the OKM Manager is running when the backup is created.

To view the details of a Backup file:

1. From the Backups List screen, double-click the Backup entry for which you want more information or highlight the Backup entry and click the Details button. The Backup Details dialog box is displayed, with all fields disabled.



2. The fields and their descriptions are given below:

Backup ID

Displays a system-generated unique identifier that distinguishes each Backup file.

KMA ID

Displays the KMA on which this Backup file is generated.

Created Date

Displays the date and time when the Backup file was created.

Completed Date

Displays the date and time when the Backup file was completed.

Downloaded Date

Displays the date and time the Backup file was downloaded.

Destroyed Date

Displays the date when the Backup file was destroyed.

Destruction Status

Indicates the status of the backup with respect to its destruction.

Destruction Comment

Displays user-supplied information on the Backup file's destruction.

3. Click the Close button to close this dialog box.

Creating a Backup

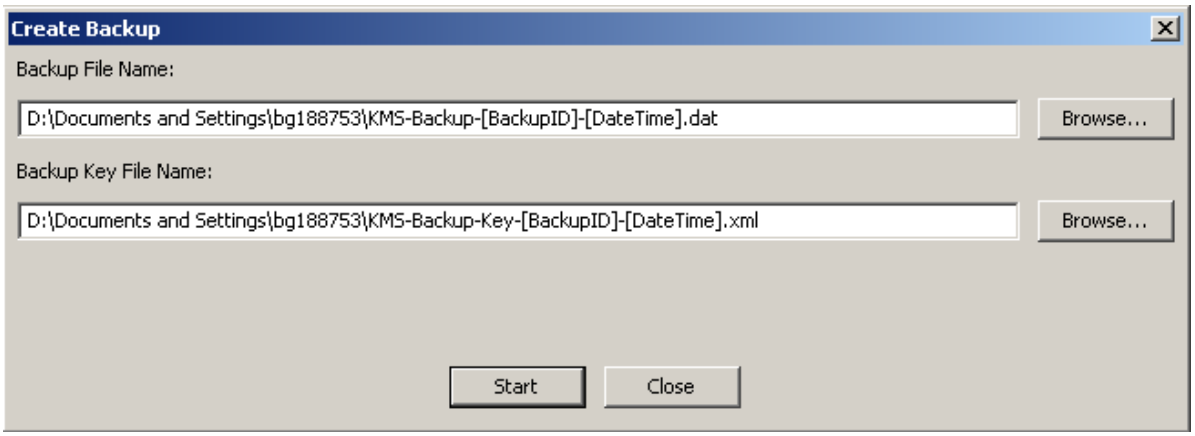
Important – The Security Officer must back up Core Security Key material before the Backup Officer can create a backup. See "Creating a Core Security Backup" on page 195.

At any given time, there is only one Backup file and one Restore file on a KMA.

This option gives you the ability to create a Backup that consists of two files: a Backup file and a Backup key file.

To create a Backup:

1. From the Backup List screen, click the Create Backup button. The Create Backup dialog box is displayed.



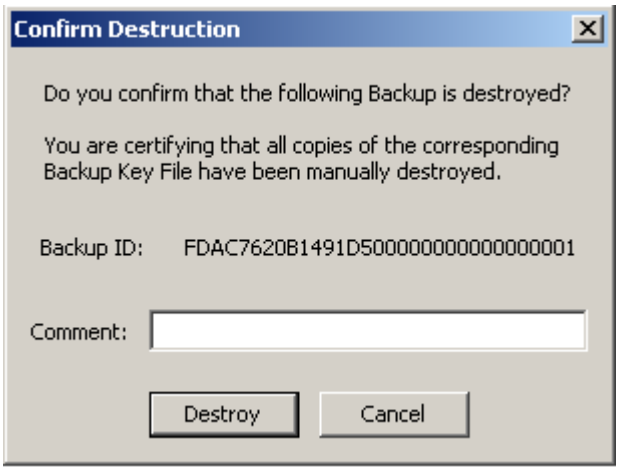
Note – Backup File and Backup Key File names are automatically generated. You can, however, edit the names. You can also click the Browse button to select a destination path.

2. Click the Start button to create the Backup file and download the Backup key file to the user-specified destination.
3. When the Backup is completed, a message indicating this is displayed. Click the Close button to close this dialog box.
4. You are returned to the Backup List screen, where the new created Backup File is displayed.

Confirming a Backup's Destruction

To confirm a backup's destruction:

1. From the Backup List screen, highlight the Backup you want to destroy and click the Confirm Destruction button. The following dialog box is displayed, confirming that you want to update the destruction status for the selected Backup. Before proceeding, ensure that all copies of the corresponding Backup Key file have been manually destroyed.



2. If you are certain that all copies of the corresponding backup key file have been manually destroyed, click the Yes button. Otherwise, click the No button to stop the process.
3. If you chose the Yes button, the backup and the Data Units that were associated with it are 'completely destroyed'.

KMA List Menu

The KMA List menu option allows you to:

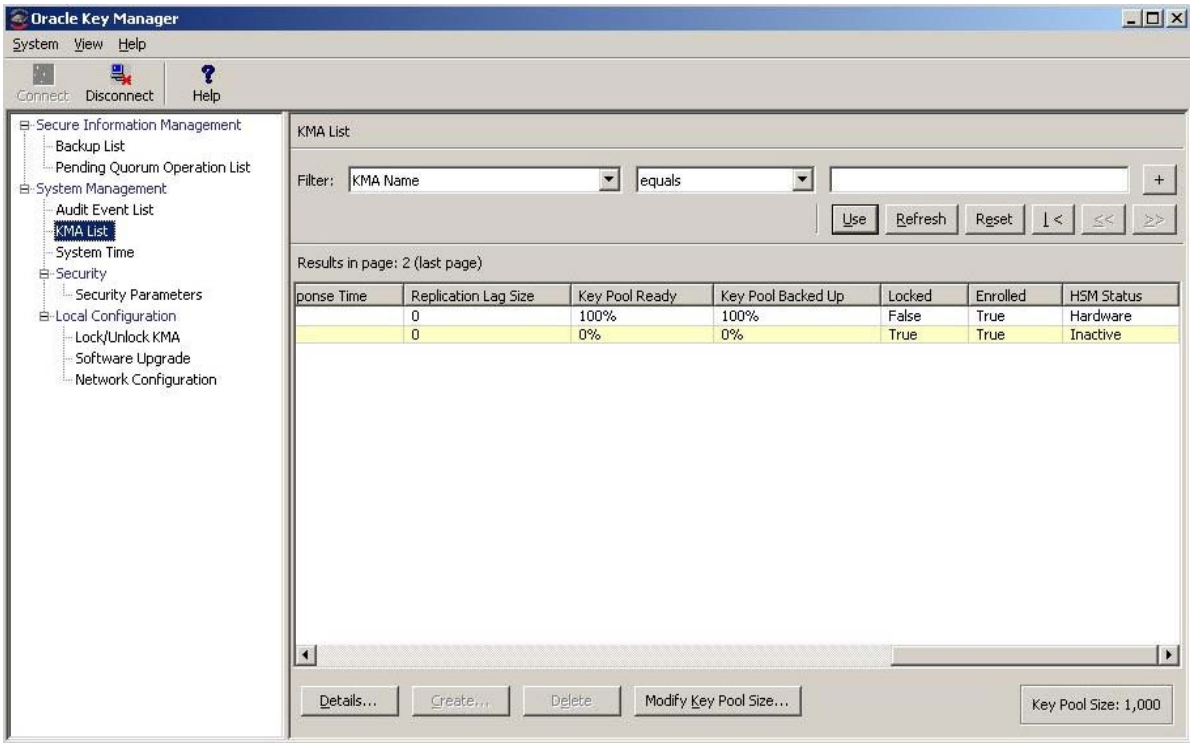
- View KMAs (refer to "Viewing KMAs" on page 104)
- Create a KMA (refer to "Creating a KMA" on page 109)
- Modify a KMA's information (refer to "Viewing/Modifying a KMA's Details" on page 112)
- Delete a KMA (refer to "Deleting a KMA" on page 117)
- Modify a Key Pool size.

Note – Backup Operators can view KMA details and modify Key Pool sizes.

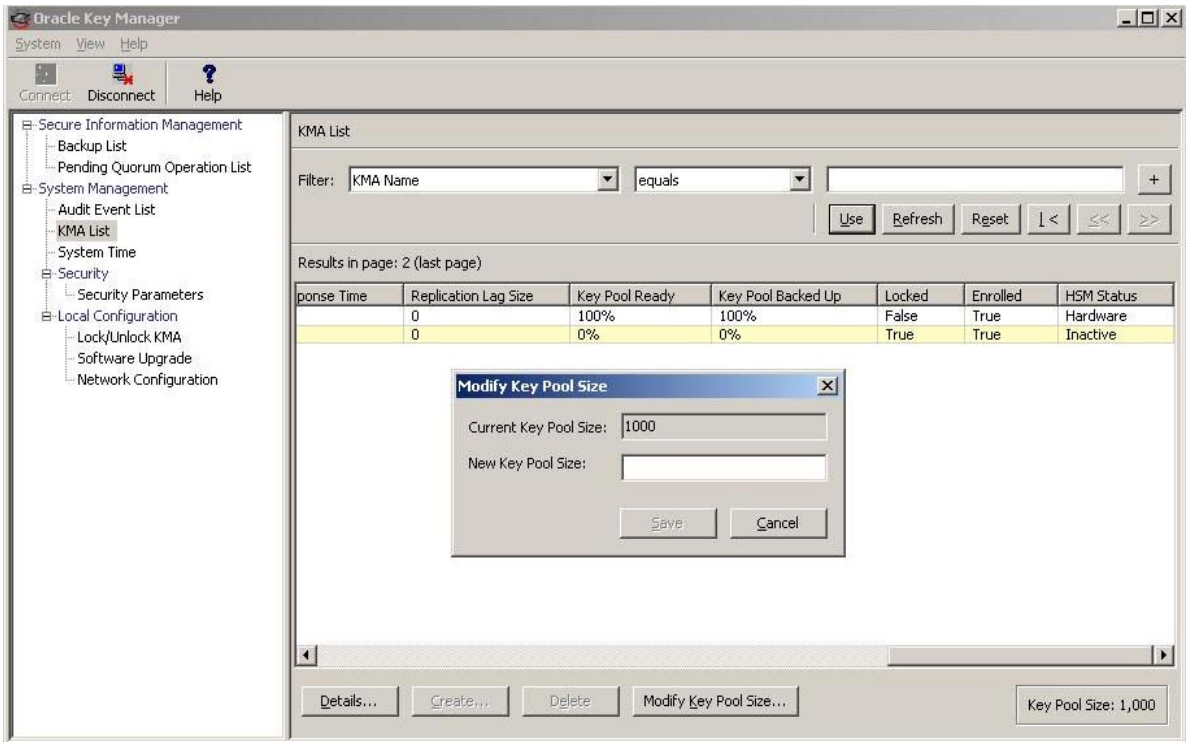
Modifying a Key Pool Size

To modify a Key Pool size:

1. From the System Management menu, select KMA List. The right side of the KMA List screen is displayed below.



2. Click **Modify Key Pool Size**. The following screen is displayed.



3. Supply the new Key Pool size.

Other Functions

A Backup Operator can also:

- View Audit Event List
- View the System time
- View the KMA locking status.

For procedures on viewing the Audit Log, refer to "Audit Event List Menu" on page 255.

For procedures on viewing the KMA's time, refer to "System Time Menu" on page 210.

For procedures on viewing the KMA locking status, refer to "Lock/Unlock KMA" on page 204.

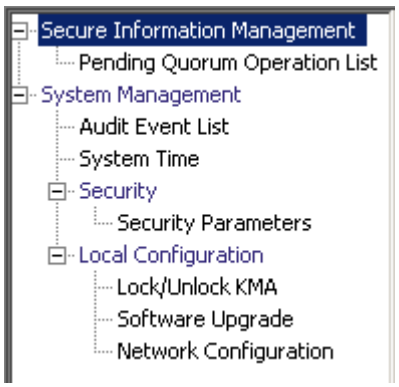
CHAPTER 9

Auditor Operations

This chapter describes the operations that a user who has been given an Auditor role can perform. If you have been assigned other roles, refer to the appropriate chapter for instructions on performing the specific role.

Auditor Role

As the Auditor, you can view the Audit List events and the KMA.



Audit List Menu

For procedures on using the Audit List menu, refer to "Audit Event List Menu" on page 255.

Security Parameters Menu

The Security Parameters List menu gives the Auditor the ability to view the KMA's security parameters. For procedures on using the Security Parameters menu, refer to "Security Parameters Menu" on page 188.

Other Functions

An Auditor can also:

- View the Lock/Unlock the KMA status.
- View the system time.

For procedures on viewing the lock/unlock KMA status, refer to "Lock/Unlock KMA" on page 204.

For procedures on adjusting the KMA's time, refer to "System Time Menu" on page 210.

For procedures on viewing the installed software versions, refer to "Software Upgrade Menu" on page 294.

CHAPTER 10

Quorum Member Operations

This chapter describes the operations that a user who has been given a Quorum Member role can perform. If you have been assigned other roles, refer to the appropriate chapter for instructions on performing the specific role.

Quorum Member Role

The Quorum Member Role views and approves pending quorum operations.

A user who has been assigned the Security Operator role must first log into the OKM Manager GUI, create one or more users, and assign them the Quorum Member role (see "Creating a User" on page 122).

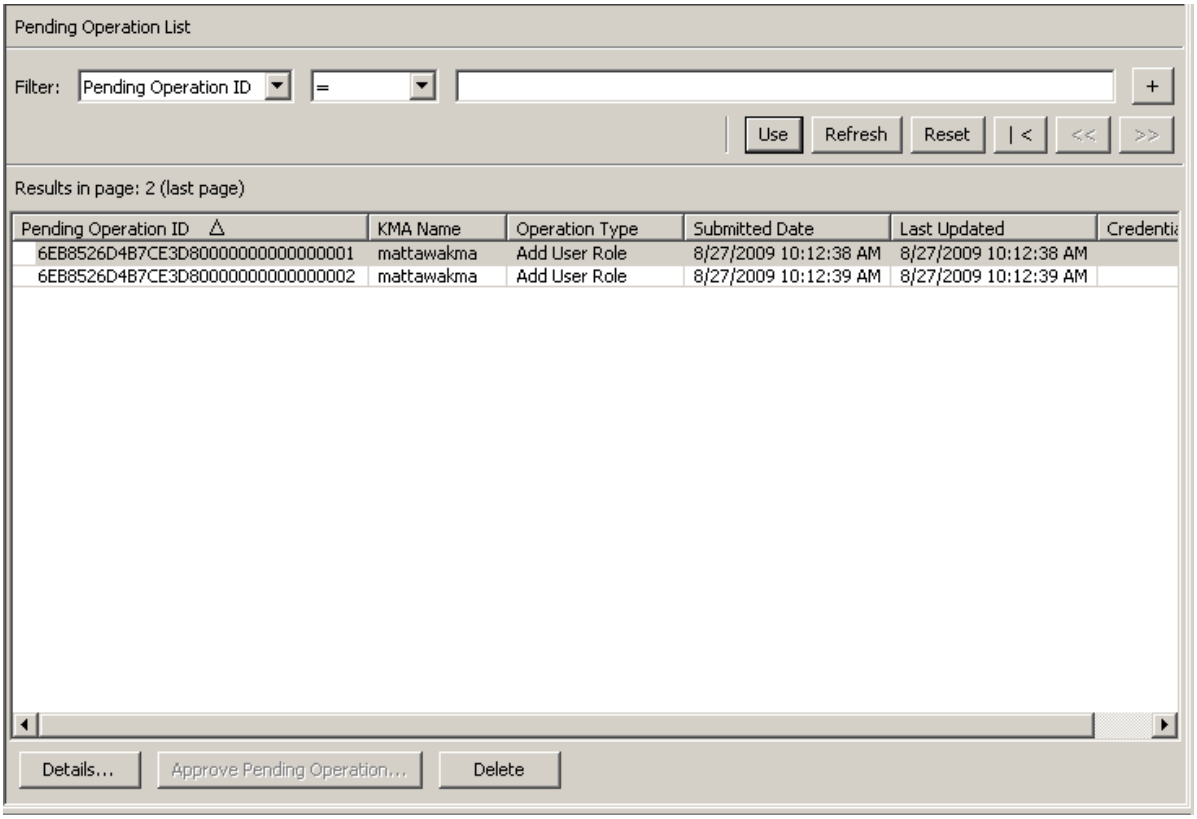
When you create a user with the Quorum Member role, the Security Officer must provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog, since not all Quorum Member Users have been created yet.

Pending Quorum Operation List Menu

The Pending Quorum Operation List menu shows any pending operations that require the approval of a quorum of Key Split Credentials before the system performs them. This menu appears when the user has the Quorum Member or Security Officer role.

The Pending Quorum Operation List menu includes the following options:

- View the Pending Operation list details
- Approve a pending operation
- Delete a pending operation.



You can filter the Pending Operations lists by any of the following keys:

- Pending Operation ID
- KMA Name
- Operation Type
- Submitted Date
- Last Updated.

The **Use** button applies the filter to the displayed list for the pending operation.

The fields and their descriptions are given below:

Filter:

Displays the fields that you can use to filter the results of queries made to the KMA. Possible values are:

- Pending Operation ID
- KMA Name
- Operation Type
- Submitted Date
- Last Updated

Filter Operator box:

Click the down-arrow and select the filter operation you want. Possible values are:

- Equals =
- Not equal <>
- Greater than >
- Less than <
- Greater than or equals >=
- Less than or equals <=
- Starts with ~
- Empty
- Not empty

Filter Value text box:

Type a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Filter Value combo box:

Click the down-arrow and select a value to filter the selected attribute by. This filter option is not displayed for all filter attributes.

Click this button to add additional filters.

Click this button to remove a filter. This button is only displayed if there is more than one filter shown.

Use:

Click this button to apply the selected filters to the displayed list and go to the first page.

Refresh:

Click this button to refresh the list.

Reset:

Click this button to remove all filters and reset the displayed list to the first page.

Click this button to go to the first page of the list.

Click this button to go to the previous page.

Click this button to go to the next page.

Results in Page:

Displays the number of records per page that were configured in the Query Page Size field in the Options dialog box.

Pending Operation ID:

Uniquely identifies the pending quorum operation..

KMA Name:

The name of the KMA from which this operation was submitted.

Operation Type:

The type of quorum operation.

Submitted Date:

The date when the pending quorum operation was submitted.

Last Updated:

The date when the quorum was last updated on this operation. The quorum on a particular pending quorum operation is updated whenever another Quorum Member provides key split user names to approve it. The pending quorum operation expires when not enough key split users approve this operation within the Pending Operation Credentials Lifetime. This date is initially set to be the same as the submitted date when the pending quorum operation is submitted.

Credentials:

A list of key split user names that have already approved this pending quorum operation.

Details:

Click this button to view detailed information about a pending quorum operation.

Approve Pending Operation:

Click this button to approve a pending quorum operation. You must be in the Quorum Member role to do this.

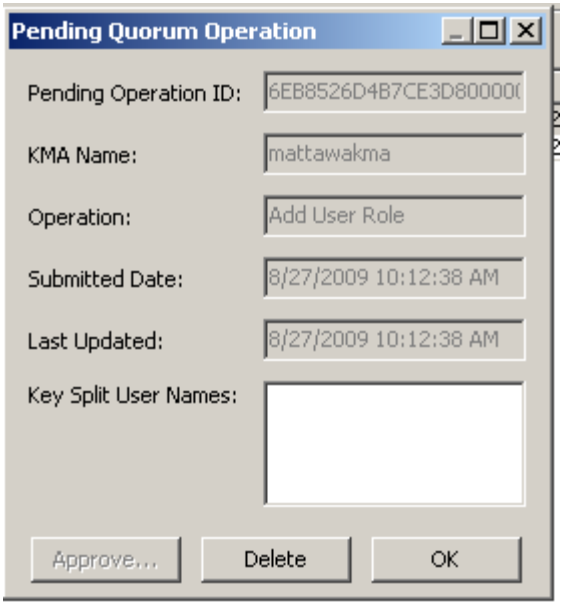
Delete:

Click this button to delete a selected pending quorum operation. You must be in the Security Officer role to do this.

Viewing Pending Operations Details

To view pending operations details:

From the Pending Operation List screen, click the Details button. The Pending Quorum Operation dialog box is displayed.



The Key Split User Names field lists Key Split Users, if any, who have already approved this operation.

To get more information about this particular pending quorum operation, you can filter audit events displayed in the Audit Event List panel (see "Viewing Audit Logs" on page 256).

1. Navigate to the Audit Event List panel.
2. Define a filter with Operation filter set to Add Pending Quorum Operation. If you have several pending quorum operations, you may want to define another filter with Created Date specifying a time period around the Submitted Date of this particular pending quorum operation.
3. Click the Use button to display those audit events that match this filter. The Message Values field of the filtered audit event should contain more information about the pending quorum operation.

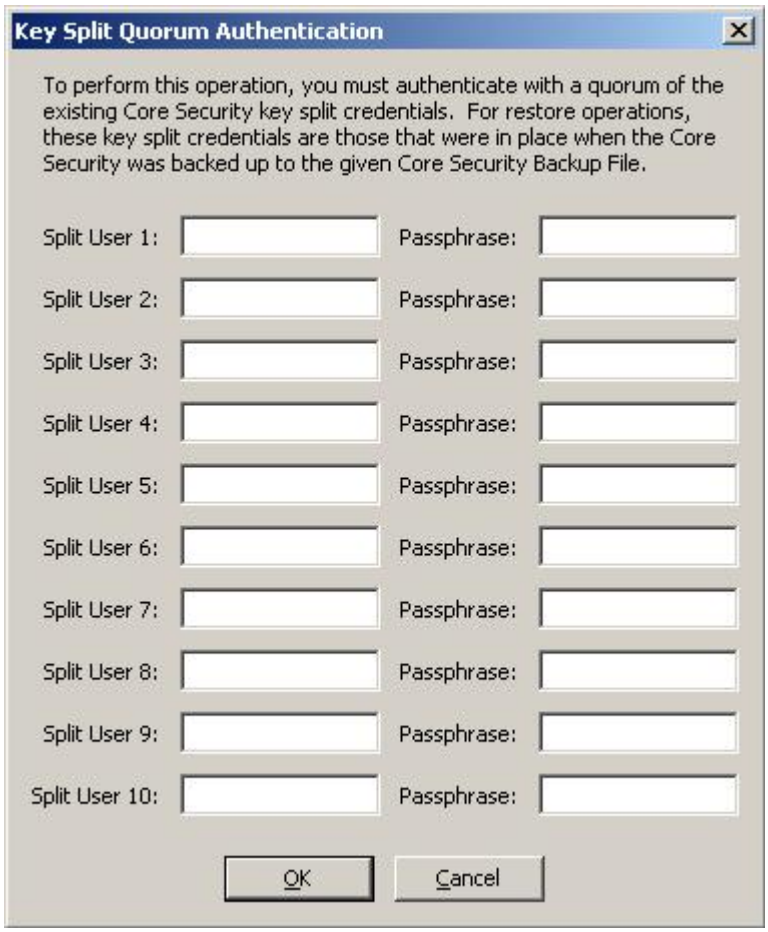
Approving Pending Quorum Operations

To approve a pending operation, you must log into the OKM Manager GUI in the Quorum Member role; otherwise, the Approve button is disabled.

Other users who have the Quorum Member role can also log in separately and approve a pending quorum operation. When a sufficient quorum of Key Split Credentials approves the pending quorum operation, then the OKM Cluster performs the operation.

To approve pending quorum operations:

1. From the Pending Operation List screen, click the Approve Pending Operation button.
2. The Key Split Quorum Authentication dialog box is displayed.



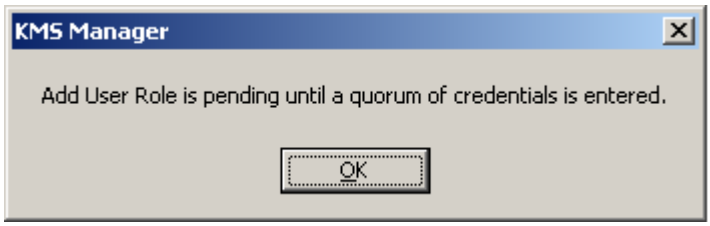
If you provide a sufficient quorum of Key Split Credentials in the Key Split Quorum Authentication dialog box, then information is updated in the OKM Cluster after you provide a quorum, not when you click the Save button.

If you do not provide a sufficient quorum in the Key Split Quorum Authentication dialog box, two different outcomes can occur depending on the replication version:

Replication Version:	Result:
10 or lower	The operation fails and no information is updated in the OKM Cluster.
11 or higher	The operation becomes pending. That is, the system adds the operation to a list of pending quorum operations (see "Pending Quorum Operation List Menu" on page 314). A popup message appears when the operation is added to this list. No information is updated in the OKM Cluster until users with the Quorum Member role (Quorum Member users) log in and provide a sufficient quorum.

3. Enter the quorum user names and passphrases to authenticate the operation.

   If you do not immediately provide a sufficient quorum of Key Split Credentials, the system adds the operation to a list of pending quorum operations and generates the following dialog box:



When you click OK, you then see this operation in the Pending Quorum Operation List screen (refer to the sample screen shown on page 314).

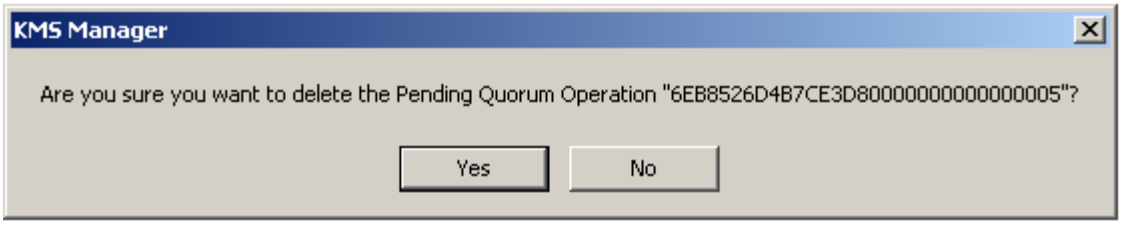
Deleting Pending Quorum Operations

To delete a pending operation, you must log into the OKM Manager GUI in the Security Officer role; otherwise, the Delete button is disabled.

To delete pending operations:

1. From the Pending Operation List screen, highlight the pending operation you want to delete and click the Delete button.

   The following dialog box is displayed, prompting you to confirm that you want to delete the selected pending operation.



2. Click the Yes button to delete the pending operation. The currently selected pending operation is deleted and you are returned to the Pending Operation List screen. The system also removes any entries that are associated with the pending operation.

Related Operations

The following operations require a quorum of Key Split Credentials:

- “Creating a KMA” on page 109
- “Setting a KMA Passphrase” on page 115
- “Creating a User” on page 122
- “Viewing/Modifying a User’s Details” on page 125
- “Setting a User’s Passphrase” on page 128
- “Creating a Transfer Partner” on page 161
- “Viewing/Modifying Transfer Partner Details” on page 165
- “Restoring a Backup” on page 182
- “Autonomous Unlock Option” on page 201
- “Lock/Unlock KMA” on page 204
- “Uploading and Applying Software Upgrades” on page 295.

CHAPTER 11

Using the OKM Console

This chapter describes the options in the OKM Console.

What is the OKM Console?

The OKM Console is a terminal text-based interface that allows you to configure basic functions of the KMA. It is accessed by physically connecting a video monitor and keyboard to the KMA or by the "remote console" function in the ELOM web browser interface (see "Accessing the KMA Through the Service Processor" on page 22).

The OKM Console is automatically launched by the operating system when the KMA boots up and cannot be terminated by a user. Depending on the roles that a user is assigned, the options in the OKM Console differ.

Before you can login to the OKM Console, the user accounts must be created in the OKM Manager. You must use the same user name/passphrase that was used for authentication in the OKM to login to the OKM Console.

Note – Only the first Security Officer account is created when the QuickStart program is launched.

Logging into the KMA

After the KMA boots up, the following information is displayed.

```
Copyright (c) 2007, 2010, Oracle and/or its affiliates. All rights
reserved.
Oracle Key Manager Version 2.3 (Build1036)
------------------------------------------------------------
Please enter your User ID:
```

1. At the prompt, type your user name and press **<Enter>**.
2. At the `Please enter your Passphrase:` prompt, type your passphrase and press **<Enter>**. Depending on the role(s) the user is assigned, the options on the OKM Console differ. The menu shows the version of the KMA and the logged on user.

User role operations are discussed on the following pages. They include:

- Operator (see "Operator Role Functions" on page 328)
- Security Officer (see "Security Officer Role Functions" on page 334)
- Other Roles (see "Other Role Functions" on page 356).

Operator

The following menu illustrates the options for an Operator role.

```
Oracle Key Manager Version 2.3 (Build1036) -- OP on glenkenchiekma
------------------------------------------------------------
Please enter your User ID: OP

Please enter your Passphrase:

Oracle Key Manager Version 2.3 (Build1036) -- )OP on glenkenchiekma

------------------------------------------------------------

(1)  Reboot KMA
(2)  Shutdown KMA
(3)  Technical Support
(4)  Primary Administrator
(5)  Set Keyboard Layout
(0)  Logout
------------------------------------------------------------
Please enter your choice:
```

Security Officer

The following menu illustrates the options for an Security Officer role.

```
Oracle Key Manager Version 2.3 (Build1036) -- SO on glenkinchiekma
------------------------------------------------------------
Please enter your User ID: SO

Please enter your Passphrase:

Oracle Key Manager Version 2.3 (Build1036) -- SO on glenkinchiekma
------------------------------------------------------------

(1)     Log KMA Back into Cluster
(2)     Set User's Passphrase
(3)     Set KMA Management IP Addresses
(4)     Set KMA Service IP Addresses
(5)     Modify Gateway Settings
(6)     Set DNS Settings
(7)     Reset to Factory Default State
(8)     Technical Support
(9)     Primary Administrator
(10)    Set Keyboard Layout
(0)     Logout
------------------------------------------------------------
Please enter your choice:
```

Note – If the user has been assigned both Operator and Security roles, then the menu options are combined as follows:

```
Oracle Key Manager Version 2.3 (Build1036) -- glenkinchiekma
------------------------------------------------------------
Please enter your User ID:

Please enter your Passphrase:

Oracle Key Manager Version 2.3 (Build1036) -- glenkinchiekma
------------------------------------------------------------

(1)     Log KMA Back into Cluster
(2)     Set User's Passphrase
(3)     Set KMA Management IP Addresses
(4)     Set KMA Service IP Addresses
(5)     Modify Gateway Settings
(6)     Set DNS Settings
(7)     Reset to Factory Default State
(8)     Technical Support
(9)     Primary Administrator
(10)    Set Keyboard Layout
(0)     Logout
------------------------------------------------------------
Please enter your choice:
```

Other Roles

For all other roles, that is, Backup Operator, Compliance Officer, Auditor, and Quorum Member, a menu that is similar to the following is displayed. The only options available are to logout from the KMA and to set the keyboard layout.

```
Oracle Key Manager Version 2.3 (Build1036) -- glenkinchiekma
------------------------------------------------------------

(1)  Set Keyboard Layout
(0)  Logout

------------------------------------------------------------
Please enter your choice:
```

Operator Role Functions

This section describes the functions that an Operator can perform. They are:

- Rebooting the KMA (page 329)
- Shutting down the KMA (page 329)
- Disabling Technical Support (page 330)
- Disabling the Primary Administrator (page 331)
- Setting the keyboard layout (page 332)
- Logging out of the KMA (page 333).

The Operator's menu is shown below.

```
Oracle Key Manager Version 2.3 (Build 1036) - OP on Glenkinchiekma)
------------------------------------------------------------
Please enter your User ID: OP

Please enter your Passphrase:

Oracle Key Manager Version 2.3 (Build 1036) - OP on Glenkinchiekma)

------------------------------------------------------------

(1)  Reboot KMA
(2)  Shutdown KMA
(3)  Technical Support
(4)  Primary Administrator
(5)  Set Keyboard Layout
(0)  Logout
------------------------------------------------------------
Please enter your choice:
```

Note – The Technical Support and Primary Administrator menu items appear only when their settings are currently enabled.

Rebooting the KMA

The Reboot KMA menu option allows an operator to stop and restart the KMA and reboot the operating system. This function is for troubleshooting purposes only.

To reboot the KMA:

1. At the `Please enter your choice:` prompt on the main menu, type **1** and press <Enter>. The following information is displayed, indicating that the support account is enabled.

```
Reboot KMA
------------------------------------------------------------
Press Ctrl-c to abort.
Are you sure that you want to reboot the KMA? [y/n]:
```

2. At the prompt, type **y** and press <Enter>. The current OKM Console session terminates as the KMA starts to reboot. After the KMA reboots, the OKM Console login prompt is displayed.

Shutting Down the KMA

This option allows you to terminate (shut down) all services on the KMA and to physically shut down the KMA itself.

To shut down the KMA:

1. At the `Please enter your choice:` prompt on the main menu, type **2** and press <Enter>. The following information is displayed, indicating that the support account is enabled.

```
Shutdown KMA
------------------------------------------------------------
Press Ctrl-c to abort
Are you sure that you want to shut down the KMA? [y/n]:
```

2. At the prompt, type **y** and press <Enter>. The following information is displayed, indicating that the system is shutting down.

```
Shutting down...
```

3. The shutdown sequence is displayed. When it is finished, the following information is displayed.

```
Power down.
```

4. The KMA is now powered off. The KMA can be powered on using either the power button or the ELOM remote power control function.

Disabling the Technical Support Account

Note – This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

To disable the Technical Support account:

1. At the `Please enter your choice:` prompt on the main menu, type **3** and press <Enter>. The following information is displayed, indicating that the support account is enabled.

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.

The support account is currently ENABLED.

Would you like to DISABLE the support account? [y/n]:
```

2. At the prompt, type **y** to disable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to DISABLE the support account? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The SSH service automatically stops.

Disabling the Primary Administrator

The Primary Administrator menu option allows you to enable/disable Primary Administrator access on the KMA.

Note – This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

Disabling Primary Administrator access takes place immediately. If someone is connected as a Primary Administrator, and then this access is disabled, the next command they attempt will fail.

1. To disable Primary Administrator access:

At the `Please enter your choice:` prompt on the main menu, type **4** and press <Enter>. The following information is displayed, indicating that the access is enabled.

```
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. At the prompt, type **y** to disable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The Primary Administrator access has been disabled.

Setting the Keyboard Layout

This option allows you to change the keyboard layout from English to a variety of languages.

Note – The keyboard layout should be set to match the layout of the keyboard attached to the KMA in order for the KMA to correctly interpret key presses.

To set the keyboard layout:

1. At the `Please enter your choice:` prompt on the main menu, type **5** and press <Enter>. The following keyboard layouts are displayed.

```
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. At the `Please enter the number for the keyboard layout:` prompt, enter the number you want to change the keyboard layout to. The new keyboard layout is applied.
3. The following information is displayed. `Press <Enter> to continue.`

Logging Out

To log out of the current OKM Console session:

1. At the `Please enter your choice:` prompt on the main menu, type **0** and press <Enter>.
2. The current session terminates and the login prompt is displayed allowing the user to re-enter the OKM Console.

Security Officer Role Functions

This section describes the functions that a Security Officer can perform. They are:

- Logging the KMA into the Cluster (page 335)
- Setting a User's Passphrase (page 337)
- Setting the KMA Management IP addresses (page 339)
- Setting the KMA Service IP addresses (page 341)
- Modifying the Gateway settings (page 343)
- Specifying the DNS settings (page 345)
- Resetting the KMA to the Factory Default State (page 346)
- Enabling/Disabling Technical Support (page 348)
- Enabling/Disabling the Primary Administrator (page 351)
- Setting the keyboard layout (page 354)
- Logging out of the KMA (page 355).

The Security Officer's menu is shown below.

```
Oracle Key Manager Version 2.3 (Build1036) - SO on glenkinchiekma
------------------------------------------------------------
Please enter your User ID: SO

Please enter your Passphrase:

Oracle Key Manager Version 2.3 (Build1036) - SO on glenkinchiekma
------------------------------------------------------------

(1)     Log KMA Back into Cluster
(2)     Set User's Passphrase
(3)     Set KMA Management IP Addresses
(4)     Set KMA Service IP Addresses
(5)     Modify Gateway Settings
(6)     Set DNS Settings
(7)     Reset to Factory Default State
(8)     Technical Support
(9)     Primary Administrator
(10)    Set Keyboard Layout
(0)     Logout
------------------------------------------------------------
Please enter your choice:
```

Logging the KMA Back into the Cluster

This menu option allows a Security Officer to log the KMA back into the Cluster after its passphrase has been changed. Before you can perform this task:

1. Bring up the OKM Manager.
2. Log in to an existing KMA as a Security Officer.
3. Navigate to the KMA List panel.
4. Create a KMA entry.

To log the KMA into the Cluster:

1. At the `Please enter your choice:` prompt on the main menu, type **1** and press <Enter>. The following information is displayed.

```
Log KMA Back 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. Log in to an existing KMA (for example, 129.80.60.172) as a Security Officer.
3. At the prompt, type the passphrase that was originally configured for the KMA, to join the Cluster and press <Enter>.

```
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. Enter the first Key Split user name established during QuickStart for the first KMA in the OKM Manager Modify Key Split Credentials function (refer to "Modifying the Key Split Configuration" on page 198).

Note – The Security Officer needs to know how many Key Split users to enter, that is, what the Key Split Threshold is. In this example, the Key Split Threshold is 2.

---

5. Type the passphrase for the Key Split user, and press <Enter>.

```
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. Enter the second Key Split user name.
7. Type the passphrase for the Key Split user, and press <Enter>

```
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. Press <Enter> next to Key Split User Name #3 to end Key Split user authorization.
9. Type **n**, and press <Enter>.

Setting a User's Passphrase

This menu option allows a Security Officer to set the passphrase for any user, including the Security Officer.

To set a user's passphrase:

1. At the `Please enter your choice:` prompt on the main menu, type **2** and press <Enter>. The following information is displayed.

```
Set User's Passphrase
-------------------------------------------------------------
Press Ctrl-c to abort.
Please enter the User Name:
```

2. At the prompt, type the name of the user and press <Enter>. The following information is displayed.

```
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. At the prompt, type the passphrase and press <Enter>.
4. At the `Please re-enter the desired Passphrase:` prompt, type the same passphrase and press <Enter>. The following information is displayed, indicating that the passphrase is set.

   ```
   Press Enter to continue:
   ```

If you tried to change the passphrase of another user, the following information is displayed:

```
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:
```

5. Enter the first Key Split user name and press <Enter>.

```
Please enter Key Split Passphrase #1:

Press Enter to continue:
```

6. Enter the first Key Split passphrase and press <Enter>.
7. Repeat Steps 5 and 6 until you have entered a sufficient number of Key Split user names to form a quorum.
8. Press <Enter> next to the `Key Split User Name` prompt to end Key Split user authorization.

Note – If you do not enter a sufficient quorum of Key Split credentials, the Setting a User's Passphrase process becomes a pending quorum operation. See "Pending Quorum Operation List Menu" on page 314 for more information.

---

9. Press <Enter> to return to the main menu.

Setting the KMA Management IP Address

This option modifies the Management address settings for the KMA. Initially, this information is set in the QuickStart program (see "Specifying the Network Configuration" on page 33), and can be changed here.

Note that in a large, multi-site Cluster, drives may only have connections to a subset of all the KMAs in the Cluster. This caution applies to the set of KMAs the drive can connect to.

Caution – This function should be used carefully. If you change the information for one KMA, all the other KMAs receive the updates immediately, assuming they are connected. If the KMA is disconnected, it updates the other KMAs when it is able to reconnect.

However, if for example you have two KMAs that are not connected to each other (network outage), and you change both IP addresses, they will not be able to reconnect when the network is repaired.

In this case, you must use the procedure for "Logging the KMA Back into the Cluster" on page 335 on one KMA to reconnect it with the other, and the Passphrase must be updated first. For example, if KMAs A and B are disconnected, and you change both IP addresses, then you must log into A and change B's passphrase. Then log into B's console and use the procedure for "Logging the KMA Back into the Cluster" on page 335 to re-attach it to A.

Care must also be taken with tape drives. Tape drives do not automatically receive the updated IP information; they only get updated IP information when a tape is mounted. Thus, if you are in a typical environment where tape jobs only run at night, and you change all the KMA's IP addresses during the day, the drives will not be able to communicate with any KMA. If this happens, the drives must be re-enrolled with the OKM Cluster. To avoid this, change KMA IP addresses one at a time, wait for all drives to receive the change, then change the next.

To set the KMA Management IP addresses:

1. At the `Please enter your choice:` prompt on the main menu, type **3** and press <Enter>.

The current KMA Management IP address settings are displayed. The IPv6 address fields are blank when the KMA is not configured to use IPv6 addresses.

```
Set KMA Management IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other KMAs or Users in your system.

Current settings:
  Management Configuration : Static
  Management IP Address    : 10.80.180.39
  Management Subnet Mask   : 255.255.254.0
  Management IPv6 Addresses: fe80::216:36ff:feca:15b6/10
                             2005::216:36ff:feca:15b6/64


Do you want to configure the Management Network interface to have
an IPv6 address? [y/n]:

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

Please enter the Management Network IP Address [10.80.180.39]:

Please enter the Management Network Subnet Mask [255.255.254.0]:

Are you sure that you want to commit these changes? [y/n]: y
```

2. Type either **n** or **y** at the `Do you want to configure the Management Network interface to have an IPv6 address` prompt.
3. Type either **n** or **y** at the `Do you want to use DHCP to configure the Management Network interface` prompt. If you type **n**, go to Step 4. If you type **y**, go to Step 6.
4. At the prompt, type the Management Network IP address and press <Enter>.
5. At the `Please enter the Management Network Subnet Mask:` prompt, type the subnet mask address, (for example **255.255.254.0**) and press <Enter>.
6. Type **y** at the `Are you sure that you want to commit these changes? [y/n]:` prompt.

Setting the KMA Service IP Addresses

This option modifies the Service address settings for the KMA. Initially, this information is set in the QuickStart program (see "Specifying the Network Configuration" on page 33), and can be changed here.

Note that in a large, multi-site Cluster, drives may only have connections to a subset of all the KMAs in the Cluster. This caution applies to the set of KMAs the drive can connect to.

Caution – This function should be used carefully. If you change the information for one KMA, all the other KMAs receive the updates immediately, assuming they are connected. If the KMA is disconnected, it updates the other KMAs when it is able to reconnect.

However, if for example you have two KMAs that are not connected to each other (network outage), and you change both IP addresses, they will not be able to reconnect when the network is repaired.

In this case, you must use the procedure for "Logging the KMA Back into the Cluster" on page 335 on one KMA to reconnect it with the other, and the Passphrase must be updated first. For example, if KMAs A and B are disconnected, and you change both IP addresses, then you must log into A and change B's passphrase. Then log into B's console and use the procedure for "Logging the KMA Back into the Cluster" on page 335 to re-attach it to A.

Care must also be taken with tape drives. Tape drives do not automatically receive the updated IP information; they only get updated IP information when a tape is mounted. Thus, if you are in a typical environment where tape jobs only run at night, and you change all the KMA's IP addresses during the day, the drives will not be able to communicate with any KMA. If this happens, the drives must be re-enrolled with the OKM Cluster. To avoid this, change KMA IP addresses one at a time, wait for all drives to receive the change, then change the next.

The current KMA Service IP address settings are displayed. The IPv6 address fields are blank when the KMA is not configured to use IPv6 addresses.

```
Set KMA Service IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other Agents in your system.

Current settings:
  Service Configuration : Static
  Service IP Address    : 192.168.1.39
  Service Subnet Mask   : 255.255.255.0
  Service IPv6 Addresses: fe80::216:36ff:feca:15b9/10
                          2005::216:36ff:feca:15b9/64


Do you want to configure the Service Network interface to have an
IPv6 address?
[y/n]: y

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

Please enter the Service Network IP Address [192.168.1.39]:

Please enter the Service Network Subnet Mask [255.255.255.0]:

Are you sure that you want to commit these changes? [y/n]: y
```

1. At the `Please enter your choice:` prompt on the main menu, type **4** and press <Enter>.
2. Type either **n** or **y** at the `Do you want to configure the Service Network interface to have an IPv6 address` prompt.
3. Type either **n** or **y** at the `Do you want to use DHCP to configure the Service Network interface` prompt. If you type **n**, go to Step 4. If you type **y**, go to Step 6.
4. At the prompt, type the Service Network IP address and press <Enter>.
5. At the `Please enter the Service Network Subnet Mask:` prompt, type the subnet mask address, (for example **255.255.255.0**) and press <Enter>.
6. Type **y** at the `Are you sure that you want to commit these changes? [y/n]:` prompt.

Viewing/Adding/Deleting Gateways

This menu option shows the current gateway settings (five gateways to a page) on the Management (M) and Service (S) network interfaces and asks the user to add a gateway, removea gateway, or accept the current gateway configuration.

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                     Netmask         IF
---- -------------------------- -------------------------- --------------- --
   1 default                    10.80.181.254               0.0.0.0         M
   2 default                    10.80.181.21                0.0.0.0         M
   3 default                    192.168.1.119               0.0.0.0         S
   4 10.0.0.0                   10.80.180.25                255.255.254.0   M
*  5 10.80.180.0                10.80.180.39                255.255.254.0   M

Press Enter to continue:

Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                     Netmask         IF
---- -------------------------- -------------------------- --------------- --
*  6 192.168.1.0                192.168.1.39                255.255.255.0   S
   7 192.168.25.0               10.80.180.25                255.255.255.0   M
   8 192.168.26.0               10.80.180.25                255.255.255.0   M
*  9 127.0.0.1                  127.0.0.1                   255.255.255.255
* 10 fe80::                     fe80::216:36ff:feca:15b6    10              M

(1) Continue
(2) Back
1
```

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                     Netmask         IF
---- -------------------------- -------------------------- --------------- --
* 11 fe80::                     fe80::216:36ff:feca:15b9    10              S

You can add a route, delete a route, or exit the gateway configuration.
Please choose one of the following:

(1)  Add a gateway
(2)  Remove a configured gateway (only if modifiable)
(3)  Exit gateway configuration
(4)  Display again
3
```

1. At the `Please enter your choice:` prompt on the main menu, type **5** and press <Enter>.
2. At the `(1)Continue (2)Back` prompt, type **1** to display the next few gateways or **2** to display the previous few gateways.
3. When the last gateways are displayed, at the `Please choose one of the following:` prompt, type **1**, **2**, **3,** or **4** and press <Enter>.

Note – If at any time the user presses Ctrl+c, no changes are saved and the user is returned to the main menu.

Specifying the DNS Settings

This menu option shows the DNS settings, and prompts the user for a new DNS domain (if you want to configure one) and the DNS server IP addresses.

```
Set DNS Configuration
------------------------------------------------------------

Press Ctrl-c to abort.

DNS configuration is optional, but necessary if this KMA
will be configured using hostnames instead of IP addresses.

Current DNS configuration:

Domain: central.sun.com
Nameservers: 10.80.0.5

Please enter the DNS Domain (blank to unconfigure DNS):
central.sun.com

Up to 3 DNS Name Servers can be entered. Enter each name
server separately, and enter a blank name to finish.

Please enter DNS Server IP Address #1: 10.80.0.5

Please enter DNS Server IP Address #2:
```

1. At the `Please enter your choice:` prompt on the main menu, type **6** and press <Enter>.
2. Enter the DNS domain name at the `Please enter the DNS Domain (blank to unconfigure DNS):` prompt.
3. Enter the DNS server IP address at the `Please enter DNS Server IP address` prompt. You can enter up to three IP addresses.
4. Press `<Enter>`, without specifying an IP address, to finish.

Resetting the KMA to the Factory Default

This menu option allows a Security Officer to reset the KMA to its factory default state.

Warning – The reset is not recoverable; the information on the KMA is gone.

This is a destructive process that results in the loss of all data that is stored on the hard disk. The system is forced to reboot and the file systems are reformatted and prepared to use the new encryption keys.

To reset the KMA to the factory default:

1. At the `Please enter your choice:` prompt on the main menu, type **7** and press <Enter>. The following information is displayed.

```
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:
```

Warning – All information on this KMA will be destroyed. Access to all protected data will be lost unless a backup of the KMA's data has been created or Cluster Peer KMAs are present.

---

2. At the `Zeroize KMA before resetting` prompt, enter either **n** or **y**. If you enter **y**, this will securely wipe all information off the hard drive.

Note – This operation takes approximately four hours.

---

3. At the `Type RESET to confirm` prompt, type RESET and press <Enter>. The following information is displayed, indicating that the KMA is resetting.

```
Resetting...
```

4. Once the authentication is completed, you are returned to QuickStart. See "Running the QuickStart Program" on page 31.

Enabling the Technical Support Account

The Technical Support menu option allows an operator to enable/disable the Operating System's support account and SSH access for that account. By default, both the Technical Support account and SSH access are disabled. Since an operator defines the passphrase for the support account, enabling the support account grants the OKM Console user limited access to the KMA.

1. To enable the Technical Support account:

At the `Please enter your choice:` prompt on the main menu, type **8** and press <Enter>. The following information is displayed, indicating that the support account is disabled.

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.

The support account is currently DISABLED.
************************ WARNING ***************************
Enabling the support account and SSH access is a SECURITY
RISK. These settings should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
************************************************************

Would you like to ENABLE the support account? [y/n]:
```

2. At the `Are you sure that you want to ENABLE the support account and assume this security risk? [y/n]` prompt, type **y** to enable the account and press <Enter>. Enabling SSH access allows Technical Support to diagnose a problem remotely.
3. At the prompt, type **y** and press <Enter>. The following information is displayed, indicating the purpose of SSH Host keys.

```
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.
```

The following screen asks you to regenerate the SSH keys and provide a passphrase for the support account.

```
Would you like to regenerate the SSH host keys? [y/n]:

A Passphrase for the support account must be at least 8
characters and at most 64 characters in length.

Please enter a Passphrase for the support account:

Please re-enter the Passphrase for the support account:

The maximum age of the Passphrase of the support account
is the maximum number of days that this Passphrase is valid.

When this age has been reached, then the support account
is disabled.

This number must be greater than 0.

Please enter the maximum age of this Passphrase: 2
```

4. At the `Would you like to regenerate the SSH host keys?` prompt, type **y** and press <Enter>.
5. Enter a passphrase at the `Please enter a Passphrase for the support account:` prompt.

Note – The passphrase must be at least as long as the passphrase minimum length security parameter. This value is set to 8 during the QuickStart program, but you can change it later in the OKM Manager GUI. See "Modifying the Security Parameters" on page 192.

---

6. Re-enter the passphrase.
7. Enter the maximum number of days the passphrase is valid.
8. Press <Enter> to return to the main menu.

```
Press Enter to continue:
```

Disabling the Technical Support Account

Note – This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

To disable the Technical Support account:

1. At the `Please enter your choice:` prompt on the main menu, type **8** and press <Enter>. The following information is displayed, indicating that the support account is enabled.

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.

The support account is currently ENABLED.

Would you like to DISABLE the support account? [y/n]:
```

2. At the prompt, type **y** to disable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to DISABLE the support account? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The SSH service automatically stops.

Enabling the Primary Administrator

The Primary Administrator menu option allows you to enable/disable Primary Administrator access on the KMA.

- To enable Primary Administrator access, you must first enable Technical Support (option **8**).
- This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

Caution – The Primary Administrator function allows someone logged in as Technical Support to gain Primary Administrator access, equivalent to root access. Since the passphrase for the Primary Administrator is known only by Oracle Support, only someone from Oracle Support can gain Primary Administrator access.

While dangerous, this may be necessary in some situations to recover the system from a problem, however, you may need direct guidance from back line support or engineering.

---

1. To enable Primary Administrator access:

At the `Please enter your choice:` prompt on the main menu, type **9** and press <Enter>. The following information is displayed, indicating that the access is disabled.

```
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. At the prompt, type **y** to enable the account and press <Enter>.

3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The Primary Administrator access has been enabled.

Disabling the Primary Administrator

The Primary Administrator menu option allows you to enable/disable Primary Administrator access on the KMA.

Note – This task can be *enabled* only by the Security Officer; it can be *disabled* by either an Operator or a Security Officer.

Disabling Primary Administrator access takes place immediately. If someone is connected as a Primary Administrator, and then this access is disabled, the next command they attempt will fail.

1. To disable Primary Administrator access:

At the `Please enter your choice:` prompt on the main menu, type **9** and press <Enter>. The following information is displayed, indicating that the access is enabled.

```
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. At the prompt, type **y** to disable the account and press <Enter>.
3. The following information is displayed, prompting you to confirm the change.

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. At the prompt, type **y** and press <Enter>. The Primary Administrator access has been disabled.

Setting the Keyboard Layout

This option allows you to change the keyboard layout from English to a variety of languages.

Note – The keyboard layout should be set to match the layout of the keyboard attached to the KMA in order for the KMA to correctly interpret key presses.

To set the keyboard layout:

1. At the `Please enter your choice:` prompt on the main menu, type **7** and press <Enter>. The following keyboard layouts are displayed.

```
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. At the `Please enter the keyboard layout [US-English]:` prompt, enter the language to want to change the keyboard layout to.
3. At the prompt, type **y** and press <Enter>. The following information is displayed, indicating that the change has been made. Press <Enter> to return to the main menu.

```
The keyboard layout has been applied successfully.

Press Enter to continue:
```

Logging Out

To log out of the current OKM Console session:

1. At the `Please enter your choice:` prompt on the main menu, type **0** and press <Enter>.
2. The current session terminates and the login prompt is displayed allowing the user to re-enter the OKM Console.

Other Role Functions

This section describes the functions the other roles (Compliance Officer, Backup Operator, Auditor, Quorum Member) can perform. They are:

- Setting the keyboard layout (page 357)
- Logging out of the KMA (page 358).

```
Oracle Key Manager Version 2.3 (Build1036)
------------------------------------------------------------

(1)  Set Keyboard Layout
(0)  Logout

------------------------------------------------------------
Please enter your choice:
```

Setting the Keyboard Layout

This option allows you to change the keyboard layout from English to a variety of languages.

Note – The keyboard layout should be set to match the layout of the keyboard attached to the KMA in order for the KMA to correctly interpret key presses.

To set the keyboard layout:

1. At the `Please enter your choice:` prompt on the main menu, type **1** and press <Enter>. The following keyboard layouts are displayed.

```
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. At the `Please enter the keyboard layout [US-English]:` prompt, enter the language to want to change the keyboard layout to.
3. At the prompt, type **y** and press <Enter>. The following information is displayed, indicating that the change has been made. Press <Enter> to return to the main menu.

```
The keyboard layout has been applied successfully.

Press Enter to continue:
```

Logging Out

To log out of the current OKM Console session:

1. At the `Please enter your choice:` prompt on the main menu, type **0** and press <Enter>.
2. The current session terminates and the login prompt is displayed allowing the user to re-enter the OKM Console.

CHAPTER 12

Command Line Utilities

This chapter describes command line utilities that allow users to launch backups, export keys, import keys, and list data units from the command line instead of from the OKM Manager GUI.

The following command line utilities are available:

- "OKM Command Line Utility" on page 360
- "Backup Command Line Utility" on page 377.

Note – The OKM Command Line utility supersedes the Backup Command Line utility. Use the OKM Command Line utility whenever possible.

OKM Command Line Utility

The OKM Command Line utility allows you to:

- Schedule automated backups
- back up OKM core security
- import and export keys
- destroy keys
- list audit events
- list data units.

Unlike the Backup Command Line utility, this utility can use X.509 certificates to authenticate itself as a valid OKM user instead of a username and passphrase, so you are not required to enter a passphrase on the command line.

The following table details the roles that can perform these functions:

TABLE 12-1 OKM Command Line Utility - User Role Access

Action:	Role:
Backup	Backup Operator
Back up OKM Core Security	Security Officer
Import/Export Keys	Operator
Destroy Keys	Operator
List Audit Events	All Roles*
List Data Units	Operator/Compliance Officer

* If you specify agent IDs, data unit IDs, or key IDs, you must have the Operator or Compliance Officer role.

This utility is installed with the OKM Manager GUI using the same installer.

Note – If you want to enter link-local IPv6 addresses, invoke the OKM Command Line Utility and specify the link-local IPv6 address. Include the Zone ID (for example, "%4") at the end of the address.

Refer to "IPv6 Addresses with Zone IDs" on page 98 to see what steps you must follow for the initial setup.

Solaris/Windows Syntax

```
kms -v | --version | --help | -h
```

```
kms backup [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
           [ --retries=retries ] [ --timeout=timeout ]
           [ --verbose=boolean ]
           --kma=networkaddress
           --output=dirname
```

```
kms backupcs [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                 [ --directory=dirname ] | --oper=username ]
             [ --retries=retries ] [ --timeout=timeout ]
             [ --verbose=boolean ]
             --kma=networkaddress
             --output=filename
```

```
kms destroykeys [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                    [ --directory=dirname ] | --oper=username ]
                [ --retries=retries ] [ --timeout=timeout ]
                [ --verbose=boolean ]
                --kma=networkaddress
                --duids=filename | --all=true
                --keystate=keystate
                --comment="text"
```

```
kms export [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] | --oper=username ]
           [ --retries=retries ] [ --timeout=timeout ]
           [ --listwait=waittime ] [ --verbose=boolean ]
           --filter=filter | --duids=filename
           --kma=networkaddress
           --output=filename
           --partner=transferpartnerid
```

```
kms import [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
           [ --retries=retries ] [ --timeout=timeout ]
           [ --verbose=boolean ]
           --kma=networkaddress
           --input=filename
           --partner=transferpartnerid
           --keygroup=keygroupid
```

```
kms listauditevents [ [ [ --cacert=filename ]
                          [ --usercert=filename ] ]
                       [ --directory=dirname ] | --oper=username ]
                     [ --filter=filter ] [ --maxcount=count ]
                     [ --retries=retries ] [ --timeout=timeout ]
                     [ --verbose=boolean ]
                     [ --output=filename ]
                  [ --agentids=agentids | --dataunitids=dataunitds
                     | --keyids=keyids ]
                     --kma=networkaddress
```

```
kms listdu [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
           [ --filter=filter ]
           [ --retries=retries ] [ --timeout=timeout ]
           [ --listwait=waittime ] [ --verbose=boolean ]
           [ --output=filename ]
           --kma=networkaddress
```

Parameter Descriptions

Subcommands

backup

The `backup` subcommand generates a backup of the OKM data and downloads this backup to a backup data file and a backup key file in the specified output directory.

backupcs

The `backupcs` subcommand generates a backup of the OKM core security and stores this backup in an output file.

destroykeys

The `destroykeys` subcommand destroys deactivated or compromised keys.

export

The `export` subcommand creates a secure key file for a Transfer Partner that has been established with the OKM. All keys associated with a list of data units are exported using this key file and are protected using an AES-256-bit key that signs the key file. This list of data units is the result of the given filter string or file name. This key file can then be used to import the keys into the Transfer Partner's OKM using the `import` subcommand. Up to 1,000 Data Units can be exported on a single invocation of the `kms` command.

import

The `import` subcommand reads a secure key file for a Transfer Partner that has been established with the OKM. Keys and their associated data units are imported using this key file. The key transfer private key of the importing OKM is used to validate the key file. This file must be one that was previously exported from another OKM using the `export` subcommand.

listauditevents

The `listauditevents` subcommand lists audit events.

listdu

The `listdu` subcommand lists data units and their properties. This subcommand can be invoked prior to executing the `export` subcommand to determine the data units that are exported using the specified filter (if any).

Options

The lists of options below show the long and short option name. A long option name is separated from its value by an equals sign (=); a short option name is separated from its value by a space.

The following options are used for user authentication.

Note – Users must first export the Root CA and user X.509 certificates from the OKM Manager GUI before invoking this utility with the `--cacert`, `--directory`, and `--usercert` options.

--cacert=*filename*

Short name: -a

Specifies a OKM Root CA X.509 certificate PEM file for this utility to use to authenticate itself with the OKM. If not specified, then the utility looks for a ca.crt file in the directory specified by the `--directory` option. This option is mutually exclusive with the `--oper` option.

--directory=*dirname*

Short name: -d

Specifies a directory in which to search for a PEM file containing a OKM Root CA X.509 certificate and a PEM file containing a OKM user X.509 certificate. If not specified, then this utility looks for the certificate files in the current working directory. This option is mutually exclusive with the `--oper` option.

--oper=*username*

Short name: -b

Specifies the OKM User ID for this utility to use to authenticate itself with the OKM. If specified, it prompts for the user's passphrase since certificates are not being used. This option is mutually exclusive with the `--cacert`, `--usercert`, and `--directory` options.

--usercert=*filename*

Short name: -u

Specifies a OKM user's X.509 certificate PEM file for this utility to use to authenticate itself with the OKM. This certificate file must also contain the user's private key. If not specified, then the utility looks for a `clientkey.pem` file in the directory specified by the `--directory` option. This option is mutually exclusive with the `--oper` option.

The following list shows additional options.

--agentids=*agentids*

Short name: -A

Specifies a comma-separated list of agent IDs for associated audit events. Each agent ID must be between 1 and 64 characters in length. The OKM user must have the Operator or Compliance Officer role to be able to specify this option. This option is mutually exclusive with the `--dataunitids` and `--keyids` options.

--all=true

Short name: -l

Indicates that this utility destroys all deactivated or compromised keys, as indicated by the `--keystate` option, for all data units. This option is mutually exclusive with the `--duids` option.

--comment="*text*"

Short name: -C

Specifies a comment describing the key destruction. This comment must be between 1 and 64 characters in length.

--dataunitids=*dataunitds*

Short name: -D

Specifies a comma-separated list of data unit IDs for associated audit events. Each data unit ID must be 32 hexadecimal characters. The OKM user must have the Operator or Compliance Officer role to be able to specify this option. This option is mutually exclusive with the `--agentids` and `--keyids` options.

--duids=*filename*

Short name: -i

For key export or destruction, this option specifies a filename containing a set of data unit IDs, one per line, newline delimited. Each data unit ID must be 32 hexadecimal characters. On the `destroykeys` subcommand, if a particular data unit does not have any deactivated or compromised keys, then that data unit is ignored. If the specified file is empty, then the `destroykeys` subcommand destroys all deactivated or compromised keys for all data units (see the `--all` option). This option is mutually exclusive with the `--filter` and `--all` options.

--filter=*filter*

Short name: -f

Specifies a filter string that is processed to generate either a list of data unit IDs to display or export or a list of audit events to display. The string must be enclosed in quotes (double quotes on Windows) if it contains white space (see "Examples" on page 370).

Note – Exporting takes time proportional to the number of data units and keys, so typically you should specify a filter that reduces the set of data units.

On the export subcommand, this option is mutually exclusive with the `--duids` option.

On the `export` and `listdu` subcommands, the syntax of this filter string is:

```
DUState=state[, Exported=boolean ][, Imported=boolean]
[, DataUnitID=duid][, ExternalTag=tag][, ExternalUniqueID=euid]
```

`DUState=`*`state`*
Where *`state`* can be "normal," "needs-rekey," or "normal+needs-rekey." If the `DUState` filter is not specified, then the default is "DUState=normal+needs-rekey."

`Exported=`*`boolean`*
Where *`boolean`* can be "true" or "false." If the `Exported` filter condition is not specified, then data unit selection does not consider the exported state, so both exported data units and data units that have not been exported yet are eligible for selection.

`Imported=`*`boolean`*
Where *`boolean`* can be "true" or "false." If the `Imported` filter condition is not specified, then data unit selection does not consider the imported state, so both imported data units and data units that have not been imported yet are eligible for selection.

`DataUnitID=`*`duid`*
Where *`duid`* is a Data Unit ID.

`ExternalTag=`*`tag`*
Where *`tag`* is an External Tag (must be padded to 32 characters with spaces for Data Units created for LTO tape drives).

`ExternalUniqueID=`*`euid`*
Where *`euid`* is an External Unique ID.

On the `listauditevents` subcommand, the syntax of this filter string is:

```
StartDate=date[, EndDate=date ][, Severity=text]
[, Operation=text][, Condition=text] [, Class=text]
[, RetentionTerm=text] [, KMAName=kmaname][, EntityID=entityid]
[, EntityNetworkAddress=netaddress] [, SortOrder=order]
[, ShowShortTerm=boolean]
```

`StartDate=`*`date`*
Where `date` has the format: *YYYY-MM-DD hh*:*mm*:*ss* and represents UTC time.

`EndDate=`*`date`*
Where `date` has the format: *YYYY-MM-DD hh*:*mm*:*ss* and represents UTC time.

`Severity=`*`text`*
Where *`text`* is an audit severity string (e.g., "Error").

`Operation=`*`text`*
Where *`text`* is an audit operation string (e.g., "Retrieve Root CA Certificate").

`Condition=text`
Where *`text`* is an audit condition string (e.g., "Success").

`Class=`*`text`*
Where *`text`* is an audit class string (e.g., "Security Violation").

`RetentionTerm=`*`text`*
Where *`text`* is an audit retention term string (e.g., "MEDIUM TERM RETENTION").

`KMAName=`*`kmaname`*
Where *`kmaname`* is a KMA name.

`EntityID=`*`entityid`*
Where *`entityid`* is an Entity ID.

`EntityNetworkAddress=`*`netaddress`*
Where *`netaddress`* is an IP address or host name.

`SortOrder=`*`order`*
Where *`order`* can be "`asc`" or "`desc`." By default, audit events are displayed in descending order by Created Date.

`ShowShortTerm=`*`boolean`*
Where *`boolean`* can be "`true`" or "`false`." By default, audit events that have a short term retention are not displayed.

--help

Short name: -h

Displays help information.

--input=*filename*

Short name: -i

Specifies the file name from which data units and keys are to be imported. This file is also known as the key transfer file.

--keygroup=*keygroupid*

Short name: -g

Specifies the ID of a Key Group that is defined to the OKM.

--keyids=*keyids*

Short name: -K

Specifies a comma-separated list of key IDs for associated audit events. The OKM user must have the Operator or Compliance Officer role to be able to specify this option. This option is mutually exclusive with the `--agentids` and `--dataunitids` options.

--keystate=*keystate*

Short name: -s

Specifies the state of keys to be destroyed. The keystate value can be "`deact`" for deactivated keys, "`comp`" for compromised keys, or "`deact+comp`" for deactivated or compromised keys.

--kma=*networkaddress*

Short name: -k

Specifies the network address of the KMA to issue the request. The network address can be a host name, an IPv4 address, or an IPv6 address.

--listwait=*waittime*

Short name: -w

Specifies the number of seconds between List Data Units requests issued by the `export` and `listdu` subcommands. The default value is 2.

--maxcount=*count*

Short name: -c

Specifies the maximum number of audit events to list. The default value is 20,000.

--output=*filename* or ***dirname***

Short name: -o

Specifies the file name where the results are stored. These results are the backup on `backup` and `backupcs` requests, the key transfer file on `export` requests, a listing of the data units and their properties on `listdu` requests, and a listing of audit events on `listauditevents` requests. On `listdu` and `listauditevents` requests, "-" may be specified for `stdout`, which is also the default. On `backup` requests, this option specifies the directory where the backup data file and backup key file are downloaded.

--partner=*transferpartnerid*

Short name: -p

Specifies the ID of the Transfer Partner that is defined to the OKM and that is eligible to send or receive exported keys.

--retries=*retries*

Short name: -r

Specifies the number of times that this utility tries to connect to the KMA, if the KMA is busy. The default value is 60.

--timeout=*timeout*

Short name: -t

Specifies the timeout value in seconds between these retries. The default value is 60.

--verbose=*boolean*

Short name: -n

Indicates that this utility generates verbose output, including progress status during the processing of the request. The *boolean* value can be "true" or "false."

--version

Short name: -v

Displays command-line usage.

Examples

All examples shown below are single-line commands. In some cases, the command line appears on multiple lines for readability. In Solaris examples, backslashes denote the continuation of a command line.

The following examples generate a backup using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.

Solaris:

```
kms backup --kma=mykma1 \
          --directory/export/home/Joe/.sunw/kms/BackupOperatorCertificates \
           --output=/export/home/KMSBackups
```

Windows:

```
kms backup --kma=mykma1
           --directory=D:\KMS\Joe\BackupOperatorCertificates
           --output=D:\KMS\KMSBackups
```

The following examples generate a backup using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
kms backup -k mykma1 -o /export/home/KMSBackups -b Joe
```

Windows:

```
kms backup -k mykma1 -o D:\KMS\KMSBackups -b Joe
```

The following examples export keys using certificates in the ca.pem and op.pem files in the current working directory for authentication.

Solaris:

```
kms export -k 10.80.88.88 -d "." -a ca.pem -u op.pem \
           -f "DUState = normal+needs-rekey, Exported = false" \
           -o Partner.dat -p Partner
```

Windows:

```
kms export -k 10.80.88.88 -d "." -a ca.pem -u op.pem
           -f "DUState = normal+needs-rekey, Exported = false"
           -o Partner.dat -p Partner
```

The following examples export keys using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
kms export --kma=mykma1 --oper=tpFreddy \
          --filter="Exported = false" --output=Partner.dat \
           --partner=Partner
```

Windows:

```
kms export --kma=mykma1 --oper=tpFreddy
          --filter="Exported = false" --output=Partner.dat
           --partner=Partner
```

The following examples import keys using certificates in the ca.crt and clientkey.pem files in the current working directory for authentication.

Solaris:

```
kms import --kma=10.80.88.88 --directory="." \
           --input=DRKeys.dat --partner=Partner \
           --keygroup=OpenSysBackupKeyGroup
```

Windows:

```
kms import --kma=10.80.88.88 --directory="."
           --input=DRKeys.dat --partner=Partner
           --keygroup=OpenSysBackupKeyGroup
```

The following examples import keys using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
kms import --kma=mykma1 --oper=Joe --input=DRKeys.dat \
           --partner=Partner --keygroup=OpenSysBackupKeyGroup
```

Windows:

```
kms import --kma=mykma1 --oper=Joe --input=DRKeys.dat
           --partner=Partner --keygroup=OpenSysBackupKeyGroup
```

The following examples list data units using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.

Solaris:

```
kms listdu  --kma=10.80.88.88 \
            --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
            --output=/export/home/KMSDataUnits
```

Windows:

```
   kms listdu --kma=10.80.88.88
              --directory=D:\KMS\Joe\OperatorCertificates
              --output=D:\KMS\KMSDataUnits
```

The following examples list data units using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
    kms listdu -k mykma1 -b Joe -f "Exported=false" \
               --output=/export/home/KMSDataUnits
```

Windows:

```
    kms listdu -k mykma1 -b Joe -f "Exported=false"
               --output=D:\KMS\KMSDataUnits
```

The following examples list audit events using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.

Solaris:

```
kms listauditevents --kma=10.80.88.88 \
               --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
                    --filter=Severity=Error \
                    --output=/export/home/KMSAuditEvents
```

Windows:

```
  kms listauditevents --kma=10.80.88.88
                     --directory=D:\KMS\Joe\OperatorCertificates
                      --filter=Severity=Error
                      --output=D:\KMS\KMSAuditEvents
```

The following examples list audit events using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
  kms listauditevents -k mykma1 -b Joe -f "Severity=Error" \
                     --output=/export/home/KMSAuditEvents
```

Windows:

```
  kms listauditevents -k mykma1 -b Joe -f "Severity=Error"
                     --output=D:\KMS\KMSAuditEvents
```

The following examples destroy all compromised keys using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.

Solaris:

```
kms destroykeys --kma=10.80.88.88 \
              --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
                  --all=true --keystate=comp \
                  --comment="Joe destroyed compromised keys"
```

Windows:

```
 kms destroykeys --kma=10.80.88.88
                 --directory=D:\KMS\Joe\OperatorCertificates
                 --all=true --keystate=comp
                 --comment="Joe destroyed compromised keys"
```

The following examples destroy deactivated keys associated with a list of data unit IDs using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
kms destroykeys -k mykma1 -b Joe -i DeactivatedDUIDs.txt \
                -s deact -C "Joe destroyed deactivated keys"
```

Windows:

```
kms destroykeys -k mykma1 -b Joe -i DeactivatedDUIDs.txt
                -s deact -C "Joe destroyed deactivated keys"
```

The following examples back up core security using certificates in the ca.crt and clientkey.pem files in the given directory for authentication.

Solaris:

```
kms backupcs --kma=10.80.88.88 \
      --directory=/export/home/Joe/.sunw/kms/SecurityOfficerCertificates \
             --output=/export/home/KMSCoreSecurity.xml
```

Windows:

```
kms backupcs --kma=10.80.88.88
             --directory=D:\KMS\Joe\SecurityOfficerCertificates
             --output=D:\KMS\KMSCoreSecurity.xml
```

The following examples back up core security using the user ID and passphrase of a OKM user for authentication.

Solaris:

```
kms backupcs -k mykma1 -b Joe -o /export/home/KMSCoreSecurity.xml
```

Windows:

```
kms backupcs -k mykma1 -b Joe -o D:\KMS\KMSCoreSecurity.xml
```

Exit Values

The following exit values are returned:

```
0    Successful completion
>0   An error occurred
```

Sample Perl Scripts

The following are some basic *perl* scripts that can be customized and run on either Solaris or Windows. These examples all use certificate-based authentication and require that the Root CA certificate and user's certificate reside in the current working directory.

Note – The perl scripts are not installed with the OKM Command Line utility. If you want to invoke the OKM Command Line utility from a perl script, use a text editor to create one that looks similar to one of the perl scripts shown here.

- `listdu.pl`

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="kms";
$KMA="kma1.somewhere.com";
$FILTER="--filter=Exported=false";
$DIRECTORY=".";
$OUTPUT="listdu.txt";
system("$cmd listdu --verbose=true --directory=$DIRECTORY --kma=$KMA $FILTER
       --output=$OUTPUT")
```

- `export.pl`

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="kms";
$KMA="kma1.somewhere.com";
$TP="DestinationPartner";
$FILTER="Exported=false";
$OUTPUT="$TP.dat";
system("$cmd export --verbose=true --kma=$KMA --directory=. --filter=$FILTER
       --partner=$TP --output=$OUTPUT");
```

- import.pl

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="kms";
$KMA="kma1.somewhere.com";
$TP="SourceTransferPartner";
$KEYGROUP="MyKeyGroup";
$INPUT="../aberfeldy/KeyBundle.dat";
system("$cmd import --verbose=true --kma=$KMA --directory=. --partner=$TP
       --keygroup=$KEYGROUP --input=$INPUT");
```

- backup.pl

```
#!/opt/csw/bin/perl
## the following must be in your path
$cmd="kms";
$KMA="kma1.somewhere.com";
$DIRECTORY=".";
$OUTPUT=".";
system("$cmd backup --verbose=true --directory=$DIRECTORY --kma=$KMA
       --output=$OUTPUT")
```

Backup Command Line Utility

The Backup Command Line utility allows you to launch a backup from the command line instead of from the Backup List menu. You can also schedule automated backups.

This utility is installed with the OKM Manager GUI using the same installer.

Note – If you want to enter link-local IPv6 addresses, invoke the Backup Utility and specify the link-local IPv6 address. Include the Zone ID (for example, "%4") at the end of the address.

Refer to "IPv6 Addresses with Zone IDs" on page 98 to see what steps you must follow for the initial setup.

Solaris Syntax

```
OKM_Backup [-UserID userid] [-Passphrase passphrase]
           -KMAIPAddress IPaddress -BackupFilePath pathname
           [-Retries retries] [-Timeout timeout]
```

Windows Syntax

```
OKMBackupUtility [-UserID userid] [-Passphrase passphrase]
                 -KMAIPAddress IPaddress -BackupFilePath pathname
                 [-Retries retries] [-Timeout timeout]
```

Parameter Descriptions

userid

The Backup Operator user ID. This **must** be a Backup Operator.

passphrase

The passphrase for the user ID.

Note – If the *userid* or *passphrase* value is not specified, the utility prompts for these values.

IPaddress

The KMA Management Network Address on which to launch the backup.

pathname

The location where the Backup File and Backup Key File should be downloaded on your system.

retries

The number of times that this utility tries to connect to the KMA, if the KMA is busy. The default is **60**.

timeout

The timeout value in seconds between these entries. The default is **60**.

Example

The following example creates a Backup File (format: OKM-Backup-*backupid-timestamp*.dat) and a Backup Key File (format: OKM-BackupKey-*backupid-timestamp*.xml)**.**

```
OKM_Backup -UserID MyBackupOperator -Passphrase secret2Me \
            -KMAIPAddress 129.80.60.172 \
            -BackupFilePath /tmp/MyKMSDownloads
```

APPENDIX **A**

SNMP Management Information Base (MIB) Data

This appendix describes SNMP information for users who have configured an SNMP Agent in their network and have defined SNMP Managers in the OKM Manager GUI. When at least one SNMP Manager is defined in the OKM Manager GUI, the KMAs will send SNMP Informs to the IP address of that SNMP Manager(s).

The KMAs use Object Identifiers (OIDs) to send the following information:

TABLE A-1 KMA Object Identifiers

OID Value	Type	Description
1.3.6.1.4.1.42.2.22.99	----	Generic trap
1.3.6.1.4.1.42.2.22.99.1	string	Date/time
1.3.6.1.4.1.42.2.22.99.2	string	Audit event class
1.3.6.1.4.1.42.2.22.99.3	string	Audit event operation
1.3.6.1.4.1.42.2.22.99.4	string	Audit event condition
1.3.6.1.4.1.42.2.22.99.5	string	Entity ID
1.3.6.1.4.1.42.2.22.99.6	string	Network address
1.3.6.1.4.1.42.2.22.99.7	string	Message

Refer to "SNMP Manager List Menu" on page 143 for details on viewing, creating, and modifying SNMP managers.

Glossary

A

Abnormal end of task (abend) A software or hardware problem that terminates a computer processing task.

Advanced Encryption Standard (AES) A FIPS-approved NIST cryptographic standard used to protect electronic data.

AES See Advanced Encryption Standard.

Agent Various types of encryption agents can be created to interact with the OKM for creating and obtaining keying material. The StorageTek T10000 models A and B, T9840D, and the HP LTO Gen 4 and Gen 5 tape drives are types of encryption agents when enabled for encrypting.

Agent API See Agent Library API.

Agent Library The Agent Library is used by an Agent to retrieve key material from a OKM.

Agent Library API The API provided by the Agent Library. Agents call this API.

Audit See Audit Log.

Audit Log The OKM Cluster maintains a log of all auditable event occurring throughout the system. Agents may contribute entries to this log for auditable events.

Auditor A user role that can view system audit trails (Audit List events and KMA security parameters).

Autonomous Lock When autonomous unlock is enabled a quorum of Security Officers is required to unlock a locked KMA. When disabled, the KMA can be unlocked by any Security Officer.

B

Backup File The file created during the backup process that contains all the information needed to restore a KMA. Encrypted with a key generated specifically for the backup. The key is contained in the corresponding backup key file.

Backup Key File A file generated during the backup process containing the key used to encrypt the backup file. This file is encrypted using the system master key. The master key is extracted from the core security backup file using a quorum of the Key Split Credentials.

Backup Operator A user role that is responsible for securing and storing data and keys.

BOT Beginning of Tape.

C

CA See Certificate Authority (CA).

Certificate A Certificate is a digitally-signed document that serves to validate the holder's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (Subject DN), a serial number, validity dates, holder's public key, Issuer's DN, and the digital signature of the Issuer for authentication. The Issuer attests that the holder's name is the one associated with the public key in the document.

Certificate Authority (CA) A Certificate Authority registers end-users, issues their certificates, and can also create CAs below them. The KMAs themselves act as the certificate authority to issue certificates to users, agents, and other KMAs.

Cluster A Cluster is a set of Key Management Appliances that are grouped together into a single system to enhance fault tolerance, availability, and scalability.

Communications key Adds another layer of encryption and authentication during transmission over a LAN from the token to the drive.

Compliance Officer A user role that manages the flow of data through your organization and can define and deploy data contexts (Key Groups) and rules that determine how data is protected and ultimately destroyed (Key Policies).

Critical Security Parameter Security-related information (for example, secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.

Crypto-Accelerator A Crypto-Accelerator is a hardware device (a card) that can be used to increase the rate of data encryption/decryption, thereby improving system performance in high demand conditions.

Crypto-active And encryption-capable tape drive that has had the encryption feature turned on in the drive.

Crypto-ready A tape drive that has the ability to turn on device encryption and become encryption-capable.

Cryptography The art of protecting information by transforming it (encrypting) into an unreadable format, called cipher text. Only those who possess a special *key* can decipher (decrypt) the message into its original form.

Cryptoperiods The length of time in which a key can be used for encryption. It starts when the key is first assigned to the drive. This value corresponds to the "Originator Usage Period" in NIST 800-57.

D

Data Unit Data units are abstract entities within the OKM that represent storage objects associated with OKM policies and encryption keys. The concrete definition of a data unit is defined by the Encryption Agent that creates it. For tape drives, a data unit is a tape cartridge.

Device key Enables the tape drive for encryption. KMS Version 1.x term.

E

EKT Enabling key token (device keys). KMS Version 1.x term.

Enable key Unique 64 character key used to enable the tape drive. See also PC Key.

Encryption The translation of data into a secret code. Encryption is one of the most effective ways to achieve data security. To read an encrypted file, you must have access to a special key or password that enables you to decipher it.

F

FIPS Federal Information Processions Standards. The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration and Laboratories, which develops and promotes standards and technology, including:

- Computer Security Division and Resource Center (CSRC)
- Federal Information Processing Standards (FIPS).

For more information visit:
http://www.nist.gov/

G

GUI Graphical User Interface.

H

Hash Message Authentication Code (HMAC) In cryptography, a keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key.

I

Internet Protocol (IP) A protocol used to route data from its source to its destination in an Internet environment.

Internet Protocol (IP) address A four-byte value that identifies a device and makes it accessible through a network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 to 255. For example, 129.80.145.23 could be an IP address.
Also known as TCP/IP address.

K

Key A key in this context is a symmetric data encryption key. Agents can request new key material for encrypting data corresponding to one or more Data Units. A key belongs to a single Key Group so that only Agents associated with the Key Group can access the key. Keys have encryption and decryption cryptoperiods that are dictated by the Key Policy associated with the Key Group of the particular key. The type of key (that is, its length and algorithm) is specified by the Encryption Agent.

Keys A random string of bits generated by the Oracle Key Manager, entered from the keyboard or purchased. Types of keys include:

- Device keys enable the tape drive encryption feature.
- Media keys encrypt and decrypt customer data on a tape cartridge.
- PC Keys enable the tape drive for encryption.
- Communication key adds another layer of encryption (authentication) to the media key during transmission over the LAN from the token to the drive.
- Split keys are unique to each drive and work with the wrap key for protection.
- Wrap keys encrypt the media key on the LAN and the token.

Key Group Key Groups are used for organizing keys and associating them with a Key Policy. Key Groups are also used to enforce access to the key material by the Encryption Agents.

Key Management Appliance (KMA) A SunFire X2100-M2 server preloaded with the OKM software. The appliance is a proven, dual-core processor with a Solaris 10 operating system that delivers policy-based key management and key provisioning services.

Key Policy A Key Policy provides settings for the cryptoperiods to be applied to keys. Each Key Group has a Key Policy, and a Key Policy may apply to zero or more Key Groups. The encryption and decryption cryptoperiods specified on the policy limit the usage of keys and trigger key life cycle events, such as the deactivation or destructions of keys.

Key Policies also control where keys governed by the Key Policy can be exported to other Key Transfer Partners or imported from other Key Transfer Partners.

Key Transfer File A file containing keys and associated data units (if defined) used to move key material from one OKM Cluster to another. Both parties to the transfer must configure a key Transfer Partner of the other party to the exchange. The key transfer file is signed and encrypted to ensure both privacy of the transferred information as well its integrity.

Key Transfer Partner The Key Transfer Partner is the recipient of keys being exported from one OKM to another.

KMA See Key Management Appliance.

M

Media key Encrypts and decrypts customer data on a tape cartridge.

N

network An arrangement of nodes and branches that connects data processing devices to one another through software and hardware links to facilitate information interchange.

NIST National Institute of Standards and Technology.

O

OKM See Oracle Key Manager.

OKM Cluster A set of one or more interconnected KMAs. All the KMAs in a OKM Cluster should have identical information. This will not be the case only when a OKM is down, or when a newly created piece of information has not yet propagated through all KMAs in the OKM Cluster. An action taken on any KMA in the OKM Cluster will eventually propagate to all KMAs in the OKM Cluster.

OKT Operational key token (media keys). KMS Version 1.x term.

Operator A user role responsible for managing the day-to-day operations of the system.

Oracle Key Manager (OKM) A system providing key management. The Oracle system has a OKM component providing key management on behalf of encryption agents.

P

PC Key Enables the tape drive to read and write in encrypted mode.

Q

Quorum Member A user role that views and approves pending quorum operations.

R

Read key This is a media key that is used when reading data from a tape.

Rijndael algorithm An algorithm selected by the U.S. National Institute of Standards and Technology (NIST) for the Advanced Encryption Standard (AES). Pronounced "rain-dahl," the algorithm was designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name.

RSA In cryptography, **RSA** is an algorithm for public-key cryptography created by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. The letters **RSA** are the initials of their surnames.

S

Secure Hash Algorithms (SHA) Secure Hash Algorithms are cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.

Security Officer A user role that manages security settings, users, sites, and Transfer Partners.

Security Policy A rigorous statement of the sensitivity of organizational data, various subjects that can potentially access that data, and the rules under which that access is managed and controlled.

Shamir's Secret Sharing An algorithm in cryptography where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore a quorum or threshold scheme is used.

Site A site is an attribute of each OKM and Encryption Agent that indicates network proximity, or locality. Encryption Agents should try first to contact a KMA at the same site, then try to contact a KMA at a different site if no KMA at the local site responds.

System Dump A user-invoked operation that results in all the relevant data being collected into a single file and then that file being downloaded to the machine from which the user invoked this operation. Once the download is complete, this file is deleted from the KMA.

T

T10000 tape drive The T10000 tape drive is a small, modular, high-performance tape drive designed for high-capacity storage of data—up to 500 gigabytes (GB) of uncompressed data.

Token KMS Version 1.x term.
Tokens are handheld, intelligent devices that connect to a token bay with an Ethernet connection. The two roles of the tokens are:

- Enabling key token
- Operational key token.

Token bay KMS Version 1.x term.
A chassis that houses the physical tokens and provides power and connectivity for one or two tokens through the rear blind-mating connector. The token bay is compatible with a standard 19-inch rack—a 1U form factor. The token bay comes in two styles: desktop and rack-mount.

Transport Layer Security (TLS) A cryptographic protocol that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

U

UID A string that serves as a unique identifier for a OKM entity, e.g. an encryption agent or user.

Ultra Tape Drive Encryption Agent Ultra-compliant encrypting tape drives utilize Ultra Tape Drive Encryption Agent software for key management. These drives acquire key material from the OKM to be used with tape volumes. Each write from BOT results in the use of fresh key material being used for encryption of data on the volume. Consequently, the definition of a data unit maps to a tape volume where the external ID of the data unit is the volume serial number.

UTC Coordinated Universal Time.

V

Volume Serial Number A six-character alphanumeric label used to identify a tape volume.

W

Wrap key Encrypts the media keys on the LAN and on the token.

Write key This is a media key that is used when writing data to a tape.

Z

Zeroize To erase electronically stored data, cryptographic keys, and Critical Security Parameters by altering or deleting the contents of the data storage to prevent recovery of the data.

Index

A

abnormal end of task (abend), defined 381
adding agents to a KMA, QuickStart Program 59
adding gateways, OKM Console 343
adding gateways, QuickStart Program 36
adding gateways, QuickStart program 36
Adjust System Time menu 212
Advanced Encryption Standard (AES), defined 381
AES, defined 381
Agent Assignment to Key Groups menu 232
Agent library API, defined 381
Agent library, defined 381
Agent List menu 269
Agent, defined 381
Agent, definition 1
Agents
  assigning a Key Group to 241
  assigning to a Key Group 234
  creating 273
  deleting 278
  removing a Key Group from 243
  removing an Agent from a Key Group 236
  setting passphrases 277
  viewing an Agent list 270
  viewing or modifying agent details 276
applying software upgrades 295
approving pending quorum operations 318
assigning a Key Group to a Transfer Partner 247
assigning a Key Group to an Agent 241
assigning a Transfer Partner to a Key Group 251
assigning an Agent to a Key Group 234
Audit Event List menu 255
Audit Logs
  defined 381
  exporting 262
  viewing 256
  viewing details 261
Auditor
  defined 381
  description 14
  operations 311
  role 311
autonomous lock, defined 381
Autonomous Unlock Option menu 201
Autonomous Unlock option, caution 43

B

Backup Command Line utility
  Example 378
  parameter descriptions 377
  Solaris syntax 377
  Windows syntax 377
Backup command line utility
  description 377
  IPv6 addresses with Zone IDs 98
backup Core Security 195
backup file, defined 382
backup files
  confirming destruction of 306
  creating 305
  restoring 182
  viewing details 180, 303
  viewing history 177, 302
backup key file, defined 382
Backup List menu 176, 301
Backup Operator
  defined 382
  description 14
  operations 301
  role 301

C

CA Certificate 93
Certificate Authority, defined 382
certificate, defined 382
certificates
  Client 93
  converting PKCS12 format to PEM format 95
  Root CA 93
  saving 93
changing the passphrase 92
checking the SCA 6000 card 107
Client Certificate 93

clock, adjusting the local clock 212
Cluster
  connecting to 87
  defined 382
  definition 1
  joining an existing, QuickStart program 46
  logging the KMA back into 335
Cluster profile
  creating 87
  deleting 91
command line utilities
  Backup 377
  description 359
  IPv6 addresses with Zone IDs 98
  OKM 360
communications key, defined 382
Compliance Officer
  defined 382
  description 14
  operations 213
  role 213
compromising keys 262
configuration settings, specifying 96
configuration, network information 208
configuring Key Transfer Partners 152
configuring the Cluster, QuickStart program 39
confirming destruction of backup files 306
connecting to the OKM 87
console, remote connection to (ELOM/ILOM) 22
converting certificate formats 95
Core Security
  creating a backup 195
  description 193
Core Security Management menu 194
creating a Cluster profile 87
creating a Core Security backup 195
creating a Key Transfer Public Key 175
creating a KMA 109
creating a site 139
creating a system dump 187
creating a Transfer Partner 161
creating a user 122
creating an Agent 273
creating an SNMP Manager 147
creating backup files 305
creating Key Groups 228
creating Key Policies 218
critical security parameter, defined 382
Crypto-Accelerator, defined 382
crypto-active, defined 382
cryptography, defined 383
cryptoperiods 383
crypto-ready, defined 382

D

Data Unit List menu 262, 282
data unit, defined 383
Data Units
  description 282
  destroying post-operational keys 293
  modifying details 287
  viewing 283
  viewing details 287
deleting a Cluster profile 91
deleting a KMA 117
deleting a site 142
deleting Agents 278
deleting an SNMP Manager 150
deleting gateways, OKM Console 343
deleting gateways, QuickStart Program 36
deleting gateways, QuickStart program 36
deleting Key Groups 231
deleting Key Policies 221
deleting pending quorum operations 320
deleting users 130
destroying post-operational keys 293
device key, defined 383
dimensions, T10000 tape drive 387
disabling the Primary Administrator, OKM Console 331, 353
disabling the technical support account, OKM Console 330, 350
disconnecting from the KMA 91

E

EKT (enabling key token), defined 383
ELOM *See* Embedded Lights Out Manager
Embedded Lights Out Manager (ELOM)
  connecting to the KMA through ELOM 22
  remote connection overview 3
  using a network connection 24
enable key, defined 383
enabling the Primary Administrator, OKM Console 351
enabling the Technical Support account, OKM Console 348
enabling the Technical Support account, QuickStart program 34

encryption, defined 383
enrolling tape drives, QuickStart Program 59
entering initial Security Officer user credentials, QuickStart program 42
entering Key Split Credentials, QuickStart program 40
exiting from the OKM Manager 100
exporting Audit Logs 262
exporting keys 154

F

FIPS (Federal Information Processions Standards), defined 383

G

Glossary 381
GUI (graphical user interface), defined 383

H

Hash Message Authentication Code (HMAC), defined 384

I

ILOM *See* Integrated Lights Out Manager
Import Keys menu 280
importing a KMS 1.0 Key Export file 253
importing keys 154
initializing the KMA, QuickStart program 39
installing the Oracle Key Manager (OKM) 62
Integrated Lights Out Manager (ILOM)
  connecting to the KMA through ILOM 22
  remote connection overview 3
  using a network connection 27
Internet Protocol (IP) address, defined 384
Internet Protocol (IP), defined 384
invoking the OKM Manager 70
IPv6 addresses with Zone IDs 98

J

joining an existing Cluster, QuickStart program 46

K

Key Export file, importing a KMS 1.0 file 253
Key Group Assignment to Agents menu 238
Key Group Assignment to Transfer Partners menu 245
Key Group List menu 224
Key Group, defined 385
Key Groups
  assigning a Transfer Partner to 251
  assigning an Agent to 234
  assigning to an Agent 241
  assigning to Transfer Partners 247
  assigning Transfer Partners to 249
  creating 228
  definition 222
  deleting 231
  removing an Agent from 236
  removing from a Transfer Partner 248
  removing from an Agent 243
  removing Transfer Partners from 252
  viewing 225
  viewing Key Group assignments to Transfer Partners 246
  viewing or modifying details 230
  viewing Transfer Partners assigned to 250
Key Groups menu 224, 268
Key Management Appliance (KMA)
  adding gateways 36, 343
  adjusting the local clock 212
  checking the SCA 6000 card 107
  connecting to 22
  creating 109
  defined 385
  definition 1
  deleting 117
  deleting gateways 36, 343
  disconnecting from 91
  locking KMA core security 204
  locking or unlocking core security 204
  logging back into the Cluster 335
  logging into 324
  modifying a Key Pool size 307
  network configuration information for 208
  rebooting 329
  resetting to the factory default 346
  setting a passphrase 115
  setting the Management IP addresses 339
  setting the Service IP addresses 341
  shutting down 329
  specifying the DNS settings 38, 345
  TCP/IP connections to 11
  unlocking core security 205
  viewing 104
  viewing gateways 36, 343
  viewing or modifying details 112

viewing SNMP Managers 144
Key Policies
creating 218
deleting 221
description 214
modifying 220
viewing 214, 220
Key Policy List menu 214
Key Policy, defined 385
Key Sharing, overview 151
Key Split Configuration menu 197
Key Split Credentials
entering 40
modifying 198
viewing 197
key states and transitions, OKM 6
Key Transfer File, defined 385
Key Transfer Partner, defined 385
Key Transfer Partners
configuring 152
feature description 151
Key Transfer process 152
Key Transfer Public Key
creating 175
viewing details 174
viewing the list of 171
Key Transfer Public Key List menu 170
Key Transfer, overview 151
key, defined 384
keyboard layout, setting 332
keys
compromising 262
defined 384
destroying post-operational keys 293
exporting and importing 154
importing from a Key Transfer file 280
KMA List Menu 103, 307
KMA *See* Key Management Appliance

L

local clock, adjusting 212
Local Configuration menu 203
Lock/Unlock KMA menu 204
locking KMA core security 204
locking the KMA 204
logging into the Key Management Appliance 324
logging out of the OKM Console session 333, 355, 358
logging the KMA back into the Cluster, OKM Console 335

M

Management Information Base (MIB), SNMP information 379
Master Key Provider button 189
media key, defined 385
menu
Adjust System Time 212
Agent Assignment to Key Groups 232
Agent List 269
Audit Event List 255
Autonomous Unlock 201
Backup List 176, 301
Core Security Management 194
Data Unit List 262, 282
Help 74
Import Keys 280
Key Group Assignment to Agents 238
Key Group Assignment to Transfer Partners 245
Key Group List 224
Key Groups 224, 268
Key Policy List 214
Key Split Configuration 197
Key Transfer Public Key List 170
KMA List 103, 307
Local Configuration 203
Lock/Unlock KMA 204
Pending Quorum Operation List 314
Role List 131
Security Parameters 188
Site List 135
SNMP Manager List 143
Software Upgrade 294
System 72, 87
System Dump 186
System Time 210
Transfer Partner Assignment to Key Groups 249
Transfer Partners 156
Transfer Partners List 157
User List 118
View 73
menu accelerator keys 76
modifying a Data Unit's details 287
modifying a Key Pool size 307
modifying agent details 276
modifying Key Group details 230
modifying Key Policies 220

modifying Key Split Credentials 198
modifying KMA details 112
modifying security parameters 192
modifying site details 141
modifying SNMP Manager details 149
modifying user details 125

N

network configuration information 208
network configuration, specifying 33
network, defined 385
NIST, defined 385

O

OKM Cluster, defined 386
OKM Command Line utility
  description 360
  examples 370
  exit values 375
  IPv6 addresses with Zone IDs 98
  options 364
  parameter descriptions 363
  sample perl scripts 375
  syntax 361
OKM Console
  Auditor options 327
  Backup Operator options 327
  Compliance Officer options 327
  description 323
  launching 30
  Operator functions
    disabling the Primary Administrator 331, 330
    logging out 333
    rebooting the KMA 329
    setting the keyboard layout 332, 329
  Operator options 325
  other role functions
    logging out 358
    setting the keyboard layout 357
  Security Officer functions
    adding gateways 343
    deleting gateways 343, 353, 350
    enabling the Primary Administrator 351, 348
    logging out 355, 335
    resetting the KMA to the factory default 346
    setting a user's passphrase 337, 354, 339, 341, 345
    viewing gateways 343
  Security Officer options 326
  using 323
OKM Manager
  GUI
    Help menu 74
    Menu accelerator keys 76
    overview 71
    panes 78
    Shortcut keys 76, 72
    Toolbar buttons 76
    View menu 73
  operation details pane 79
  operations tree pane 78
  session audit log pane 80
  status bar 81
  using online help 77
OKM *See* Oracle Key Manager
OKT, defined 386
online help, using 14, 77
operations, role-based 15
Operator
  defined 386
  description 14
  operations 267
  role 267
Operator functions
  disabling the Primary Administrator 331
  disabling the technical support account 330
  logging out of the OKM Console session 333
  rebooting the KMA, OKM Console 329
  setting the keyboard layout 332
  shutting down the KMA 329
Oracle Key Manager (OKM)
  changing the passphrase 92
  Cluster, definition 1
  concepts
    Agents 2
    data units, key, Key Groups, and key policies 10
    initial setup, direct connect or remote console 3, 4
    key lifecycle 4
    network connections 2
    OKM Clusters 2, 6
    state transition 5
    users and role-based access control 9
  connecting to the OKM Cluster 87
  converting certificate formats from PKCS12 to PEM 95
  creating a Cluster profile 87
  defined 386
  deleting a Cluster profile 91
  description 61
  exiting from 100
  GUI
    definition 1

installing 62
introduction 1
invoking the OKM Manager
Solaris startup 70
Windows startup 70
saving certificates 93
setting up and managing 20
software requirements 14
specifying configuration settings 96
states
active 6
compromised 7
deactivated 7
pre-activation 6
typical network deployment 13
user roles 14
using the System menu 87
other role functions
logging out 358
setting the keyboard layout 357

P

passphrase
changing 92
setting 128
setting for a KMA 115
setting for a user 337
PC Key, defined 386
pending operations
approving 318
deleting 320
viewing details 317
Pending Quorum Operation List Menu 314
Post-operational Keys, destroying 293
Primary Administrator, disabling 331, 353

Q

QuickStart program
adding agents to a KMA 59
adding gateways 36
configuring the Cluster 39
deleting gateways 36
enabling the Technical Support account 34
enrolling tape drives 59
entering initial Security Officer user credentials 42
entering Key Split Credentials 40
initializing the KMA 39
joining an existing Cluster 46
restoring a Cluster from a backup 52
running 31
setting the Key Pool size 44
setting the KMA Management IP address 33
setting the KMA Service IP address 35
specifying the Autonomous Unlock preference 43
specifying the DNS settings 38
specifying the network configuration 33
starting 32
synchronizing KMA time 45
viewing gateways 36
Quorum Member
defined 386
description 14
operations 313
role 313

R

read key, defined 386
rebooting the KMA, OKM Console 329
remote connection to the console, ELOM/ILOM 22
removing a Key Group from a Transfer Partner 248
removing a Key Group from an Agent 243
removing a Transfer Partner from a Key Group 252
removing an Agent from a Key Group 236
resetting the KMA to the factory default 346
resetting the KMA to the factory default, OKM Console 346
restoring a backup 182
restoring a Cluster from a backup, QuickStart Program 52
retrieving security parameters 189
retrieving the system time 211
Rijndael algorithm, defined 386
Role List menu 131
role, viewing operations for 134
role-based operations 15
roles, Oracle Key Manager 14
roles, viewing 132
Root CA Certificate 93
RSA, defined 386

S

saving certificates 93
SCA 6000 card, checking 107
Secure Hash Algorithms (SHA), defined 386

Security Officer
  defined 386
  description 14
  operations 101
  role 102
Security Officer functions
  adding gateways 343
  deleting gateways 343
  disabling the Primary Administrator 353
  disabling the technical support account 350
  enabling the Primary Administrator 351
  enabling the Technical Support account 348
  logging the KMA back into the Cluster 335
  resetting the KMA to the factory default 346
  setting a user's passphrase 337
  setting the keyboard layout 354
  setting the KMA Management IP addresses 339
  setting the KMA Service IP addresses 341
  specifying the DNS settings 345
  viewing gateways 343
security parameters
  Master Key Provider 189
  modifying 192
  retrieving 189
Security Parameters menu 188
security policy, defined 387
setting a KMA passphrase 115
setting a user passphrase 128
setting a user's passphrase, OKM Console 337
setting an Agent's passphrase 277
setting the Key Pool size, QuickStart program 44
setting the keyboard layout 332
setting the keyboard layout, OKM Console 332, 354, 357
setting the KMA Management IP address, OKM Console 339
setting the KMA Management IP address, QuickStart program 33
setting the KMA Service IP address, OKM Console 341
setting the KMA Service IP address, QuickStart program 35
Shamir's Secret Sharing, defined 387
shortcut keys 76
shutting down the KMA 329
site details, viewing or modifying 141
Site List menu 135
site, defined 387
sites
  creating 139
  deleting 142
  viewing 136
size of tape drive 387
SNMP Manager
  creating 147
  deleting 150
  viewing for a KMA 144
  viewing or modifying details 149
SNMP Manager List menu 143
SNMP, Management Information Base information 379
software requirements, Oracle Key Manager 14
Software Upgrade menu 294
software upgrades, uploading and applying 295
specifying configuration settings 96
specifying the Autonomous Unlock preference, QuickStart program 43
specifying the DNS settings QuickStart program 38
specifying the DNS settings, OKM Console 345
specifying the network configuration, QuickStart program 33
starting the KMA, QuickStart program 39
starting the OKM Manager 70
starting the QuickStart program 32
states and transitions, OKM keys 6
synchronizing KMA time, QuickStart program 45
syntax, OKM Command Line utility 361
system dump
  creating 187
  defined 387
System Dump menu 186
system menu, using 87
System Time menu 210
system time, retrieving 211

T

T10000 tape drive
  defined 387
  description of 387
  size 387
technical support account
  disabling 330
token bay, defined 387
token, defined 387
toolbar buttons 76
Transfer Partner Assignment to Key Groups menu 249

Transfer Partners
assigning a Key Group to 247
assigning to a Key Group 251
assigning to Key Groups 249
creating 161
deleting 169
importing Keys and Data Units from a key transfer file 280
Key Group Assignment to 245
List 157
removing from a Key Group 252
removing Key Groups from 248
viewing and modifying details 165
viewing assignments to Key Groups 250
viewing Key Group assignments to 246
Transfer Partners menu 156
Transport Layer Security (TLS), defined 387

U

UID, defined 387
Ultra Tape Drive Encryption Agent, defined 388
unlocking KMA core security 205
unlocking the KMA 204
uploading software upgrades 295
user details, viewing or modifying 125
User List menu 118
user passphrase, setting 128
user roles, Oracle Key Manager 14
users
creating 122
deleting 130
viewing 119
using online help 77
using the OKM Console 323
using the System menu 87
UTC, defined 388
utilities, command line 359
utility, Backup command line
description 377
IPv6 addresses with Zone IDs 98
utility, OKM Command Line
description 360
utility, OKM command line
IPv6 addresses with Zone IDs 98

V

viewing a Data Unit's details 287
viewing agent details 276
viewing Audit Log details 261
viewing Audit Logs 256
viewing backup files details 180, 303
viewing backup files history 177, 302
viewing Data Units 283
viewing gateways, OKM Console 343
viewing gateways, QuickStart Program 36
viewing gateways, QuickStart program 36
viewing Key Group assignments to Transfer Partners 246
viewing Key Group details 230
viewing Key Groups 225
viewing Key Policies 220
viewing key policies 214
viewing Key Transfer Public Key details 174
viewing KMA details 112
viewing KMA SNMP Managers 144
viewing KMAs 104
viewing operations for 134
viewing pending operations details 317
viewing roles 132
viewing site details 141
viewing sites 136
viewing SNMP Manager details 149
viewing the Agent List 270
viewing the Key Split credentials 197
viewing the Key Transfer Public Key list 171
viewing Transfer Partner assignments to Key Groups 250
viewing user details 125
viewing users 119
volume serial number, defined 388

W

wrap key, defined 388
write key, defined 388

Z

zeroize
defined 388
resetting the KMA to the factory default 346
Zone IDs, specifying IPv6 addresses 98